Title	Description
UK	
Information Commissioner's Office (ICO)	
31 August 2014	**Local Authorities Audit Report** The ICO has recently released its annual audit outcomes report into its review of 16 local authorities during 2013. Local authorities are required to submit to audits at the request of the ICO, unlike private sector organisations. The ICO found: • No authorities were able to show a high level of data protection assurance. Almost half of authorities fell into either the "limited" or "very limited" assurance categories. • Examples of areas for improvement included the failure to keep version control and process management for policies and procedures, failure to appropriately log and monitor subject access requests methodically, failure to provide and monitor attendance at training for key staff (eg those processing SARs) and putting in place data sharing agreements as and where required. • Areas of good practice included assigning information security responsibilities and ownership at a senior level and the use of penetration testing to ensure security of a high standard. For the full outcomes report, read **here**.
2 September 2014	**Privacy Seal Scheme** The ICO has launched a consultation on the framework criteria for potential privacy seal schemes that wish to qualify for ICO endorsement. The aim of the scheme is to act as a "stamp of approval" enabling organisations to demonstrate that they maintain good privacy standards. Any scheme that the ICO chooses to endorse will be operated by an independent third party in the UK, who must be officially accredited by the UK Accreditation Service (UKAS). The requirements for any scheme are that it must: • be a new privacy scheme; • cover personal data processing in the UK; • be "consumer-facing", promoting consumer trust and protection; and • focus on a specific "product; process or service". Further, scheme operators must be able to show that there is a case for the scheme in its target area, which can be sector-specific or have cross-sector scope, as well as be in the public or private sectors. The ICO's consultation closes on 3 October 2014, with proposals due to be selected in early 2015, and the first scheme(s) launched in 2016 for a minimum of three years. The framework criteria can be found **here.**
4 September 2014	**Data Protection Guide for the Media** The ICO has launched its guidance for the media, following a consultation on a copy of the draft guidance earlier this year. There have

	been changes from the consultation draft, in particular ,there is a broad approach to interpretation of the exemption for processing for journalism (s.32 of the Act). Highlights of the guidance include : • A balancing test ought to be applied as between the public interest in publication and the privacy rights of the individual, and editors/journalists should be responsible for deciding what is in the public interest rather than the ICO; • It is possible to meet retention requirements even where "*contact details and background research are a vital journalistic resource and you are likely to want to keep them for a long period or indefinitely, even if there is no specific story in mind at present";* • "Journalism" should be interpreted broadly, including "*the entire output of print and broadcast media, with the exception of paid for advertising*" and work of non-media organisations "*to publish information, opinions or ideas for general public consumption*"; and • Unlike the draft guidance, reliance on the exemption is permitted where it is "*unreasonable to comply* (with the Act) *in light of your journalistic aims*", not merely *impossible* to comply. The full guidance can be found **here**.
30 September	**Credit Reference Agencies Review** The ICO has published a report detailing reviews of Callcredit, Equifax and Experian (the three main credit reference agencies in the UK). The ICO conducted the consensual reviews with the aim of helping the agencies identify improvements and address any particular issues, following the airing of an episode of Channel 4's *Dispatches* in which Experian's processing of inaccurate personal data was raised. The report emphasises that, generally, the credit reference industry has a good understanding of data protection and the ICO found that, in some respects, the credit reference agencies went beyond the steps necessary for compliance. However, the ICO have made some recommendations to improve practice, for example, credit reference agencies should develop a process to remind customers of data protection obligations and should audit customer compliance at least once per year. The full report can be found **here**.
Enforcement	
	Enforcement for the contemplated period includes: 2 monetary penalty notices, 4 new undertakings (and 1 follow-up review of an existing undertaking), 2 enforcement notices and 4 prosecutions. Please see below Enforcement Table for more details
Other	
26 June 2014	***CR19 v Chief Constable of the Police Service of Northern Ireland [2014] NICA 54*** The Court of Appeal in Northern Ireland awarded nominal damages of £1 and upheld a £20,000 general damages award, which it found took into account compensation for distress caused by a data breach. The case concerned files containing personal data of a former police offer, the appellant, which had been stolen from a police station in Northern Ireland in 2002 by presumed terrorists. As a

	consequence, the appellant's post-traumatic stress disorder worsened. The police force admitted a breach of section 4 of the DPA by failing to keep the appellant's personal data secure. The trial judge awarded the appellant £20,000 in compensation for personal injuries, loss and damage, without referring to the breach of the DPA, which the appellant had not raised at trial. The police officer appealed for a higher award, but the Court found that the trial judge's assessment had included the distress caused by the breach of the DPA and that related damages "must be considered to be subsumed" into that award. However, the Court awarded nominal damages to acknowledge that there had been a breach of section 4 of the DPA, following *Halliday v Creation Consumer Finance* (2013) and *AB v Ministry of Justice* (2014). **Read the full case here.**

Europe	
CJEU	
	YS v. Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v. M, S The facts Three people applied under Dutch asylum law for fixed-term residence permits. One application was refused and two others granted. All three applicants made subject access requests for the 'minutes' prepared by the case officers. These included, i.a., personal details such as name, date of birth, nationality, gender, ethnicity, religion and language. They also included administrative details relating to the case officer, the 'reviser', procedural history, statements made by the applicant, documents submitted and the relevant law, as well as legal analysis - an assessment of the applicant's circumstances in the light of the relevant law. The authorities refused to release details of the legal analysis in response to the subject access requests. Two Dutch courts referred various questions to the CJEU, summarised as: 1. Whether the data relating to the applicants in the 'minutes' and also the 'legal analysis' are personal data; 2. Whether the applicants have a right of access to data concerning them in the 'minutes' and if so does that give a right to the documents themselves; and 3. Whether article 41(2)(b) of the EU Charter of Fundamental Rights can be relied on against national authorities. The decision *What is personal data?* The personal details about the applicants set out in the 'minutes' were 'personal data': '*There is no doubt that the data relating to the applicant for a residence permit and contained in a minute, such as the applicant's name, date of birth, nationality, gender, ethnicity, religion and language, are information relating to that natural person, which is identified in that minute in particular by his name, and must consequently be considered to be "personal data" …*' *Is 'legal analysis' personal data'?*

	The analysis here was '*the legal classification of facts relating to an identified or identifiable person (or event involving such persons) and their assessment against the background of the applicable law'.* Although it may contain personal data, the analysis does not in itself constitute personal data: '*such a legal analysis is not information relating to the applicant …, but at most … is information about the assessment and application by the competent authority of that law to the applicant's situation, that situation being established inter alia by means of the personal data relating to him which that authority has available to it.'* The court considered that one of the purposes of data protection is that a '*person may be certain that the personal data concerning him are correct and that they are processed in a lawful manner. … it is in order to carry out the necessary checks that the the data subject has … a right of access… the legal analysis is not in itself liable to be the subject of a check on its accuracy by the applicant …'* *Does data protection give a right to documents held?* No: a right to personal data is not the same as a right to the documents containing such data. *'For that right to be complied with, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with [Directive 95/46/EC], so that he may, where relevant exercise the rights conferred on him by that directive.'* *Can art.41(2)(b) of the EU charter of rights be relied on against member states?* This grants individual a right to have their affairs handled impartially by Union bodies and the right includes a right of access to the individuals file. However, the court followed the plain wording of the charter – the rights are only granted in relation to Union bodies, not those of member states. Key take-aways 1. Consider if the data being released will assist the data subject in exercising data protection rights (eg of correction, or of arguing that there is no lawful basis for processing). If not, the data may not be personal data at all. 2. Subject access should be distinguished from other legal rights and procedures available to an individual – the case may, possibly, be useful for those faced with an applicant who is using data protection as an alternative to discovery of documents in litigation. 3. Data protection is a right to information not documents: this could be extracted from documents and provided in that way. **Read the full case here.**
Data Protection Reform	
11 and 12 September 2014	**Development relating to the Personal Data Protection Reform Package** The Council Working Group on Information Exchange and Data Protection (DAPIX) has discussed Chapter IV of the proposal and the right to be forgotten.
Article 29 Working Party	

4 June 2014	**WP29 Opinion 7/2014 on the protection of personal data in Quebec** The Article 29 Working Party (WP29) has issued an opinion on the adequacy of the Québécois regulatory system on the protection of personal data. Under provincial Québécois law this is regulated by Articles 35 to 41 of the Quebec Civil Code and the Quebec Act respecting the protection of personal information in the private sector. The Canadian federal law on data protection, the Personal Information Protection and Electronic Document Act (PIPEDA) was declared as providing an adequate level of protection by a decision of the European Commission in 2001. The opinion of the WP29 compares the provisions of the Québécois regulatory system with the main provisions of Directive 95/46/EC, taking into account the WP29's opinion "*Transfers of Personal Data to Third Countries: Applying article 25 and 26 of the EU data protection directive*" (WP12). The opinion notes that the federal and provincial positions on the scope of the application of the Quebec Act do not coincide. The WP29 concluded that it is necessary to clarify the territorial scope of the Quebec Act before any decision on its adequacy is taken by the European Commission. The opinion also highlights some points to be drawn to the attention of the European Commission. **The opinion is available here.**
1 August 2014	**WP29 Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Directive** The statement issued by the WP29 welcomes the Court's Ruling and summarises the reasons on which the ruling is based, namely: 1. The Directive entails a wide-ranging and particularly serious interference with the fundamental rights to privacy and to the protection of personal data; 2. It fails to sufficiently circumscribe such interference to ensure that it is limited to what is strictly necessary for the purpose of fighting 'serious crime', thereby leaving it too open for Member States to decide on the scope of data retention; 3. It fails to define the guarantees surrounding data retention; and 4. It does not require that the data be retained within the EU, and that consequently it does not fully ensure the control of compliance with the requirements of protection and security by an independent authority on the basis of EU law. The WP29 confirms that national measures based on the invalidated Directive are not directly affected by the ruling. However, the statement urges Member States and European institutions to evaluate its consequences on national data retention laws and practices. In particular, national data retention laws and practices should ensure: (i) there is no bulk retention of all kinds of data; (ii) that access by authorities is limited to the strictly necessary and that it is subject to substantive and procedural conditions; and (iii) that national laws provide for effective protection against the risk of unlawful access and any other abuse.

	The WP29 requests that the European Commission provides clear guidance on the consequences of the Court's judgment. **The statement is available here.**
16 September 2014	**WP29 Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU** The WP29 intends to follow the development of big data trends closely. In the interim, the WP29 has produced this statement which communicates a number of key messages on this issue. A few of these are summarised below: 1. The WP29 would support genuine efforts at EU or national levels which aim to make the benefits from the development of big data real for individuals in the EU. 2. Big data operations raise important social, legal and ethical questions so benefits can only be reached if the corresponding privacy expectations of users are appropriately met and their data protection rights respected. 3. The EU legal framework is applicable to the processing of personal data in big data operations (including Directive 95/46/EC). The WP29 emphasises that the EU data protection principles under this legal framework remain valid and appropriate for the development of big data, subject to further improvements to make them more effective in practice. 4. "Big data" is a broad term that covers a great number of data processing operations, and the operations do not always involve personal data. 5. Some developments that are qualified today as big data have long been implemented in many EU Member States – these have already been addressed within the framework of the existing data protection rules. The WP29 has recently released a number of Opinions based on these shared experiences which are relevant to the analysis of privacy concerns raised with regard to big data. 6. Increased international cooperation will be required between the relevant regulators as many frameworks may apply simultaneously at a global level. **The statement is available here.**
16 September 2014	**WP29 Opinion 8/2014 on the Recent Developments on the Internet of Things (IoT)** The WP29 specifically focused its report on three IoT developments: (1) wearable computing; (2) quantified self; and (3) home automation ("domotics"). The aim of the opinion is to highlight a number of significant privacy and data protection challenges that these developments may present. Their concerns regarding IoT technology include: 1. The lack of control for a user over the dissemination of his/her data; 2. The quality of the user's consent may be compromised. Consequently the WP29 recommends that new ways of obtaining the user's valid consent should be considered by IoT stakeholders;

	3. Modern techniques relating to data analysis and cross-matching may lend the data to secondary uses which may be unrelated to the purpose assigned to the original processing; 4. The detailed detection of an individual's behaviour patterns could impact on the way an individual actually behaves; 5. The possibility of remaining anonymous and preserving one's privacy in the IoT will become increasingly difficult; and 6. Device manufacturers will need to balance battery efficiency and device security to prevent the IoT becoming a potential privacy and information security target. The opinion also considers the extent to which the existing EU law addresses these issues and makes some recommendations to facilitate the application of EU legal requirements to the IoT. **The opinion is available here.**
17 September 2014	**WP29 Statement on the results of the last JHA meeting** The WP29 broadly welcomes the general approach reached by the EU Council on specific aspects of the draft data protection regulation at the Justice and Home Affairs (JHA) meeting. The WP29's views on the general approach are summarised below: 1. The provisions regarding territorial scope clarify the point and underline the need to broadly ensure the application of EU rules on controllers that are processing personal data of EU data subjects but are not established in the EU. However, the WP29 highlights the necessity for covering non-EU processors when the processing targets an EU citizen, as proposed by European Parliament. 2. The WP29 broadly agrees with the approach taken by the EU Council with regards to "Transfers of Personal Data to Third Countries or International Organisations" (Chapter V). However the WP29 suggests an amendment to the application of Binding Corporate Rules and the introduction of new tools for transfers. **The statement 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)**

28 July 2014	Reactiv Media Limited ('RML') trading as Discover Finance Consumer Helpline	Monetary Penalty Notice	The Commissioner found that, in breach of regulation 21 PECR, RML had made 601 unsolicited marketing calls to consumers whose numbers were listed on the TPS 'do not call' list. The recipients had not given prior consent to RML to receive calls.	A monetary penalty notice of £50,000, to be paid by 27 August 2014.
5 August 2014	1st Choice Properties (SRAL)	Prosecution	1st Choice Properties (SARL), a property lettings and management company, has been prosecuted for failing to notify with the ICO, as required under section 17 of the Act.	£500 fine, £815.08 costs and £50 victim surcharge.
6 August 2014	A Plus Recruitment Limited	Prosecution	A Plus Recruitment Limited, a recruitment company, has been prosecuted for failing to notify with ICO, as required by section 17 of the Act. The defendant pleaded guilty.	£300 fine, £489.95 costs and £30 victim surcharge.
13 August 2014	Wokingham Borough Council ('WBC')	Follow-up review of undertaking (originally signed April 2014)	The Commissioner found that WBC had addressed some requirements of the undertaking (for example, data protection and information security training has been implemented and guidance on transporting paper documents has been created), however, further steps are needed to implement a 'refresher training structure'.	WBC must provide staff training in data protection and information security every two years, at least.
22 August 2014	Dalvinder Singh	Prosecution	Mr Singh was employed by Santander UK and worked in the suspicious activity reporting unit. Mr Singh had access to customer accounts, as part of his role involved investigating money laundering allegations. Despite receiving clear data protection training from Santander UK, Mr Singh used his access to view the accounts of 11 of his colleagues, checking their salaries and bonuses, contrary to s 55 DPA 1998. Under s 55 DPA 1998, unlawfully obtaining or accessing personal data is a criminal offence.	£880 fine, £440 costs and £88 victim surcharge.

26 August 2014	Ministry of Justice ('MoJ')	Monetary Penalty notice	The National Offender Management Service is part-of the MoJ, and responsible for Prison and Probation Services across England and Wales. A portable hard drive used to back up the prisoner intelligence database went missing from a prison's Security Department. The hard drive contained highly sensitive personal data relating to 2,935 prisoners. The hard drive was not password protected or encrypted. The hard drive has not been recovered, but there is no evidence that the content has been circulated.	A monetary penalty notice of £180,000, to be paid by 22 September 2014.
28 August 2014	Racing Post ('RP')	An undertaking to comply with the seventh data protection principle (Part 1 of Schedule 1 of the Act)	In October 2013, the RP website was targeted by an attacker who managed to gain access to a customer database containing the details of 677,335 individuals. No financial information was contained in the database, but data included name, address, password, date of birth and telephone number. Vulnerabilities in the RP website code had made the attack possible. RP had also failed to ensure that up-to-date security patches were in place and there was no regular security testing. The Commissioner felt that the data was at an unacceptable level of risk of inappropriate processing.	RP must, by 28 February 2015: 1. Implement appropriate periodic security testing; 2. Implement an appropriate and secure method of password storage; 3. Define and implement an appropriate software updates policy (which must require software to be supported by security updates); and 4. Ensure that compliance with RP's policies on data protection and information security is monitored.

3 September 2014	Winchester and Deakin Limited trading as Rapid Legal and Scarlet Reclaim ('W&D')	Enforcement Notice	The Commissioner received numerous complaints from individuals directly and via the TPS regarding unsolicited direct marketing calls from W&D. The complainants had previously registered their telephone number with the TPS or had notified W&D that they did not wish to receive calls.	W&D must, within 35 days of the date of the notice: 1. Neither use nor instigate use of a public electronic communications service to make unsolicited direct marketing calls to: (a) A subscriber who has previously notified W&D 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 has not notified W&D that they do not object to such calls. 2. Cease sending marketing communications that do not identify W&D as the sender.
8 September 2014	All Claims Marketing Limited ('ACM')	Enforcement Notice	In April and May 2014, the Commissioner received 3,488 complaints from individuals alleging to have received unsolicited marketing via text message. The Commissioner found that these messages were sent or instigated by ACM. The Commissioner was also informed that 5,781,000 unsolicited marketing messages were sent or instigated by ACM during that time.	ACM must, within 35 days of the date of the notice: 1. Not transmit unsolicited direct marketing communications by electronic mail, without the recipient's consent. 2. Not transmit a marketing communication by electronic mail unless ACM is clearly identified in the communication as the sender.

9 September 2014	Isle of Scilly Council (the 'Council')	An undertaking to comply with the seventh data protection principle (Part 1 of Schedule 1 of the Act)	In June 2013 a document containing information relating to a disciplinary hearing and third parties (not redacted) was attached, in error, to an email sent to the employee subject to the disciplinary hearing and their union representative. The Commissioner learned of another incident at the Council, involving disclosure of two documents containing sensitive personal data. The documents were, initially, disclosed to authorised persons, however, weak security mechanisms surrounding document-sharing resulted in the documents being circulated publicly.	The Council must: 1. Implement and enforce mandatory data protection training, with completion to be recorded and monitored; 2. Establish a refresher programme to ensure that data protection training is updated at regular intervals, with completion to be recorded and monitored; 3. Draft and communicate to staff appropriate guidance on safe transfer of personal data by email (where appropriate, use of an encryption platform to protect electronic information should be considered); 4. Implement a policy on application of redactions; and 5. Monitor compliance with policies on data protection and IT Security.
9 September 2014	James Pickles	Prosecution	Mr Pickles was a paralegal employed by a firm of solicitors in Yorkshire. In the weeks before he left the firm, Mr Pickles sent himself six emails containing workload lists, template documents and file notes containing the sensitive information of over 100 people, hoping to use the information in his new role. Under s 55 DPA 1998, unlawfully obtaining or accessing personal data is a criminal offence.	£300 fine, £438.63 costs and £30 victim surcharge.

22 September 2014	Oxford Health NHS Foundation Trust (the 'Trust')	An undertaking to comply with the seventh data protection principle (Part 1 of Schedule 1 of the Act)	In May 2013 it was reported that a file containing the personal data of 4,200 registered website users was unintentionally placed on the internet. The file, containing email addresses, usernames, passwords and billing addresses, had been created to transfer user information to the new website Oxford Centre for Cognitive Therapy website. The website was developed by a third party. Although some of the mistake was attributable to human error, there were other means by which the data could have been securely provided from the old website developer to the new. It was also found that there was no contract in place between the Trust and the processor at the time of the incident. The Commissioner also learnt that, in January 2013, a letter containing mental health information of an individual was sent to an incorrect address.	The Trust must ensure that: 1. Adequate data processor contracts are in place, which include data protection provisions and are consistent with internal standards; 2. A procedure is introduced to conduct appropriate due diligence checks when selecting data processors (by 31 March 2015); 3. Appropriate information governance and IT oversight is in place and a privacy impact assessment process (by 31 March 2015); and 4. A breach management plan is implemented (by 31 March 2015). Steps taken will be recorded to assess ongoing risk.

25 September 2014	Norfolk Community Health & Care NHS Trust (the 'Trust')	Undertaking to comply with the First, Third and Seventh data protection principle	The Trust provided an IT support service to a referral management centre ('RMC'). Towards the end of the contract, the RMC requested an electronic copy of a patient database, to aid transition to a new service provider. In the process of sharing this database, the Trust inadvertently shared additional data with the RMC, which had not been requested and was not required. It transpired that the RMC had been given a backup file belonging to a third party, containing a dataset relating to 128,842 data subjects. Some of the data involved related to health and were, therefore, sensitive data. The Commissioner found that a contractual arrangement between the Trust and the RMC was in place, but no data sharing agreement or guidance for staff compiling such data sets existed. This lead to the Trust disclosing the incorrect data set.	The Trust must ensure that: 1. A departmental procedure governing compilation and transfer of data to third parties is implemented and periodically reviewed. Staff should be appropriately trained on how to follow the procedure by 28 February 2015; 2. Staff are aware, on an ongoing basis, of requirements of existing data protection policies/procedures; 3. Appropriate third party information sharing agreements are in place and a register of these agreements is maintained and reviewed, by 28 February 2015; and 4. Contractual arrangements contain safeguards on management and protection of data (especially at the commencement and end of the contractual period) by 28 February 2015.