Date	Description
UK	
Information Commissioner's Office (ICO)	
30 July 2015	**ICO updates guidance on crime prevention** On 30 July 2015, the ICO published updated guidance on the crime and taxation exemption provided for by section 29 of the Data Protection Act 1998 ("DPA") which, despite being the most commonly used exemption, is also one of the most uncertain in its application. The updated guidance will be of assistance to organisations that process personal data in connection with the detection and prevention of crime, the apprehension or prosecution of offenders and the assessment and collection of taxes. While the guidance will be of particular relevance to policing and prosecuting authorities it will also be of relevance to any organisation processing personal data for relevant purposes. The guidance outlines the way in which the exemption applies both to permit disclosures that are necessary for the purpose of detecting or preventing crime, and to limit data subject access rights where complying with these rights will prejudice the prevention or detection of crime. The guidance reminds data controllers of the importance of adopting a case by case approach when applying the section 29 exemptions; it is not the case that all personal data processed for the detection or prevention of crime are exempt from the DPA. It explains that the section 29 exemptions can be relied on only where complying with usual requirements in relation to non disclosure and subject access would be likely to prejudice relevant protected purposes. Accordingly, data controllers seeking to rely on the exemption should be able to demonstrate the nature of the prejudice likely to arise as a result of the application of usual rules, for example in relation to subject access and third party disclosure. Any such prejudice must be "real, actual and of substance" and there should be a clear nexus between the application of usual data protection rules and the likely prejudicial effect. Data controllers are reminded that case law imposes a high threshold for the application of the section 29 exemptions in that they should be applied only to the extent necessary in order to safeguard relevant purposes.
6 August 2015	**The ICO fines the Money Shop £180,000** On 6 August 2015, The Money Shop was served with a monetary penalty notice imposing a £180,000 fine following the loss of two servers containing personal data relating to customers and employees. One server was stolen from a branch in Northern Ireland, while the second was lost in a separate incident after being couriered to Swindon. The ICO found that the company had failed to take appropriate measures to transport and store the server; these measures

Date	Description
	would have included the use of locked rooms in branches and a policy of encryption to prevent unlawful access to personal data while servers were being transported around the UK. These failures amounted to a breach of the seventh data protection principle which requires appropriate technical and organisational measures to be taken by data controllers to prevent accidental loss and to prevent the unlawful processing of personal data in the event of accidental loss.
20 August 2015	**Google ordered to delist news links by ICO** On 20 August 2015 the ICO issued its first enforcement notice in relation to the so called 'right to be forgotten '. The case concerns a report of minor historic offences which Google had initially delisted at the request of the complainant following the procedure implemented by Google in the wake of the CJEU's judgment in the Case C - 131/12 Google Spain SL & Google Inc. v Agencia Espanola De Proteccion De Datos Mario Costeja Gonzalez ([2014] 1 QBD 1022). Google's initial delisting decision was followed by an online article regarding the removal of the link. This in turn resulted in re-reporting of the original story about the complainant's conviction. The complainant's request for the removal of links to these websites generated by searches made using his name as a search term was rejected by Google on the basis that the search results were now relevant to topical reporting regarding implementation of the Costejas judgment and the availability of the search results was in the public interest given the newsworthiness of current debate regarding the 'right to be forgotten'. The ICO determined however that the processing of the complainant's personal data in this way by Google Inc (which, following Costejas, the ICO considers to be the data controller in respect of personal data processed in the context of commercial and advertising activity conducted in the UK by Google UK Ltd) breaches the first and third data protection principles. In reaching this conclusion, the ICO considered it relevant that the complainant was not a public figure, the data included sensitive personal data, the convictions concerned were relatively minor and were historic and the existence of the links complained of had a disproportionately negative impact on the complainant's privacy. Furthermore the ICO considered that the availability of the web links objected to by the complainant was likely to cause the complainant distress. The enforcement notice accordingly required Google Inc. to remove links to specified websites from the list of results displayed following a search based on the complainant's name in the case of any search carried out by Google Search in the context of the activities of Google UK Ltd or any other Google company established in the UK. The notice, which is being appealed by Google, falls short of ordering delisting in respect of other Google domains, for example Google.com.
26 August 2015	**Information Commissioner v Colensso-Dune: Upper Tribunal rejects Information Commissioner's appeal against disclosure**

Date	Description
	The Information Commissioner has recently lost its appeal against an order of the First-tier Tribunal requiring the disclosure under the Freedom of Information Act (FOIA) of a list of 305 journalists seized at the home of private investigator Steve Whittamore following an ICO raid in 2003 in connection with Operation Motorman. The judgment of the Upper Tribunal throws interesting light on the proper approach to the disclosure of personal data requested under FOIA and in particular on the definition of sensitive personal data. Mr Whittamore was prosecuted for offences contrary to section 55 DPA (obtaining and disclosing personal data without the consent of the data controller) and received a conditional discharge in 2004. The journalists whose names appeared in the list held by ICO had commissioned his services but had not been prosecuted or interviewed in connection with any offences. The ICO had argued that the journalists' names constituted sensitive personal data by virtue of section 2(g) DPA; given the context, the list consisted of information as to the alleged commission of criminal offences by at least some of the journalists concerned. Sensitive personal data is usually exempt from disclosure under FOIA because, other than in exceptional circumstances, no condition from Schedule 3 DPA operates to permit disclosure in response to an FOIA request. All parties agreed that, to the extent the list constituted sensitive personal data, it was exempt from disclosure in response to an FOIA request. The Upper Tribunal agreed with the First-tier Tribunal's finding that the list of names did not constitute sensitive personal data. It held that the list simply amounted to a list of individuals who had commissioned Mr Whittamore's services and did not constitute evidence of the commission or alleged commission of any offence. In particular the Upper Tribunal noted that, irrespective of inferences that might be drawn regarding the culpability of individual journalists in this case, a data controller could not be expected to carry out a search of publicly available information in order to check whether there was anything in the public domain which, when combined with the personal data being processed, changed its nature into sensitive personal data; the question as to whether information is sensitive personal data " has to be answered in the immediate context of the information in question". The Upper Tribunal found that " the fact that some people might misconstrue the fact that a journalist's name was in the material seized from Mr Whittamore as an allegation that he had committed an offence did not convert personal data into sensitive personal data". Having determined that the requested list did not constitute sensitive personal data, the Upper Tribunal went on to consider whether the list should be disclosed under FOIA. This required assessment of whether disclosure would breach the first data protection principle and in particular whether the condition at paragraph 6(1) of Schedule 2 DPA was satisfied. The ICO argued that disclosure would cause undue reputational damage to the journalists concerned and would therefore result in an interference with their privacy that was unwarranted; accordingly none of the Schedule 2 conditions was satisfied. The Upper Tribunal however disagreed. It noted that the First Tier Tribunal had concluded that any reputational damage suffered by the journalists would be justified, in that they would be subject to legitimate criticism for using Mr Whittmore's services. Although the journalists had a legitimate interest in protecting their reputational rights, that interest did not carry significant weight in the circumstances. The Upper Tribunal agreed with the requester that, in this case, for the purpose of the balancing act required by paragraph 6(1) Schedule 2 DPA " what matters ultimately are a person's *deserved* reputational rights". The First Tier Tribunal's

Date	Description
	assessment that the balancing exercise favoured disclosure was upheld; ICO reports that the list has now been disclosed.
31 August 2015	**Optical Express appeal rejected by the First-tier Tribunal – clarification of the interpretation of consent under PECR** On 31 August 2015 the First-tier Tribunal rejected an appeal by Optical Express against an enforcement notice issued by the ICO on 19 December 2014 regarding complaints against the company dating back to November 2012. The enforcement notice concerned unsolicited text messages containing details of a competition to win free laser eye surgery. The ICO found these messages had contravened Regulation 22 of the Privacy and Electronic Communication Regulations (PECR) 2003 (which implements Directive 2002/58/EC prohibiting the sending of marketing messages without prior consent). The enforcement notice required Optical Express to cease its unsolicited marketing communications. This case clearly illustrates important points in the enforcement of data protection rules, especially in relation to the nature of unsolicited communications and the approach to consent under the PECR. Regulation 22 PECR requires that companies must obtain consent before sending unsolicited direct marketing communications to personal email accounts, unless customer information has been gained during the course of business and unless subsequent marketing communications relate to similar products and services. ICO guidance on direct marketing issued in September 2013 confirms that customer information obtained from third parties (Optical Express had received its marketing data from third party suppliers) cannot be used for email marketing in the absence of specific consent. Optical Express argued that the communications it had sent were not unsolicited and that Regulation 22 PECR did not apply. The Tribunal observed however that it is not possible for marketing to be solicited from an unknown sender; since recipients had not solicited marketing directly from Optical Express, the text messages constituted unsolicited marketing communications. Optical Express also argued that the meaning of consent had been misinterpreted by the ICO. However, the Tribunal confirmed that consent will be effective only where it is fully informed and specific; in order for consent to direct marketing to be effective recipients must be properly informed about who will be using their data for marketing purposes. Insofar as customers whose data had been supplied by a third party to Optical Express had not been made aware specifically that their details would be used by Optical Express, consent had not been fully informed and could not be relied on. This case joins a line of Tribunal decisions which take a critical view of spam marketing communications and send a clear signal to businesses that they should adopt robust compliance procedures. Businesses that compile data for direct marketing purposes should pay particular attention to the ways in which third parties collect customer data on their behalf. In cases where the PCR apply, it is important to ensure that clear and unambiguous consent has been obtained from marketing recipients, that recipients have been made aware of the specific identity of organisations that will be sending emarketing communications, and have been given an opportunity to opt-out of marketing communications. Businesses that engage in emarketing should consider

Date	Description
	implementing close monitoring of their consent arrangements to enable them to demonstrate compliance with PECR should they receive complaints about their use of customer data, or be subject to an investigation by the ICO.

3 September 2015	**ICO publishes analysis of Council common position on EU Data Protection Regulation**
	
	The EU's Justice and Home Affairs Council agreed its stance on the new Data Protection Regulation on 15 June 2015. Its agreed text recommends significant changes from both the Commission's original proposals and the subsequent position of the European Parliament.
	
	The ICO has now published its views on the Council's recommendations. It offers suggestions for improvement in a number of key areas:
	• Material scope: Although the ICO recognises the need for Member State flexibility in their application of the Regulation to processing carried out by public authorities, there is a concern that different data protection regimes may develop across the EU. While Member States do want local arrangements to preserve data protection agreements that exceed current EU standards, the number of separate arrangements must be minimised and should be consistent with Regulation standards.
	• Pseudonymisation: The ICO advocates a single definition for 'personal data' and supports the Council's recommendation to remove 'pseudonymous data' as constituting its own category. However, ICO also suggests that:
	  ○ it should not be defined in the context of 'personal data' since pseudonymisation should only be relevant as a privacy enhancing technique; and
	  ○ the requirements of pseudonymisation should be clarified to incentivise its use.
	• Incompatible further processing: The Article 6 provisions concerning 'incompatible further processing' of personal data are criticised as conflating the legal bases for processing and purpose limitation. The ICO suggests that these should be kept separate.
	• Consent: The ICO states that unclear references to 'explicit' and 'unambiguous' consent could confuse data controllers. A single, high standard of consent that should be either 'explicit', 'unambiguous' or both (and not one or the other depending on the context) should be preferred.
	• Children's consent: While the ICO supports enhanced protection for children whose personal data is processed, the current proposals present multiple issues. ICO identifies potential lack of clarity following the removal of a definition of 'child' and the introduction of inflexible age verification and parental consent systems.
	• Subject access rights: The ICO notes that this is the right most utilised by individuals and its parameters must therefore be as clear as possible. It criticises the distinction between the right to free access of personal information (Art 15(1)) and the right to obtain a copy of personal data without excessive charge. The ICO says that Art 15(2a) is unacceptable in its removal of data controllers' obligations to provide a copy of someone's personal data where this would involve the disclosure of another data subject's personal data.
	• Right to object: The ICO recommends that this should not be watered down from the Commission proposal. The 'complex matrix' of rights and the legal basis now underpinning this right will lead to confusion for individuals and

Date	Description
	businesses. • Security breach notification: Given the ICO's concerns about a large influx of notifications relating to trivial breaches, the Council's narrower focus on 'high-risk' breaches is welcomed. • DPOs: The ICO supports the Council's suggestion that the appointment of DPOs should not be mandatory unless required under Member State law. Although it agrees that DPOs should be suitably skilled, the prescribed tasks set out in Articles 36 and 37 are excessive and unrealistic. • Administrative fines: The ICO criticises the proposed 'three-tier' fine structure as inflexible and possibly arbitrary, stating that there should be more scope for supervisory authority discretion. A single list of breaches that *could* attract a fine would be preferred.
Cases	
24 July 2015	**Alfa Finance v Quarzwerke** This recent case, arising from a dispute in relation to the interpretation of a contractual audit provision imposing an obligation to use 'best endeavours' to grant 'reasonable access', will be of interest to data controllers and data processors engaged in agreeing organisational measures for the purpose of compliance with the seventh data protection principle and in understanding the scope their respective rights and obligations under existing data processing agreements. The following article, by Bird and Bird partner, Andrew White, summarises the case and highlights the implications for businesses in general:- **For the full article, by Bird & Bird partner, Andrew White, please see here.**
27 July 2015	**R (C) v Northumberland County Council & Another [2015] EWHC (Admin) 2134** In R (C) v Northumberland County Council & Another the Administrative Court considered a judicial review application concerning the length of time that local authorities may reasonably retain child protection records. The judgment focuses on the retention of records obtained or created in the course of investigations conducted under section 47 of the Children Act 1989. However, it makes a number of general observations which are likely to be of wider relevance and may assist all organisations that have to set data retention periods in order to comply with the Data Protection Act's fifth principle. The application was brought on behalf of family members of an individual who had been the subject of a section 47 investigation in childhood. The claimants sought an order quashing the defendant's data retention policy in relation to relevant records. They argued that the retention policy, which recommended a standard retention for a period of 35 years following case closure, was in breach of the common law, the Data Protection Act and the Human Rights Act. The Information Commissioner, who was joined as an interested party, argued before the court that records should be retained only for as long as necessary having regard to the purpose for which they continued to be held. ICO considered that once a relevant child had reached the age of 18, it could no longer be the case that relevant records were held for child protection purposes and such records should be retained only by the authority's legal department and for the purpose of responding to any potential legal claim. On this basis it would not ordinarily be possible to justify retaining records for longer than the statutory

Date	Description
	limitation period in tort (i.e. a maximum of 6 years following the child's 18th birthday). The ICO took the view that longer retention periods might be justified on a case by case basis for example where records might continue to be of relevance to the protection of other children but that in order to justify longer retention periods periodic review would be necessary. The court found that in setting retention periods the authority was entitled to take a wide approach and to consider the potential relevance of records to future criminal, statutory or local investigations and to consider the extent to which records might be of interest to affected children far into adulthood. It was for the local authority to determine the appropriate retention period but the court found that a policy designating a retention period of 35 years from case closure was lawful; it was carefully considered, reflected the purposes for which the records could be required and was applied proportionately and flexibly. The court specifically rejected, as imposing an unreasonable burden, the view that the authority should periodically review relevant records on a case by case basis to justify retention periods of longer than 6 years from case closure.
30 July 2015	**R v (1) Waqar Bhatti (2) Noasheen Muhammad and (3) Sohail Akhtar [2015] EWCA CRIM 1305** The appellants appealed against their convictions for conspiracy to facilitate a breach of immigration law by non-EU citizens, contrary to s.1(1) of the Criminal Law Act 1977. The convictions had centred on allegations that they had established and run a 'sham' college to issue false immigration documentation and thereby 'establish bogus immigration status' for its 'students'. Only the second ground of appeal raised data protection issues. The appellants alleged the police had acted unlawfully by obtaining personal information from the credit-ratings agency, Experian Ltd. This included particulars of bank accounts and credit ratings. They argued that the police had bypassed the procedural requirements of the Police and Criminal Evidence Act 1984 ('PACE') to acquire confidential information which could not otherwise have been obtained. This should have led to the exclusion of important evidence from the jury's consideration under s.78(1) PACE. **1. THE ARGUMENTS** The appellants argued that the process by which the Prosecution acquired information was unlawful in two respects: • Although Experian purported to have disclosed relevant personal data to the police under the 'crime and tax' exemption in s.29(1) DPA, Experian had made no assessment as to whether the material should be released. This abrogated the requirement that data is processed 'fairly and lawfully' under the first data protection principle. • By approaching Experian, the police contrived to by-pass the procedural requirements of PACE 'in order to acquire confidential information which it could not otherwise have obtained.' Experian was effectively making material available to the prosecution without the necessary 'order for production' from a judge. Such order would not have been made without stringent conditions. This evidence should therefore have been inadmissible under s.78(1) PACE. **2. THE OUTCOME** The CA dismissed the appeal, holding that neither Experian nor the police had acted unlawfully in relation to the disclosure. The

Date	Description
	Court found in favour of the Crown's case, which included the following arguments: • Court 'orders for production' of evidence under PACE are designed to cover circumstances in which the prosecution had tried without success to obtain material. In this case, Experian voluntarily made it available in the first instance. The procedure was therefore not relevant. • Experian did not disclose the information in breach of confidence, as it acquires credit information based on a customer understanding/consent that it will be shared. Experian does not 'own' the data held on its systems, but acts under license (i.e. the data is provided for and 'owned' by other organisations who obtain customer consent to sharing as a condition of providing financial services). • Although Experian holds a Credit Account Information Sharing ('CAIS') file - a file from which credit information may be accessed - customers expressly agree in their credit applications that their data may be shared for the purpose of crime detection, prevention and prosecution. • In relation to whether or not the s.29 DPA 'crime and tax' exemption had been engaged, Experian had legitimately relied on the representations of the investigating officer as he sought to obtain the data. He identified himself as a police officer with specific training and as being subject to audit, stated that the information was for the purposes set out in s.29, set out the offence he was investigating and communicated the fact that the information requested was essential for the purpose of an investigation into organised crime. The Court of Appeal acknowledged that customers may be surprised to find credit referencing information within a CAIS system and that it may be accessed by the police under s.29 DPA, but concluded that neither Experian nor the Police acted unlawfully in relation to the disclosure of this information. There was therefore no issue of evidence inadmissibility.
6 August 2015	**Ashley Judith Dawson-Damer & Others v Taylor Wessing LLP& Others [2015] EWHC 2366** In August 2015, the High Court handed down its decision in the case of Ashley Judith Dawson-Damer & Others v Taylor Wessing LLP& Others. The judgment concerns a contested subject access request made against the background of legal proceedings in the Supreme Court in the Bahamas concerning family trusts and considers a number of issues that commonly present challenges for data controllers when responding to subject access requests including the scope of search obligations, the relevance of the requester's motive, the exemption in relation to legal privilege and duties in relation to manual records. In considering the scope of the exemption at paragraph 10 of schedule 7 of the DPA concerning legal privilege, the Court found that the exemption should be interpreted purposively and extends 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. Insofar as the defendant's search obligations were concerned, the court noted that there was virtually no evidence of the searches carried out by the defendant. The court however accepted the defendant's argument that it was not reasonable or proportionate for the defendant to be required to carry out a search given that, if such a search were to be carried out, it would not be possible for the defendant to apply the exemption for legal privilege without first engaging lawyers skilled in the Bahamian law of privilege to identify privileged material.

Date	Description
	Given the finding of the court in relation to the defendant 's search obligations, the comments which Behrens HHJ went on to make in relation to the court's discretion and the question of motive in contested SAR cases were obiter. However, Behrens HHJ indicated that had he found otherwise in relation to the defendant's search obligations, he would have exercised his discretion under section 7(9) DPA to decline to order the defendant to comply with the SAR because the real purpose of the SAR was to obtain information to be used in connection with the Bahamian proceedings. There was no suggestion of mixed motives or of any wish on the data subjects' part to access their data in order to check its accuracy. Behrens HHJ found that the SAR claim would not have been brought at all but for the purpose of the Bahamian proceedings, and, following the judgment of Auld LJ in Durant v FSA, this was not a proper purpose. The judgment is currently under appeal.
25 August 2015	**Zaw Lin and Wai Phyo v Commissioner of Police for the Metropolis [2015] EWHC 2484 (QB)** This is an interesting subject access case - although probably of limited relevance to most data controllers. The applicants were facing trial in Thailand for the murder of two British tourists. They made a subject access request to the Metropolitan Police in London to access data held by the MPS about them, as a result of a report which the MPS prepared for the victims families. Mr Justice Green concluded that the crime prevention exemption could cover information held for police family liaison purposes and that the requested information was exempt under s.29. The inability of the applicants' advisers to to review the disputed material so as to advance arguments on it, presented real difficulties in this case and the judge recommended that in future cases such issues should be resolved at an early stage as part of case management arrangements. **FACTS** The applicants had been charged, in Thailand, with the murder of two British tourists in 2014. If convicted, they face the death penalty. The applicants initially confessed, but later retracted their confessions, claiming that the confessions were the result of torture. The murder, arrest and subsequent claims of abuse had received significant international media coverage. In order to re-assure the families of the victims that the case was being properly handled, the Thai authorities agreed that the Commissioner for the Metropolitan Police (MPS) could send personnel to Thailand with a view to obtaining information about the investigation, so as to report to families of the victims on this. At the outset of the investigation, the MPS specifically agreed with Thai police that the report would only be shared with the families. The role of the MPS was not to assist in investigation of the crime - UK policy was not to provide assistance in cases where the death penalty could be imposed. This policy also meant that the MPS did not provide a copy of the report to Thai police. The MPS was aware that release of the report may prejudice the conduct of the Thai trial: this would be detrimental not just to this case, but to the wider reputation of the MPS and to the willingness of overseas authorities to share data with it in future. The

Date	Description
	assurances of confidentiality and non-disclosure which were given were, therefore, significant. The judge reviewed the report. Some of the content related to third parties (witnesses, the victims etc); some related to the Thai police and the way the investigation had been conducted. Some did relate to the applicants - but the judge concluded that this was less than 10% of the content of the report. He noted that the contents of the report were not in the category of state secrets. In November 2014, the applicants made subject access requests to the MPS for personal data contained in the report. They argued, i.a., that (1) they should have a right to correct any inaccuracies and (2) they should have access to information which may assist their defence. The MPS refused to provide the information, relying on s.29 DPA - i.e. that disclosure would prejudice the prevention and detection of crime. **PROCEDURAL CONCERNS** Where a data protection case involves material which one party claims is exempt from disclosure to the data subject, then the Data Protection Act provides that the court has a power to inspect this material, but that it should not be provided to the data subject. The judge determined that this power (s.15(2)) also included an ancillary power to require the data controller to answer questions about the material, where this was necessary to allow the judge to understand the material. The judge expressed significant concern that there was no mechanism for any representative of the claimants (for example, a special advocate) to inspect the material. He was greatly troubled that defendants at risk of the death penalty should have to argue about points in the abstract, without any mechanism allowing them to inspect the relevant material. These difficulties were compounded by the urgency of the proceedings and the fact that the parties had not addressed them at an earlier stage of proceedings. If similar issues arose in future cases, they should be addressed by a case management conference at an early stage. **DATA PROTECTION ANALYSIS** **1.** s.29 had to be applied reasonably and proportionately: in effect applying similar standards to judicial review, when considering a decision taken by a public authority. The judge rejected arguments advanced by MPS that proportionality was irrelevant and that there was no need for the MPS to consider the relative importance of MPS policing objectives against the importance of the issues for the claimants.

Date	Description
	2. the MPS argued that broader European law considerations and principles of interpretation were irrelevant to the question at issue here. This was because, whilst the DPA was enacted to implement the Directive, questions of international law enforcement fell outside the scope of the Directive. It followed that, whilst the DPA does apply to such maters, the Directive did not - and the approach to interpretation should reflect this. The judge concluded that the point was not, ultimately, important: there would be little difference to the interpretative approach adopted under common law. **3.** s.29 could be applied to police family liaison purposes. However, as the defendants were asking for the data in connection with proceedings where they could face the death penalty, a narrow interpretation would be appropriate. This said, the judge found that the arguments advanced by MPS about the chilling effect of disclosure and the possible adverse (procedural) effect on the Thai trial to be significant. **4.** The judge divided the personal data into 3 categories: that adverse to the defendants (where he concluded that release would not assist them and where he assumed that such data would have been provided to them as part of the proceedings anyway); data neutral to them - where the S29 considerations above would, he thought, trump their interests; data positive to them - where more consideration was needed. **5.** The judge noted that the data was limited and broad brush. Much would have been known to the applicants anyway and none was exculpatory. On this basis the judge considered that it was right to argue that the information was exempt on the basis of s29.
Other	
17 July 2015	**Morrisons employee jailed for data fraud** On 17 July 2015, a former senior auditor of the UK supermarket chain Morrisons was sentenced to eight years in prison for leaking the personal details of 100,000 of its employees to newspapers and public websites. The auditor, whose actions were prompted by a grudge against his employer, leaked information that included salaries, National Insurance numbers and bank details. He was convicted of fraud, unauthorised access to computer material, as well as the unlawful disclosure of personal data. The supermarket, which announced a package for affected employees which includes identity theft protection,has incurred costs in the region of £2 million in order to safeguard employees and guard against the risk of identity theft following the data breach. The case highlights the importance of maintaining effective systems to monitor against data theft and fraud and the risk of reputational damage where data security is compromised as a result of the malicious acts of third parties and illustrates the costs that can be associated with protecting potential victims of unlawful disclosures attributable to third parties.
July 2015	**Supreme Court grants part-permission to appeal Google v Vidal Hall** In July 2015, the Supreme Court granted Google Inc leave to appeal two of the three questions determined by the Court of Appeal in Google Inc v Vidal Hall & Others ([2015] EWCA Civ 311). Leave to appeal the Court of Appeal's finding that misuse of

Date	Description
	private information gives rise to a claim in tort rather than in equity was not granted. The Supreme Court will now consider the following questions: **1.** Was the Court of Appeal right to hold that section 13(2) DPA is incompatible with Article 23 of the Data Protection Directive? **2.** Was the Court of Appeal right to disapply section 13(2) DPA on the grounds that it conflicts with rights guaranteed by Articles 7&8 of the EU Charter of Fundamental Freedoms? The decision of the Supreme Court is not expected to be handed down until 2016.
Europe	
27 July 2015	**Opinion 3/2015 "Europe's big opportunity": EDPS recommendations on the EU's options for data protection reform** The European Data Protection Supervisor ('EDPS') has published its Opinion ('opinion') for data protection reform. The main objective of the opinion is to facilitate the final stages of the EU reforms to the General Data Protection Regulation ('GDPR') revisions. The EDPS has highlighted the following reasons why the reform of the GDPR remains an important priority in Europe and requires careful attention for the following reasons: **1)** The GDPR has a potential effect on all individuals and organisations which process personal data within the EU. Moreover, it will have an impact on organisations outside of the EU which process the personal data of EU citizens. **2)** The GDPR requires high-level "legal engineering" as laws in this area are complex and technical, and so the EU must be selective and focused. The brief list of recommendations by the EDPS includes the following: **1)** The rights of data subjects should be protected more effectively. For instance: • Obtaining consent should avoid coercive tick boxes because there is no meaningful choice for individuals as a consequence; On international transfers, the GDPR should provide safeguards against requests for transfer issued by authorities in a third country to data located in the EU. Requests should only be recognised where they respect Mutual Legal Assistance Treaties, international agreements or forms of international cooperation.; • All authorities should be ready to effectively fulfil their functions on the date of the regulation entering into force. **2)** The opinion demands greater clarity and simplicity for bodies responsible for processing of personal data. For instance:

Date	Description
	• The reduction of documentation obligations on controllers; • Guidance should be issued by supervisory authorities to data controllers to develop internal rules of procedure in the spirit of new regulation. **3)** Reform should be future-oriented, based on the dignity of the individual and informed by ethics. **4)** The EDPS supports the introduction of the principles of data protection by design and by default in order to promote market-driven solutions.
8 September 2015	**EU-US signs umbrella agreement on transatlantic data protection** The EU and US have initialled an 'umbrella agreement' designed to protect data exchanged between the unions for the purpose of law enforcement cooperation. Key safeguards and guarantees include: • transferred personal data may only be used for the purpose of preventing, investigating, detecting or prosecuting criminal offences; • onward transfers to non-US/EU countries or international organisations require the prior consent of the competent authority in the origin country; • retention periods must be made public and should not be longer than necessary or appropriate; • individuals may access their personal data (subject to law enforcement conditions) and request that it is corrected if inaccurate; • a new mechanism will ensure data security breaches are notified to the competent authority and, where necessary, the data subject; and • EU citizens may obtain judicial redress and enforce their rights before US courts if their data is incorrectly or unlawfully processed (e.g. unlawfully disclosed). The agreement will not be formally signed until the US Judicial Redress Bill, which proposes to grant such equal treatment to EU citizens in the US, is adopted by the US Congress.
11 September 2015	**EDPS sets up an Ethical Advisory Board** On 11 September 2015, the European Data Protection Supervisor (EDPS) published an Opinion, entitled *Towards a New Digital Ethics*, on the importance of an ethical approach to the development of future technologies and the collection of personal data, such that people are not reduced to mere data subjects. In order to pursue this objective, the EDPS will establish an Ethics Advisory Board in response to emergent trends which "raise the most important ethical and practical questions for the application of data protection principles," according to the Opinion. The Ethics Advisory Board will be formed of "a select group of distinguished persons" drawn from the social sciences, such as

Date	Description
	philosophy, sociology and psychology, as well as experts in technology, economics and finance. Additionally, the group will pool additional expertise from areas such as health, media, government and national security. This broad approach will go some way to ensuring the effective protection of data subject rights, which has yet to be finalised in the Data Protection Regulation. In July, the EDPS published a draft of the Data Protection Regulation which included a clause on "human dignity", which has been repeated in this published Opinion.
1 October 2015	**Weltimmo v NAIH** On 1 October 2015, the Court of Justice of the European Union (CJEU) delivered its ruling in Weltimmo v. NAIH [the Hungarian Data Protection Authority] (C-230/14). It affirmed that a data controller who processes personal data, and has its registered seat in one Member State may nevertheless be subject to another Member States' jurisdiction in certain circumstances. The Data Protection Directive ensures this is possible where such processing is carried out 'in the context of activities of an establishment of the controller' located within that second territory. The CJEU held that the concept of 'establishment' is 'broad' and 'flexible', extending to 'any real and effective activity – even a minimal one – exercised through stable arrangements.' The presence of one representative outside of the registered territory, who sought to negotiate debts with third parties, was sufficient. Although the nationality of those concerned by data processing is irrelevant, the CJEU highlighted that: (1) the fact that the controller's activities are mainly or entirely targeted/directed at the second Member State; and (2) the existence of a representative in the second Member State who carries out functions on behalf of the controller could, in particular, be taken into account when determining whether processing falls within 'the context of activities of an establishment of the controller' within a second territory. The court also found that where a DPA finds it does not have jurisdiction to respond to a complaint based on the above principles, although it may investigate immediately, it cannot impose penalties outside of its own territory. Requests would have to be made to the supervisory authority of that other Member State to ask them to establish infringements and impose penalties, where their applicable law permits. **We will be releasing our full commentary on this case on the Bird & Bird Data Protection & Privacy site shortly.**
6 October 2015	**CJEU invalidates Safe Harbor** The Court of Justice of the European Union (CJEU) handed down its judgment in Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, in which it found the Commission's US Safe Harbor Decision to be invalid. **For our full article on this, please see here. To view our complimentary webinar, please see 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)**
24 September 2015	**Flybe Limited**	Undertaking	Flybe Limited has signed an undertaking to comply with the seventh data protection principle. On 14 November 2014, Flybe informed the ICO of a data protection incident involving a temporary employee who had scanned and emailed a picture of another employee who worked on the air side. The ICO found that Flybe did not provide adequate data protection training for staff, including this temporary employee. It also found that Flybe had an inadequate data protection policy.	Flybe will ensure it processes data in line with the seventh data protection principle, including • the revision of its data protection policy which covers use and storage, and • that staff training is provided for all employees who handle personal data, whether temporary or permanent.
24 September 2015	**Martin & Company**	Undertaking	Martin & Company has signed an undertaking to comply with the seventh data protection principle. In January 2015, Martin & Co informed the ICO that a DVD of evidence provided to the firm by the Crown Office & Procurator Fiscal Service had been lost. The DVD had been collected from the Crown Office by a colleague from another firm, but was mislaid by the third party. The DVD was not encrypted. The ICO found that the firm provided inadequate staff guidance on data protection compliance and training. There was also no formal procedure in place for the collection of personal data outside of the office.	Martin & Co will ensure it processes data in line with the seventh data protection principle, including • the implementation of appropriate procedures for the collection of data from third parties, and • safeguards are put in place to encrypt media used to store or transmit data. Martin & Co have three months to implement these changes.
16 September	**Cold Call Elimination**	Monetary penalty notice	Cold Call Elimination has been fined £75,000 for making unsolicited marketing calls to sell cold call blocking devices. The	The monetary penalty must be paid to the ICO by 15 October 2015. Cold

2015	**Ltd**		penalty related to a contravention of regulation 21 of the Privacy and Electronic Communications (EC Directive) Regulations 2003. The ICO began its investigation in November 2013 following complaints to the ICO and TPS. Cold Call Elimination had confirmed that it received its data from a third party, and did not screen that data itself against the TPS. ICO found that the company had made unsolicited calls to numbers registered with the TPS and that individual subscribers had not given their prior consent. The ICO regards this as a serious contravention of the regulations which was likely to cause substantial distress to those who received the calls, particularly in the case of elderly or vulnerable subscribers who felt pressurised into giving bank details. While the company was found not to have acted deliberately, it had been negligent given that in the issue of unsolicited calls had been highly publicised in the media. The ICO had also provided Cold Call Elimination in 2013 with warnings against its behaviour. ICO found that the company had failed to take reasonable steps to prevent the contraventions by, for example, screening its data against the TPS.	Call Elimination has 28 days in which to appeal.
16 September 2015	**General Dental Council**	Undertakings	General Dental Council has signed an undertaking to comply with the seventh data protection principle. The General Dental Council (GDC) reported two incidents to the ICO. The first involved the receipt by a registrant of allegations regarding his fitness to practice and a CD which contained background information all of which had been sent to him by GDC. The registrant complained to GDC that these had been sent in error. The GDC investigated and found that the recipient had a similar name to the individual who was the subject of the allegations and the allegations and the CD had been sent to him in error. GDC's employees had failed to implement its checking process or encrypt the contents of the CD.	The General Dental Council must ensure that • all employees who process personal data receive data protection training by 30 September 2015, • It must also establish a mandatory refresher programme at least every two years and by 30 November 2015, • All training sessions must

			The ICO established that, despite written policies, the General Dental Council failed to provide data protection refresher training and that training was conducted in an ad hoc basis. The ICO found that, considering the high degree of sensitivity of the personal data, the General Dental Council had failed to implement sufficient organisational measures. A second incident involved the loss of a set of patient data. This data had likely not left GDC's offices and had been destroyed securely in error. ICO found that GDC had failed to provide appropriate data protection training to the employee involved.	be fully monitored and completion statistics must be reported to relevant senior management, • Appropriate follow up measures are put in place for non-attendance
18 August 2015	**Google Inc**	Enforcement notice	The ICO has ruled that Google Inc must remove nine search results which linked to information about a person that was no longer relevant in contravention of the first and third data protection principles that personal data must be adequate, relevant and not excessive. This enforcement notice follows Case C-131/12 *Google Spain v Agencia Espanola* and the application of the ICO's own criteria.	Google must remove links to the websites displayed on the basis of a specific search term. Google must comply within 35 days of the order. Google has a right to appeal the notice.
18 August 2015	**British Show Jumping Association**	Undertakings	The British Show Jumping Association has signed an undertaking to comply with the seventh data protection principle. In December 2014, the ICO was informed that a file containing a large amount of membership information had been sent to a distribution list of unintended recipients. The file contained the personal data of 14,152 members. The ICO found that the organisation had no relevant procedures or training in place for staff in relation to the emailing of personal data, or on the retention and naming of documents contained on shared drives. The staff also received no data protection training.	The British Show Jumping Association must ensure that • staff are provided with guidance on checking the content of and attachments to emails which contain personal data, and • there is an appropriate policy regarding the use of shared network drives, which includes retention and use of file names.
14 August	**Anxiety UK**	Undertaking	Anxiety UK has signed an an undertaking to comply with the	Anxiety UK must implement:

2015			seventh data protection principle. In February 2015, the ICO was informed by Anxiety UK that personal data, which was held in a password protected area of its website, had been publicly available for 12 months as the data appeared on the results of a search engine search. The ICO found that Anxiety UK had failed to take sufficient technical measures to ensure the security of its systems. , Anxiety UK should, for example, have conducted penetration testing prior to the launch of its website, or should have adopted other appropriate quality assurance controls.	• appropriate periodic security testing of its website, and • adequate contractual controls for those who mechanise the processing of personal data on its behalf.
10 August 2015	**Point One Marketing Ltd**	Monetary penalty notice	Between 1 February 2014 and 31 March 2015, the ICO received 169 complaints about the company from individual subscribers who were registered with the TPS. The company repeatedly called subscribers, often being rude and aggressive and preying on vulnerable people. Bank details were obtained from some of the subscribers. Ironically, the company was trading as "Stop the Calls" and offering services including a call blocking device and the removal of customers's details from cold calling databases. ICO considered this an aggravating factor in relation to the company's contravention of PECR rules.	Monetary penalty notice of £50,000.
6 August 2015	**Brunel University London**	Undertaking	Brunel University London has signed an undertaking to comply with the seventh data protection principle. Staff at the University locked 17 boxes of files in a room during a renovation. Ten of the boxes went missing. The University had a number of policies in place at the time of the breach, including data retention schedules and a Data Protection Policy.	The University shall ensure: • Staff members receive training on the requirements of the Data Protection Act upon induction; • Mandatory refresher training shall be provided to all staff who routinely process data; • Other relevant security measures are

				implemented.
6 August 2015	**The Money Shop**	Monetary penalty notice	In April 2014, a server was stolen from the Money Shop store in Northern Ireland. The server had been left on a manager's desk, next to a locked fire escape through which the burglar gained entry. The server was not sufficiently encrypted and has not been recovered. Although the Money Shop had a procedure whereby servers had to be locked in a separate room, some of the Money Shop stores in the UK are too small for a room. In May 2014, the Money Shop lost a second server. At the time of the loss, the encryption process had not been completed. The servers contained full customer records, including bank account details. The ICO considered that the Money Shop failed to take appropriate technical and organisational measures against the unauthorised processing and accidental loss of personal data.	Monetary penalty notice of £180,000.
4 August 2015	**Doncaster Metropolitan Borough Council ('the Council')**	Undertaking	The Council lost a file containing 66 records of families in receipt of health services. It was likely that the file had been lost as a result of an internal office move. An ICO investigation revealed that although mandatory data protection training was in place for staff, completion rates were low.	The Council shall: • Conduct an analysis of all roles within the organisation to determine the data protection awareness required for the role; • Deliver mandatory data protection training to staff identified you this analysis; • Ensure all staff undertake mandatory training within the timescales identified.