Date	Description
UK	
Information Commissioner's Office ("ICO")	
10 June 2016	**'Jihadi John' might not be dead! Statement on decision notice FS50624782** Our readers will recall that the notorious 'Jihadi John' was believed to have been killed in a US drone strike in November 2015. He has subsequently been identified as the Mohammed Emwazi who had graduated from the University of Westminster in information studies and business management. Some of his university academic record has been leaked and published in the media.[1] If he is indeed dead, the Data Protection Act 1998 (DPA) will no longer apply to his personal data. In February 2016, Chris Vallance, a BBC Radio 4 reporter, made a formal request to the University under the Freedom of Information Act 2000 (FoIA) asking for all the electronic records it had about Emwazi. The University declined to provide the information and on appeal to the Information Commissioner, the University's decision was upheld.[2] There was media reaction to that decision, particularly because the detailed reasoning was contained in a confidential annex. On 10 June 2016, the Commissioner published an explanatory statement drawn from that confidential annex. The University has been reported as responding to the request by saying that it cannot be confident either that Mohammed Emwazi known as 'Jihadi John' is dead or that he is the same person about whom it holds a record.[3] How, therefore, did the Commissioner reach his decision? S 40 (2) of FoIA exempts from that Act any information about another individual falling within s 1(1) (a) to (d) of the DPA in cases where 'the disclosure of the information to a member of the public otherwise than under this Act [FoIA] would contravene— (i) any of the data protection principles, or (ii) section 10 of that Act (right to prevent processing likely to cause damage or distress) […]' Consequently, any organisation within the scope of FoIA which receives a request about an individual must consider whether the s 40 exemption applies. The Commissioner makes remarks of a general nature before reaching a conclusion. First, he *considers that 'any student*

[1] http://www.dailymail.co.uk/news/article-3242617/Radical-alert-Jihadi-John-s-university-report-finds-Islamic-students-society-dominated-hardline-believers.html
[2] https://ico.org.uk/media/action-weve-taken/decision-notices/2016/1624340/fs_50624782.pdf
[3] http://www.independent.co.uk/news/uk/home-news/jihadi-john-could-still-be-alive-foi-request-to-his-former-university-reveals-a7075346.html

Date	Description
	of a University will hold the expectation that any information held about their studies and their time at the University, including copies of correspondence with any departments within it, will remain confidential and out of the public domain'. Second, he continues to state that such a student will expect that the data would not be revealed in response to an FoI request. Third, the Commissioner nevertheless recognises that there is a legitimate public interest in disclosing information about Jihadi John. The Commissioner's latest statement makes no reference to doubts about the death of Jihadi John. The University, according to the Commissioner, could not be certain that the record it held for a Mohammed Emwazi was the record of the Mohammed Emwazi known as 'Jihadi John' and not the record of a person of a similar name. Consequently, the University treated the record it held as personal data which would be improper to disclose if it happened to belong to some innocent other person of the same name. The Commissioner concluded that disclosure of an unconnected person's data *'would be clearly and grossly unfair and unlawful. It would cause significant distress and upset to an unconnected individual. Such potential consequences clearly outweigh any legitimate public interests in the information being sought.'* The Commissioner's position is interesting in several respects and it would be valuable for it to be examined in the courts. First, his view about the confidentiality of student records. There was a time before the passing of the Data Protection Act 1984 when public and university examination results were treated as a matter of public record and published in newspapers. Disciplinary, health and similar records should also be confidential. But should students expect confidentiality for their examination results? Second, the Commissioner has adopted a highly precautionary approach to the application of the DPA. It would seem to be the case that a data controller must have definite proof of identity before disclosing personal data. In subject access cases, the Commissioner has previously taken a flexible approach – perhaps because, in practice, most individual data subjects are known personally to a representative of the organisation from whom they are seeking subject access and certainly the Commissioner has not previously expected highly formal documented evidence of identity in all cases. But the decision is consistent with the Commissioner's desire to see proper security around personal data as evidenced by his imposition of monetary penalties. **The full ICO statement can be found here.**
14 June 2016	**Worldwide Fight to Tackle Nuisance Messages Intensifies** A group of 11 enforcement authorities, including the ICO, has signed a memorandum of understanding (MoU) under which it has committed to sharing cross-border intelligence regarding nuisance calls and SMS messages. Along with the ICO, all signatories are also members of the London Action Plan, a group committed to collectively combating the global problem of nuisance messages. The signatories include:

Date	Description
	ACM (the Netherlands), the ACMA (Australia), CRTC and OPC (Canada), FTC and FCC (USA), NTSIT (UK) and KISA (Korea), the Department of Internal Affairs (New Zealand) and National Consumer Commission (South Africa). The MoU bolsters existing efforts by the ICO to tackle nuisance calls and SMS messages. In the last year, the ICO has issued a total of £2.3m in fines to organisations responsible for making more than 72m nuisance calls and sending almost 2m nuisance SMS messages. In a statement on the MoU Stephen Eckersley, ICO head of enforcement, said: *"This MoU means that authorities across the world, including the Information Commissioner's Office, are now actively sharing intelligence. This will help us enforce the law and stop the scourge of nuisance calls and spam texts."* **The full ICO press release can be found here.**
28 June 2016	**Annual Report and Financial Statements 2015-16 Published** The ICO has published its annual report for 2015/16 in which it outlines its key activities from the year, as well as its aims and concerns for the coming year. Of particular interest are the statistics provided by the ICO on the volume and nature of complaints received, and follow-up actions taken by the ICO. Operational Performance • The ICO saw an increase in data protection concerns brought to it, up by 15.1% to 16,388 cases. • Where the relevant sector was disclosed, the ICO identified Health as the sector generating most concerns (relating to 12% of the concerns received). • Where the nature of the complaint was disclosed, the ICO identified subject access as the reason generating most concerns (relating to 42% of the concerns received), followed by disclosure of data (18%), inaccurate data (12%), security (9%), right to prevent processing (6%), use of data (4%), fair processing (3%), retention of data (2%), obtaining data (2%) and excessive/irrelevant data (1%). • 75.4% of complaints resulted in no action for the data controller, 18.6% resulted in the ICO requiring the data controller to take action, in 2.4% of cases an improvement action plan was agreed, in 1.3% of cases an undertaking was served, in 0.7% of cases an advisory visit was recommended, and in 0.4% of cases a civil monetary penalty was issued. Privacy and Electronic Communications Regulation ('PECR')

Date	Description
	• Fewer PECR concerns were reported in 2015/16, down to 161,190 from 180,188 the previous year. 210 of these concerns related to cookies (up from 164 the previous year). • 17 civil monetary penalties totalling £1,985,000 were issued, including a £130,000 penalty issued to Pharmacy2U Ltd after it sold details of over 20,000 customers to a list marketing company (in breach of the "fair processing" principle). This was the first time that the ICO had issued a civil monetary penalty for this type of breach. • 3 mandatory fines were paid where communications service providers failed to report personal data breaches within the required timescales. • 9 enforcement notices were served on a range of marketing organisations. <u>The Right to be Forgotten</u> • Over 370 people sought help after search engines refused to remove results about them under the right to be forgotten - 1/3 related to criminal convictions. • The ICO issued an enforcement notice to Google Inc., requiring it to remove nine search results about an individual under the right to be forgotten. Google Inc. removed the links from the European versions of the search engine, however, the ICO ruled that Google Inc. should also remove the links from all versions of its search engine that were accessible from the UK. Google Inc. initially appealed this decision, but then agreed to remove the results. • 3 preliminary enforcement notices about delisting were issued to Google Inc. during the year, which were complied with. <u>Enforced subject access</u> S 56 DPA 1998 came into force in March 2015, making enforced subject access a criminal offence. In November 2015, the ICO finished its first criminal investigation, which resulted in a caution. <u>Prosecutions</u> • 8 prosecutions for non-notification offences; • 3 prosecutions for failure to respond to an information notice; • 3 prosecutions for unlawfully obtaining data; and • 3 cautions (two for unlawfully obtaining data, one for enforced subject access). **The full report is available here.**

Date	Description
Other UK News	
23 June 2016	**The UK votes to leave the EU: more information on the data protection implications of this can be found here.**
28 June 2016	**ICO Brexit Statement** In an announcement at the launch of the ICO's annual report on 28 June 2016, the Information Commissioner, Christopher Graham, updated the ICO's statement on the referendum result of 23 June 2016: *"Over the coming weeks we will be discussing with Government the implications of the referendum result and its impact on data protection reform in the UK.* *With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations and to consumers and citizens. The ICO's role has always involved working closely with regulators in other countries, and that will continue to be the case.* *Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to government to present our view that reform of the UK law remains necessary."* **The full ICO press release can be found here.**
5 July 2016	**Digital Economy Bill published** The Digital Economy Bill (the 'Bill') was published on 5 July 2016 and aims to implement a large number of different government commitments on the digital economy made in the Conservative Party Manifesto. The Bill is lengthy (currently running to 145 pages) and covers the following different elements, some of which will be of interest to data protection practitioners: Part 1: Access to Digital Services: This section will implement a new Broadband Universal Service Obligation (USO) for the UK, giving all citizens the legal right to request a 10Mbps broadband connection and enhancing Ofcom's powers to help consumers get access to better information. Consumers will also be able to switch providers more easily and the Bill ensures that consumers are automatically compensated if things go wrong with their broadband service. Part 2: Digital Infrastructure: This section introduces a new Electronic Communications Code to cut the cost, and simplify the building, of mobile and broadband infrastructure, new planning rules for building broadband infrastructure, and new measures to manage radio spectrum. Part 3: Online Pornography: This section will make it compulsory for all pornography websites to require age verification

Date	Description
	to prevent access to under 18s. It also introduces the concept of an 'age verification regulator' with new enforcement powers, including the ability to impose financial penalties on website operators failing to adhere to the new rules. Part 4: Intellectual Property: This section ensures that the penalties for online copyright infringement will equate to the penalties for physical copyright infringement. This means an increase in the current maximum prison sentence from two years to ten years. There is also the introduction of a new online design registration system, known as 'webmarking' to protect the registered design rights that businesses hold. Part 5: Digital Government: This section of the Bill aims to improve data sharing among government departments and, in particular, how data is used to tailor public services. The main changes being introduced are aimed at: • allowing public authorities to share personal data with other public authorities in specific contexts in order to improve the welfare of individuals (for example, to deliver winter fuel discounts); • improving access to civil registration data like births, deaths and marriages, so that public authorities do not send letters to people who are deceased and to make processes easier for users; • helping to detect and prevent the losses that the Government currently experiences due to fraudulent activity each year; • providing new mechanisms to detect and collect public sector debt; • helping individuals to manage their debt by providing a means of support; and • making it easier to use data for research purposes so that official statistics are more timely and accurate. Each clause includes proposed safeguards to protect the data, including through the DPA, and will ensure that data is shared appropriately and proportionately in the public sector. Part 6: Ofcom and other Regulation: This section provides new powers to Ofcom, including the power for Ofcom to require communications providers to collect, generate or retain information for the purpose of publication, either by the communications provider or by Ofcom. It also broadens the ability of Ofcom to regulate the activities of the BBC. This section also makes amendments to the DPA which places the ICO under a duty to publish, and keep under review, a direct marketing code of practice which will contain practical guidance promoting good practice in direct marketing activities. In preparing the code, the ICO must consult with trade associations and data subjects. The main benefit of the code would be that the ICO is better able to enforce sanctions against nuisance callers and spammers, and ensure that appropriate consent is obtained from consumers. The Bill will have its first debate at the Second Reading stage and is expected to complete its passage through the House of

Date	Description
	Commons and move to the House of Lords in Autumn 2016. Royal Assent is expected in Spring 2017. **The text of the Bill and explanatory notes are available here.**
Enforcement	
17 February – 6 May 2016	Enforcement for the period includes: 3 monetary penalties, 2 new undertakings (and 1 follow-up review of an existing undertaking), 5 enforcement notices, and 2 prosecutions. Please see the **Enforcement Table** at the end of the Bulletin for more details.
Cases	
19 May 2016	**PJS v News Group Newspapers [2016] UKSC26** On 19 May 2016, the Supreme Court overturned the Court of Appeal's 18 April 2016 decision in the *PJS v News Group Newspapers* case (the so-called *"celebrity threesome"* case), and reinstated the interim reporting injunction pending a trial. The Supreme Court reinforced the principle of privacy by finding that not only is there a blurred boundary between the private sphere and the public sphere, but also between different areas within the public sphere. In particular, the implications on the right to privacy were different as a result of publication on the internet, in print and in the mainstream media. The facts The case concerned the appellant, PJS, a well-known individual in the entertainment industry, and his partner YMA, who is also well-known in this industry. In December 2011, PJS and YMA engaged in a threesome with claimant AB who, in January 2016, approached the *Sun on Sunday* with details of this encounter. PJS was successful in arguing that the publication of this story would constitute both a breach of confidence and an invasion of privacy, and was granted an interim injunction on 22 January 2016. However, the injunction was subsequently flouted on social media and in the United States, where AB took steps to publish the story. This caused various publications in England and Wales to challenge their inability to also publish the story. On 18 April 2016, the Court of Appeal granted an application to dismiss the injunction on the basis that, as PJS's name was now so widely known, it was, in effect, *"pointless"*. The judgment The Supreme Court noted that the Court of Appeal's key error lay in its interpretation, and application, of sections 12(3)

Date	Description
	and (4) of the Human Rights Act 1998: • Section 12(3) provides that a pre-publication injunction should not be granted *"unless the court is satisfied that the applicant is likely to establish that the publication should not be allowed"; and* • Section 12(4) provides that particular consideration should be given to the freedom of expression, the public availability of the information and the public interest in its publication. The Supreme Court held that the Court of Appeal had erred in concluding that section 12 *"enhances the weight which Article 10 rights carry in the balancing exercise"*. In contrast, neither Article 8 nor Article 10 should take precedence, but rather a balance should be struck. The balance was struck by the Supreme Court as follows: while there was no genuine public interest in this story, publication in print and the mainstream media in England and Wales would cause *"significant incremental damage to the applicant's privacy"* and that of his children. Further, damages would not be an adequate, alternative remedy in this case. **The judgment is available here.**
EU	
EU News	
13 April 2016	**Article 29 Working Party: Essential Reading on Essential Guarantees for Transferred European Data** On 13 April 2016, the Article 29 Working Party published a Working Document on data transfers which looked at the impact of surveillance measures on countries wishing to receive personal data from the EU (WP237). The Working Document has been rather eclipsed by the accompanying publication of the Working Party's critical views on the adequacy of the Privacy Shield. However, it is an important document which merits closer reading. First, the Working Party emphasises that data protection authorities can suspend individual data transfers made on the basis of Standard Contractual Clauses, where they conclude that the law of the importing country does not respect EU fundamental rights, which is an implicit warning that the CJEU litigation in *Schrems* and *"Schrems II"* may not be the end of the story. Second, in the light of the Brexit referendum, the Document has added importance for those concerned about data flows to the UK: post-Brexit, will the UK be considered to meet these 'European Essential Guarantees'?

Date	Description
	The Document is the conclusion of work undertaken by the Working Party analysing cases of the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR) which look at surveillance in Member States and in states which are parties to the European Convention on Human Rights. The Working Party concludes that four 'European Essential Guarantees' can be extrapolated from these cases. Actions which fall foul of these European Essential Guarantees will amount to an unjustified interference with fundamental rights. A 3-page Annex lists the cases considered by the Working Party. Perhaps worryingly for those concerned about Brexit, more cases feature the UK than any other Member State. The Annex, however, is not complete. For example, the 2010 ECtHR case of *Kennedy v UK* (which considered the Regulation of Investigatory Powers Act, and which concluded that, in that case, UK practice did not breach Article 8 of the Convention) is not listed in the Annex, although, curiously, it is referred to in the Working Document itself. The fact that the Working Party has chosen to conflate CJEU and ECtHR cases, may, paradoxically, be helpful for the UK. Post-Brexit, the UK will no longer be subject to the CJEU. However, Theresa May has now committed to the UK remaining a signatory to the European Convention of Human Rights: as UK law relating to national security will have to comply with Convention rights, this may make it harder to successfully to argue that the UK rules on communications data fall short of the Working Party's Guarantees. The four European Essential Guarantees are that:

A: Processing should be based on clear, precise and accessible rules	The processing must be in accordance with a precise, clear and publicly accessible law. The legal basis for surveillance should be set out in statute. The law should also set out the types of offences in respect of which interception or surveillance can be used, the categories of people who can be the subject of surveillance, a limit on the duration of the surveillance, the procedures for examining, storing and using the data and the precautions when communicating the data to others. Rules governing access (both the justifications for access and the procedural matters relating to access) should also be set out.
B: Processing must be necessary & proportionate to the (legitimate) objectives pursued	Legislation which authorises storage of all personal data transferred from the EU, without setting out rules appropriate to the objective pursued and without objective criterion to determine access and subject use, is not necessary and proportionate. Mass surveillance must be subjected to very close scrutiny; access should be determined by objective criteria; if an individual is targeted, then this should be on the basis of reasonable suspicion and the individual should be clearly identified.

Date	Description	
		The Working Party acknowledges that the Courts have not yet considered the lawfulness of mass, indiscriminate, data collection and the subsequent use of such data - this may be considered in part in the pending *Tele2/Watson* case and in advice to be given on the validity of the agreement relating to the transfer of Passenger Name Record data to Canada. Legislation allowing access to the content of communications on a 'generalised basis' is not lawful, but the meaning of 'generalised basis' has not been spelled out.
	C: There must be an independent oversight mechanism	Independent oversight is essential. Where surveillance is secret and, as a result, abuse potentially easy, supervisory control by a judge is preferred. Access to stored data should also be dependent on the prior review of a court or independent administrative body, whose decisions seek to limit access. The Working Party notes that while a judge is preferred, other bodies or persons could be responsible as long as they are sufficiently independent, and the qualification of the person is also relevant (for example, the fact that an appointee is qualified to hold judicial office, rather than being a member of the executive). The degree to which the supervisory authority's activities are open to public scrutiny is also relevant. On independence, the Working Party references cases assessing the independence of data protection authorities themselves, which note that functional independence by itself may not be sufficient and that reviewers should not be directed or subjected to external influence.
	D: There should be effective remedies for the individual	ECtHR case law suggests that an effective remedy also involves the individual being notified once surveillance is over. If this is not done, then there can still be an effective remedy if complaints are considered in a court, which is independent and impartial, with its own rules of procedure, and consisting of members who hold, or have held high judicial office or are experienced lawyers. The court should also have access to all relevant information (including closed materials) and have powers to remedy non-compliance.

The Working Party does note that the cases analysed recognise that Member States have a right to introduce legislation to maintain national security and to collect data for intelligence purposes. It also notes that the Member States have a 'fairly wide margin of appreciation' in achieving this aim, for example, including secret surveillance measures, as long as suitable guarantees are in place.

Date	Description
	As the Working Party itself acknowledges, it can be difficult to extrapolate general principles from particular cases which are very specific to their facts. Some cases relate to wire-tapping and, indeed, is it right that principles stated in the context of interception should be applied, as-is, to collection and later access to communications data? Some of the cases cited by the Working Party also do not exactly relate to national security and law enforcement access at all. For example, *Halford v UK* is included, which readers will remember related to interception of calls on a private network by the police - not for national security purposes but to check on legal advice being given to Ms Halford in relation to her discrimination claims against the police force. Working Party Opinions are influential but should not be treated in the same way as case law. As statements by the authorities tasked with enforcing data protection law and promoting good practice, they reflect the policy objectives of those authorities. However, Working Party Opinions should always be read with care, which is particularly true of this paper, and the Working Party itself draws attention to this by adopting this as a more provisional Working Document, rather than an Opinion. Not only are the Working Party's Essential Guarantees somewhat imprecise and tentative, their data protection impact is also unclear. The Working Party notes that its 'Essential Guarantees' test is a different test to that required for an adequacy decision. In this case, the CJEU set out a test of 'essential equivalence'. However, as all processing of personal data (including data transfers) must comply with the requirements of the EU Charter and European Convention of Human Rights, the Working Party suggests that data transfers should also be assessed against these European Essential Guarantees. The Working Party also reiterates that the Standard Contractual Clauses allow (in fact, oblige) data protection authorities to determine if the law applicable to the data importer goes 'beyond the restrictions necessary in a democratic society'. In other words, even if the Working Party is wrong in its suggestion that these Essential Guarantees should be relevant in adequacy decisions, these Guarantees are still what the Working Party will turn to in considering individual complaints about data transfers under the Standard Contractual Clauses. **The full Working Document is available here.**

Date	Description
30 May 2016	**European Data Protection Supervisor Issues Opinion on Privacy Shield** The European Data Protection Supervisor (EDPS) Opinion is the latest in a series of European criticisms of the Privacy Shield. EDPS reiterates many of the comments made by the Article 29 Working Party. As EDPS participated in the Working Party Opinion, this comes as no surprise. The EDPS Opinion purports to offer 'pragmatic' advice - noting both that a transatlantic data transfer method is essential and that the method must be robust enough to survive future court challenge. The 'pragmatic' advice is designed to help move debate forward so as to achieve both of these goals. Some of the EDPS' 'asks' repeat those of the Working Party, for example, redrafting the Principles so as to address retention restrictions and rules on automated decision taking. However, EDPS also offers new approaches, such as suggesting that the arrangements for transfers of financial transaction data could be used as a model for involvement of EU supervisory authorities in oversight mechanisms. The Opinion also makes wider ranging comments about Privacy Shield. For example, EDPS notes that commitments should be given by legislation, not letters from officials, and suggests restrictions on surveillance so that it is subject to supervision by data protection authorities and may only take place when it can be demonstrated as indispensable to achieving the particular objective. With ongoing legislative debate on the Investigatory Powers Bill in the UK and other EU Member States looking at similar initiatives, this is a further example of the double standards at work: the EU suggesting that the US agree to restrictions, which the EU does not itself consistently respect. No pragmatic suggestion is offered in relation to these comments, leaving their status unclear: are they aspiration or requirement? Given the ongoing uncertainty over the practical application of the Privacy Shield (please see below for more information) and the referral to the European Court which has recently been made in relation to Standard Contractual Clauses, it seems that individual consent may be the way of addressing transatlantic data flows which will have most longevity. Consent also continues to be recognised under the GDPR, although the requirements for valid consent are increased. This approach of course provides fewer safeguards for individuals: there is a real risk that the only outcome of protracted dialogue, court challenge and uncertainty is lower protection for transferred data, with transfers based on consent. **The full opinion can be found here.**

Date	Description
2 June 2016	**EU – U.S. "Umbrella" Agreement Signed** On 2 June 2016, the EU and the US signed the 'Umbrella Agreement' (the 'Agreement'), establishing a high-level data protection framework for criminal law enforcement cooperation. The Agreement covers all personal data exchanged between police and criminal justice authorities of the EU Member States and the US federal authorities for the purpose of prevention, investigation, detection and prosecution of criminal offences, including terrorism. The Agreement is designed to facilitate co-operation between law enforcement agencies, and also to guarantee the legality of data transfers. The safeguards set out in the Agreement include clear limits on data use and the requirement that agencies seek consent before data is transferred. The Agreement will only apply to Denmark, the UK or Ireland if the European Commission notifies the US in writing that those jurisdictions have decided that the Agreement applies to them. It is not in itself a legal instrument for any transfer of personal information to the US but it supplements, where necessary, data protection safeguards in existing and future data transfer agreements or national provisions authorising such transfers. The European Commission made the Agreement conditional on the passage of the Judicial Redress Act ('JRA') through the American Congress, which will give EU citizens the right to challenge how their data are used in US courts. The JRA was passed in February 2016. Examples of the key principles are listed below, many of which are broadly similar (albeit some more qualified) than those found in other EU data protection laws: • Purpose and Use Limitation: the transfer shall be for the prevention, detection, and investigation of criminal offences including terrorism. The further processing of the data cannot be incompatible with that purpose and thus will include processing pursuant to the terms of international agreements, and international frameworks for the prevention, detection or prosecution of similar crimes. In addition, the EU and US shall provide, in their applicable legal frameworks, specific retention periods for records containing personal information. • Onward Transfer: where a competent authority of either the EU or US transfers personal data relating to a specific case to a competent authority of the other party, that information may be transferred on to a state not bound by the agreement only with the prior consent of the original competent authority responsible for sending the information. Where that information doesn't relate to a specific case, the onward transfer of personal information may only take place in accordance with specific conditions set forward in the Agreement. • Notice: a competent authority shall provide notice to an individual to outline the nature and purposes of the data

Date	Description
	processing: the notice may be through publication of general notices or actual notices. • Maintaining Quality and Integrity of the Information: the US and EU are to take reasonable steps to ensure that personal information is maintained with such accuracy, relevance, timeliness and completeness necessary and appropriate for the lawful processing of the information; • Sensitive Data: this data will only be processed under appropriate safeguards in accordance with law, including by way of example, the restriction of the purposes for which the data is to be processed, masking or deleting the data after effecting the purpose for which it was processed, and/or restricting access to certain individuals, etc. • Information Security: the EU and US shall ensure they put in place appropriate technical, security and organisational arrangements for the protection of personal information against accidental or unlawful destruction, accidental loss, and unauthorised disclosure, alteration, access, and other processing. • Breach Notification: upon discovery of a breach of personal data in which there is a significant risk of damage, the receiving competent authority shall assess the likelihood and scale of damage and take actions to mitigate such damage. Action to mitigate damage includes notification to the transferring competent authority, and where appropriate, the affected individual. However, there are qualifications such that notification and mitigation does not have to be carried out under certain circumstances (for example, where it may endanger national security or official inquiries, investigations or prosecution of criminal offences). • Access: the parties shall ensure that any individual is entitled to seek access to his or her personal information and, subject to any restrictions, obtain it (and under certain circumstances correct or rectify it). Such access shall be sought and obtained from a competent authority in accordance with the applicable legal framework of the State in which relief is sought. However, access will be subject to reasonable restrictions permitted under domestic law, including by way of example, safeguarding the rights and freedoms of others, safeguarding national security, avoiding the obstruction of official inquiries, etc. • Accountability: the EU and US are to have in place measures to promote accountability for processing personal information within the scope of the Agreement by their competent authorities, and any other of their authorities to which personal data has been transferred. Serious misconduct is to be addressed through appropriate and dissuasive criminal, civil or administrative sanctions. • Judicial Redress: any citizen of either the US or EU is entitled to seek judicial review with regard to denial of access to records containing personal information, denial of amendment of personal records, and unlawful

Date	Description
	disclosure of such information that has been willfully or intentionally made. The Agreement will enter into force on the first day of the month following the date on which the EU and US exchange notifications indicating that their internal preparatory procedures have been completed. **See the European Commission's press release here and the full text of the Agreement here.**
8 June 2016	**Article 29 Working Party: Public Bodies and the Management of Conflicts of Interest and Anti-Corruption Measures** On 8 June 2016, the Article 29 Working Party published an Opinion on the publication of Personal Data for Transparency purposes in the Public Sector (WP239). The Opinion is limited to the specific issues arising out of the publication of data linked to anti-corruption measures and conflict of interest measures. It does not tackle wider issues about balancing freedom of information policies and data protection. The Working Party acknowledges that publication of data about staff can be an appropriate part of anti-corruption/ conflict of interest measures, and that this serves a legitimate purpose. Publication of such data could be justified either as being necessary for compliance with a legal obligation or as being necessary for an activity carried out in the public interest, or in the exercise of official authority. Predictably, the Working Party emphasises that such measures must be proportionate and respect data minimisation principles. The Working Party gives the example that it may be appropriate to collect data about the assets of a public official and of his or her family members, and how these were funded. However, it may not necessarily be proportionate to publish this information. Publication of sensitive personal data will rarely be justified. Factors such as the individual's power and seniority, spending authority, salary and term in office should all be considered in assessing proportionality. The Working Party suggests that the balance should be set out in relevant legal provisions. Different rules may be necessary for different groups of officials, with the most senior subject to the most scrutiny. Where routine or extensive publication of information is envisaged, then the Working Party recommends carrying out a Privacy Impact Assessment. **The full report is available here.**

Date	Description
July 2016	**EU should preserve and not reduce ePrivacy rules say the Article 29 Working Party and the EDPS in separate, but consistent, preliminary opinions on the review of the ePrivacy Directive** On 19 and 22 July 2016, the Article 29 Working Party and the EDPS provided Opinions on the review of amended Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive). Both the Working Party and EDPS support the European Commission's proposal to "modernise, update and strengthen" the provisions of the ePrivacy Directive. • Opposition to industry suggestions that the ePrivacy regime is no longer needed: both Opinions take the contrary view the high standards in the ePrivacy Directive should be maintained: there remains an ongoing need to have specific rules to "protect the confidentiality and security of electronic communications", and to "complement and particularise the requirements of the GDPR" as it applies to these communications. • 'Functionally equivalent' means of communication and private messaging should be covered: the ePrivacy Directive was drafted with traditional forms of communication (fixed, mobile, Internet, email) in mind. It recognised that such service providers had a privileged position allowing them to monitor individuals' communications in real time and to draw up detailed profiles about them. However, services have developed. VoIP services, or chat functions within other information services are not clearly covered by the ePrivacy Directive, but pose the same risks. Further, individuals see all such services as "functionally equivalent". Individuals must therefore be covered by the same level of protection, regardless of their chosen means of communication. This should be the case whenever the service provider takes the position of a neutral carrier. • Wi-Fi hot spots to be subject to confidentiality requirements: the confidentiality of users' communications on publicly accessible private networks (e.g. Wi-Fi in airports, corporate Wi-Fi access offered to visitors and guests, public hotspots, etc.) should be protected. The Working Party Opinion notes that it had previously advocated against treating publicly accessible private networks in the same way as public networks as it did not wish to subject more providers to mandatory communications data retention regimes. However, with the invalidation of the Data Retention Directive (2006/24/EC), this concern has been removed, meaning that the Working Party is able to give greater emphasis to the obligations owed by such providers. The Working Party suggests that the new instrument contains a commitment by the EU that it will never re-introduce data retention at a pan-European level. • Consent requirement for traffic and location to be preserved, strengthened and broadened: the concepts of traffic and location data should be merged and there should be a general requirement for consent for use of 'metadata' (it is

Date	Description
	unclear what this would encompass). Any use of such data (i.e. not just by public electronic service providers) should require consent. Existing exemptions for processing which is strictly necessary to deliver the requested service and for security purposes should be maintained. Other exemptions could be introduced for low privacy-intrusive types of processing, subject to rules around data minimisation and anonymisation. • Interception and communications secrecy to be strengthened and updated: the new text should make clear that communications need not be one-to-one to be protected by secrecy laws. A conference call or message sent to a defined group of recipients should also attract protection. The Working Party even makes the (mathematically ludicrous) suggestion that protection should be offered to any communication with a finite number of parties. • The long-standing distinction between content and traffic should be reviewed: the EDPS notes the evidence that traffic data can be as revealing as content. Both note that clear distinctions between traffic and content make sense in the world of voice calls, but breakdown online where a destination URL could be both a party to a communication (so traffic data) and content at the same time. Both suggest rethinking on this point, with detailed examples of what should be viewed as traffic data and what as content. • Both advocate a broad interpretation of interception: so that technical matters such as injecting an identification code into a communication (i.e. an advertising ID) should count as interception. • Complete or partial ban on 'cookie walls': the requirement for consent in Article 5(3) (the cookie consent rules) should be "maintained and strengthened". Consent must be "freely given" as per the GDPR, and legislators should contemplate a complete or partial ban on so-called "cookie walls" (i.e. in situations in which a user who does not accept cookies is denied access to a website). Both recommend adding a non-exhaustive list of examples where such walls would not be permitted (e.g. where the provider of the service is in a dominant position or government funded; where a website or app auctions its advertising space and unknown third parties may track and monitor users through the website or app; for sites which could lead to inferences about sensitive data; or in other cases where GDPR suggests that consent will not be freely given (e.g. where there is imbalance of bargaining power). Both Opinions follow the lead of the GDPR to state that consent must be 'granular' – bundled consent will not be valid and elements of processing which are separate should have separate consents. News media are singled out by the Working Party for criticism in this regard. The Working Party acknowledges that their economic survival is important, but that 'invasive tracking' is not the way to achieve this. • Cookie control tools with privacy-friendly default settings: the onus for cookie compliance should not only fall on publishers. Both propose the involvement of browser and application manufacturers so that they can offer cookie

Date	Description
	control tools such as Do Not Track (or equivalent). Such tools must be offered with privacy-friendly default settings and be actively configured by the user. The EDPS also states that users' rights to install ad-blockers should be protected. • First-party analytic cookie exemption: the revised ePrivacy rules should confirm the scope of the current first-party analytic cookie exemption developed by the Working Party in its Opinion 04/2012. Such an exception should "be limited to cases where the use of such first party analytics cookies is strictly limited to aggregated statistical purposes". The data should also be irreversibly anonymised (no separate ability for a service provider to access; hashing or encryption is not enough); any service provider must act as a data processor; analysis must be limited to a single area (so no cross-device or cross-website analytics); there must be an easy opt-out and no collection of sensitive data. • Extended protection from other forms of tracking: cookie provisions should not be limited to cookies. Device fingerprinting is on the radar of the EDPS, whilst the Working Party talks about the need to extend similar protections to MAC addresses which are collected to track users. • Both talk about the need to extend security for a communication to security for the device: so software pre-loads and pushed information should not be allowed. Rather than forcing an update, the user should be notified and allowed to complete the installation himself. The EDPS calls for additional security measures (e.g. security standards) for actors such as networks, providers of network components, IoT devices, etc. • End-to-end encryption (without "back-doors"): for the EDPS, this should be permitted and encouraged to allow users to safeguard their communications. Conversely, "decryption, reverse engineering or the monitoring of communications protected by encryption should be prohibited". The Working Party suggests the new instrument should include a right for users to encrypt their communications. • No more specific mandatory breach regime for telcos/ISP: this industry specific regime provided by the current ePrivacy Directive should be deleted and replaced with the general breach notification regime provided under the GDPR, with reports of breaches going to data protection authorities. • Harmonisation between competent regulators (e.g. DPA vs. telco regulator) (with bigger role for DPAs): at the moment, some elements of enforcement in some countries fall to the data protection authority, and some to telecoms authorities or others. The EDPS suggests that where a national data protection authority can efficiently perform a task, the same national data protection authority should be considered to be the competent authority for ePrivacy matters. Unsurprisingly, the Working Party also suggests that its members should be the enforcement agent for ePrivacy matters. • Unsolicited communications big bang: consent should be required from recipients before they receive any type of

Date	Description
	unsolicited commercial communication, regardless of (i) the "means" (e.g. email, voice calls, texts, but also direct-messaging, i.e. within an information society service) and (ii) behavioural advertisement. The EDPS also suggests that the level of protection should be the same irrespective of whether in the context of B2C or B2B operations (this is less clear in the Working Party Opinion, which does mention harmonisation of rules on B2C and B2B but not in the section on direct marketing). In addition, the concepts of "existing relationship" and "similar products and services" with regards to soft opt-in considerations and "commercial communications" should be clarified. The Working Party notes that the burden of proof for consent should be with the person commissioning the communication, who should be required to keep time-stamped evidence of consent, together with a record of what was shown to the user to obtain consent. Consent should also be easy to revoke and there should be a mechanism for users to revoke consent across an industry or a sector. • Directories of subscribers: the right for subscribers to object to the publication of their details in public (printed or electronic) directories should be maintained and expanded so that it applies to all kinds of directory services. In addition, this right should apply to other details such as e-mail addresses or user names used in the context of 'reverse lookup' functionalities. • Calling Line Identification: this should also be maintained – and the Working Party suggests possible strengthening, such as inclusion of rules preventing CLI spoofing. **The EDPS Opinion is longer – what else does it cover?** • Territorial scope and applicable law: to avoid any confusion, the new ePrivacy rules should "have unambiguously the same territorial scope compared with the GDPR", subject to some technical adjustments. • Duty for organisations to issue government access reports: the EDPS calls for an obligation borne by organisations to disclose, at least periodically and in aggregate form, law enforcement and other government requests for information. • Two legal grounds for the revised ePrivacy regime: the EDPS proposes that the European Commission "consider a dual legal basis for the new legal instrument for ePrivacy". This, it suggests, should be both Article 16 of the Treaty on the Functioning of the European Union (TFEU) (the legal basis of the GDPR), and Article 114 TFEU on approximation of laws (the legal basis of the ePrivacy Directive). According to the EDPS, a single basis (Article 16) would not suffice, as "the new provisions will not only 'particularise' some provisions of the GDPR, but will also 'complement' it with provisions that are not limited to the protection of personal data". • Goodbye directive, hello regulation: for the revised ePrivacy rules, the EDPS recommends using a regulation instead

Date	Description
	of a directive. This suggestion is made on the basis that such an approach would, for instance, be more consistent with the GDPR. In the meantime, the EDPS recognises that Member States should be left with room for manoeuvre (without indicating for which topics). However, for the EDPS, the ability of Member States to deviate should be kept to the minimum necessary. The Working Party states that it does not mind which instrument is used, as long as variation is minimised. • Framework Directive clarification needed: the EDPS also suggests that the European Commission should clarify how it intends to re-structure the relationship between the revised ePrivacy regime and the Framework Directive (2002/21/EC) dealing with electronic communications. **The EDPS opinion can be found here.** **The Article 29 Working Party opinion can be found here.**
12 July 2016	**European Commission Formally Adopts Privacy Shield** • On 12 July 2016, the EC formally adopted a decision confirming the adequacy of Safe Harbor's replacement - the EU-U.S. Privacy Shield. The revised draft addresses many of the concerns raised by the Working Party who, on 14 April 2016, whilst stating that the Privacy Shield was an 'improvement' from Safe Harbor, concluded that it did not meet EU standards. • US organisations may self-certify to the standards set out in the Privacy Shield from 1 August 2016. • In order to adopt the Privacy Shield, an organisation must be subject to the investigatory and enforcement powers of the FTC, the US Department of Transport or another statutory body agreed to by the EC. These bodies will oversee compliance with the Privacy Shield principles. So, as was the case for Safe Harbor, US businesses operating in certain sectors (such as financial services and telecommunications) are not currently eligible to participate. • To self-certify for the Privacy Shield, an organisation must, among other things, file a submission signed by a corporate officer confirming compliance with the Shield's principles. A full and publicly available privacy policy must also be published, as must contact details for the handling of complaints and subject access requests, and details of the independent recourse mechanism that is available to investigate unresolved complaints. • We expect that further information on how to self-certify to the Privacy Shield will be provided on the US Department of Commerce's website in the coming weeks • Microsfot and Salesforce among the first certified companies.. **The European Commission press release can be found here.**

Date	Description

26 July 2016	**Article 29 Working Party Issues Statement on Privacy Shield**
	
	• On 26 July 2016, the Working Party issued a Statement on the revised Privacy Shield.
	• It stated that a number of its original concerns remained regarding both the commercial aspects and the access by U.S. public authorities to data transferred from the EU:
	  ○ Commercial aspects: the Working Party *"regrets the lack of specific rules on automated decisions and of a general right to object. It also remains unclear how the Privacy Shield Principles apply to processors."*
	  ○ Access by public authorities to data transferred to the U.S. under the Privacy Shield: the Working Party *"expects stricter guarantees concerning the independence and the powers of the Ombudsperson mechanism. Regarding bulk collection of personal data, the Working Party notes the commitment of the ODNI [(Office of the Director of National Intelligence)] not to conduct mass and indiscriminate collection of personal data. However, it regrets the lack of concrete assurances that such practice does not take place."*
	• Isabelle Falque-Pierrotin, the Chair of the Article 29 Working Party, has confirmed that EU data protection authorities would not challenge the adequacy of the Privacy Shield for at least one year. Therefore, no challenge is imminent.
	
	The Article 29 Working Party Statement can be found here.

Cases	
12 May 2016	***Patrick Breyer v. Federal Republic of Germany* (C-582/14)** In May, the Advocate General delivered his Opinion in this case, concluding that dynamic IP addresses qualify as personal data insofar as additional information held by the internet provider allows for identification of the visitor. To read Bird & Bird's full article on the website, please click here.
28 July 2016	***Verein für Konsumenteninformation v Amazon EU Sàrl* (C-191/15)** Background This case concerns an action brought by the Austrian Consumer Information Association, *Verein für Konsumenteninformation* (VKI), against Amazon EU Sàrl (Amazon), a company established in Luxembourg but which, among other things, offers goods and services to consumers resident in Austria through a website with the domain name extension *'.de'*. VKI brought an action against Amazon for an injunction to prohibit the use of all terms contained in Amazon's general terms and conditions with such Austrian consumers on the basis that it thought those terms were unfair. One such term stated that the applicable law was that of Luxembourg.

Date	Description
	Judgment The Austrian Supreme Court referred three questions to the CJEU. One concerned the applicable law for data protection purposes, and the others were on how the Rome I and II Regulations should be interpreted to determine the applicable law relating to contractual and non-contractual matters. The data protection question was whether a company, established in one country (Luxembourg), but directing its activities to another country (Austria) must comply exclusively with the data protection law of the Member State in which it is established or must also comply with the data protection rules of the Member State to which its commercial activities are directed. The CJEU decision referenced *Weltimmo (C-230/14, EU:C:2015:639)*, noting that the definition of *'establishment'* extends to *"any real and effective activity, even a minimal one, exercised through stable arrangement"*. The Court approvingly referenced the Advocate General's (AG) Opinion, that the lack of a branch or subsidiary in a Member State does not preclude establishment in that Member State. However, the Court concluded that mere accessibility of the undertaking's website from a Member State would not be sufficient as to amount to establishment. In this case, Amazon had no activities in Austria, and mere accessibility of its services in Austria did not make it established in Austria for data protection purposes. As regards the definition of *'in the context of'*, the CJEU referenced its previous observation in *Weltimmo* that, *"[Article 4(1)(a)] requires the processing of personal data in question to be carried out not 'by' the establishment concerned itself but only 'in the context of the activities' of the establishment"*. The CJEU noted that the answer to this question was to be determined by national courts. It did not provide an answer itself, although it did, in passing, note that if there was an Amazon German establishment, that the national referring court could conclude that German was the applicable law rather than that of Luxembourg. In relation to the remaining questions, the CJEU emphasised the need to distinguish between: 1. The law applicable to the action for the injunction, on the basis that earlier case law established that injunctions for unfair contract terms concerned were to be considered non-contractual, this must be determined in accordance with Article 6 (1) Rome II Regulation; and 2. The law applicable to the assessment of the particular contractual term, which must be determined in accordance with the Rome I Regulation. **The 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)**
26 May 2016	**Mark Lloyd**	Prosecution	Mark Lloyd, an employee of a waste management company in Shropshire, emailed the details of 957 clients to his personal email address as he was leaving to start a new job at a rival company. The documents contained customer contact details, their purchase histories, and other "commercially sensitive" information. He was prosecuted for the offence of "unlawfully obtaining data".	£300 fine, £405.98 costs, £30 victim surcharge
26 May 2016	**Leeds Community Healthcare NHS Trust**	Undertaking follow-up	This action concerned an ICO "follow-up" assessment of the actions taken by the Leeds Community Healthcare NHS Trust (the Trust) in relation to an undertaking it signed on 13 November 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented. The review demonstrated that the Trust had taken appropriate steps and put plans in place to address some of the requirements of the undertaking. However, the Trust will need to complete further work to fully address the agreed actions. In particular, the Trust confirmed that it had taken the following steps: • all staff, students and agency workers are now required to complete the HSCIC training; • information has been circulated to staff	The Trust should take further action as follows: • review and update SAR policies and procedures; • provide specific role-based training annually to staff involved in handling SARs; • review and update IG policies and procedures; and • provide specific role-based data protection training for all staff involved in handling personal data.

			regarding the requirement to complete information governance (IG) training every 12 months; • the induction training checklist has been updated to ensure that new starters complete IG training on the first day of their employment by the Trust; • standard operating procedures, detailing the Trust's management of IG training compliance, have been produced; • training records for IG training compliance are maintained by the Trust; • notifications are sent to staff line managers informing them about employees that are due to complete refresher training in the upcoming months; and • the Trust has carried out a workshop for staff.	
6 June 2016	**Wolverhampton City Council**	Undertaking	Wolverhampton City Council (the Council) has signed an undertaking committing the Council to ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I Schedule 1 to the Act. This action follows two separate incidents. The most recent incident occurred on 5 January 2016, when the personal information of employees at 73 educational institutions was sent in error to an external recipient via email. A second, previous incident occurred on 26 November 2015, when the data controller 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 data controller shall ensure that personal data are processed in accordance with the First Data Protection Principle in Part I of Schedule 1 to the Act, and in particular: • the data controller shall devise and implement a system to ensure that completion of data protection training is monitored and that procedures are in place to ensure that staff who have not completed training within the specified time period do so promptly. This should be completed within three months; and • the data controller shall ensure that all staff handling personal data receive data protection training

			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.	and that this training is refreshed at regular intervals, not exceeding two years. The data controller should ensure that all staff that handle sensitive personal data regularly, receive refresher training within six months of the date of the undertaking.
7 June 2016	**Money Saving Champions Limited**	Prosecution	Money Saving Champions Limited was prosecuted as a result of its failure to notify under section 17 of the DPA, having processed data without having an entry in the data protection register.	£350 fine, £497.75 costs
8 June 2016	**Debbie Urch t/a Kings Ransom**	Enforcement notice	Debbie Urch (trading as Kings Ransom) was ordered by the ICO to respond to a subject access request (SAR), following its failure to respond to the same SAR made by a complainant on 17 September 2015.	Debbie Urch shall inform the complainant whether the personal data processed by the data controller includes personal data of which the complainant is the data subject and shall supply him with such details in accordance with the requirements of section 7 DPA and the Sixth Data Protection Principle.
8 June 2016	**Chief Constable of Dyfed-Powys Police**	Monetary penalty	On 18 June 2015, an officer from Dyfed-Powys Police force sent an email with a chain dating back to 4 February 2015 containing information relating to eight registered sex offenders, to five internal recipients. The officer also sent the same email to a member of a community scheme in error, as her external address was the first in a global address book, which was only supposed to be for internal emails. Between 14 and 18 April, the same community scheme member received five emails from various police officers containing personal data. She telephoned the force and emailed the recipients to alert them to the problem.	Monetary penalty notice of £150,000.

8 June 2016	**Central Compensation Office Limited**	Enforcement notice	Between 6 April 2015 and 31 August 2015, the ICO received 23 complaints and the TPS 167 complaints about unsolicited direct marketing calls made by Central Compensation Office Limited (the Company) trading under various names.	The Company shall, within 35 days of the Notice: • 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 called line is that of: (a) a subscriber who has previously notified the Company that such calls should not be made on that line; and/or (b) a subscriber who has registered their number with the TPS at least 28 days previously and who has not notified the Company that they do not object to such calls being made.
9 June 2016	**Quigley & Carter Limited**	Monetary penalty	Quigley & Carter Limited (the Company) is a claims management company offering services in respect of mis-sold packaged bank accounts via its website www.mybankrefund.com. It is authorised by the Claims Management Regulator. Between 6 April 2015 and 9 June 2015, 2620 complaints were made to the 7726 service about the receipt of unsolicited direct marketing text messages sent by the Company. In the same period, 69 complaints were made direct to the ICO.	Monetary penalty notice of £80,000.
9 June 2016	**Advanced VOIP Solutions Ltd**	Monetary penalty	Advanced VOIP Solutions Ltd (the Company) provides telephony services including 'voice broadcasting' to help companies such as Money Help Marketing Ltd (MHML) to maximise its potential sales. MHML is a lead generating	Monetary penalty notice of £180,000.

			company. Between January and October 2015, the ICO received 6,381 complaints via the online reporting tool (3,375 after 6 April). The gist of the complaints was that repeated automated marketing calls had been received by subscribers without their prior consent. The CLI's were prefixed with the number 0843 724. If the subscriber re-dialled the 0843 724 number, they were connected to yet another recorded message identifying MHML as the company that had sent the automated marketing call. On further investigation, it was discovered that a telecom provider had allocated the calling line identities (CLIs) to the Company, which acted as a reseller to MHML, the subscriber of the CLIs. The CLI ranges being used for the automated calls were 'added value' numbers, that is, they are non-geographical and charged at the standard network rate plus 4.1667p per minute. The subscribers were charged at this rate if they re-dialled the 0843 724 number.	
29 June 2016	**Cheshire West and Chester Council**	Enforcement notice	The complainant requested dates relating to a specific building control application which were previously available online, but later removed by Cheshire West and Cheshire Council (the "Council"), which thereafter decided to charge members of the public £59 for access to such information. In doing so, the Commissioner considered that Chester West and Chester Council breached regulation 4 of the Environmental Information Regulations 2004.	The Commissioner requires the public authority to take the following step to ensure compliance with the legislation: • reinstate web access to the building control dates that were on the Council's website prior to the request. The Council must take this step within 35 calendar days of the date of the enforcement notice.

8 July 2016	**Change and Save Ltd**	Enforcement notice	Change and Save Ltd (the "Company") is a company that falsely claimed it was phoning people as part of a lifestyle survey – a practice known as "sugging". Between 1 June 2014 and 31 December 2015, 254 complaints were made about unsolicited direct marketing calls made by the Company. 38 complaints were made direct to the ICO, and 216 to the TPS. All of these complaints were made by individual subscribers who had registered with the TPS.	The Commissioner requires that the Company shall, within 35 days of the date of the notice: • 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 called line is that of: (a) a subscriber who has previously notified the Company that such calls should not be made on that line; and/or (b) a subscriber who has registered their number with the TPS at least 28 days previously and who has not notified the Company that they do not object to such calls being made.
19 July 2016	**Northern Health & Social Care Trust**	Undertaking	Northern Health & Social Care Trust (the "Trust") has signed an undertaking committing the Trust to ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I Schedule 1 to the Act. This action follows repeated incidents where 11 emails intended for a doctor's personal non-trust email account, some of which contained personal data and on one occasion sensitive personal data, were sent to a member of the public with the same name over a two year period. Following an investigation, it was discovered that none of the emails were securely protected in line with policy. Although the recipient advised the	The data controller shall ensure that personal data are processed in accordance with the seventh Data Protection Principle in Part I of schedule 1 to the Act, and in particular that: • The data controller must ensure that all staff, including locum doctors, 3rd party contractors, temporary (agency/bank staff) and volunteers, whose roles involve the routine processing of personal and sensitive personal data, undertake mandatory data protection and data handling induction training

			sender that the emails had been sent to the wrong address, the matter was not escalated as an information governance incident. The data controller only became aware of the problem when the recipient's wife contacted the information governance team directly.	and regular refresher training on the requirements of the Act. • Provision of such training shall be recorded and monitored with oversight provided at a senior level against agreed Key Performance Indicators to ensure completion. • The data controller shall ensure that staff, including locum doctors, 3rd party contractors, temporary (agency/bank staff) and volunteers are aware of the content and location of its policies and procedures relating to the processing of personal data. • The data controller shall implement such other security measures as are appropriate.
19 July 2016	**Consumer Finance Claims Ltd**	Enforcement notice	Consumer Finance Claims Ltd (the Company) was ordered by the ICO to respond to a subject access request (SAR), following its failure to respond to the same SAR made by a complainant on 29 June 2015.	The Company shall inform the complainant whether the personal data processed by the data controller includes personal data of which the complainant is the data subject and shall supply him with such details in accordance with the requirements of section 7 DPA and the Sixth Data Protection Principle.