Date	Description
UK	
Cases	
7 October 2016	***Andrea Brown v Commissioner of Police for the Metropolis and Chief Constable of Greater Manchester Police [2016] Claim Nos. 3YM09078 & A53YP250*** **(CC at Central London)** **Summary** On 7 October 2016, HHJ Luba QC, sitting in the County Court at Central London, handed down a judgment on remedy whereby he ordered the payment of damages for breaches of the Data Protection Act 1998 ("DPA") and the Human Rights Act 1998 ("HRA"), and for the tort of misuse of private information as a result of the unauthorised disclosure and use of the Claimant's personal data, and of information concerning her, by the Metropolitan Police Service ("MPS") and Greater Manchester Police ("GMP"). The assessment of damages in this case is notable. Firstly, because of HHJ Luba QC's global, as opposed to separate, assessment in order to ensure that *"there is no 'double-counting' or overlap of HRA damages with awards of damages made under different causes of action"*, and on the basis that *"the same facts and matters sustain the claims in each of the respects on which they have succeeded..."*. Secondly, because of HHJ Luba QC's assessment of the extent of the Claimant's distress, and emphasis of the point made by LJ Arden in *Gulati & Ors v MGN Limited [2015] EWCA Civ 1291* that *"in addition to compensating for distress, the award of general damages should embrace compensation for the fact that the Claimant has lost control of personal information"*. **Facts** The claimant, Andrea Brown, was an officer in the Metropolitan Police Service ("MPS") until her resignation in November 2013. In December 2011, she travelled to Barbados with her daughter while on sick leave, without first informing her line manager of her travel plans. Her actions were considered a breach of police service procedures in relation to 'absence management'. Airlines provide information to the National Border Targeting Centre (“NBTC”) in relation to passengers travelling to and from the UK by air, which is then stored on a database. Greater Manchester Police ("GMP") manages policing operations at the NBTC. A senior MPS officer submitted a request for information to the NBTC, with the aim of gathering evidence for a potential disciplinary procedure involving Ms Brown. A GMP officer provided the information requested, including personal details about the claimant and her daughter. The MPS officer then made a further request for information relating to the claimant's specific travel arrangements in Barbados, and the airline with which she had travelled duly provided this information. The MPS ultimately found that Ms Brown had a "case to answer", but that it would only take

Date	Description
	"informal management action". Ms Brown then took action against the MPS, arguing that it had misused its data and information gathering capacities which, should only be used for the detection or prevention of crime, not employment disciplinary matters. She also asserted that GMP should not have provided the information, given the basis on which it had been requested. Both defendants admitted liability – i.e. that this was an unauthorised disclosure and the use of the claimant's personal data was a breach of the DPA and the Human Rights Act 1998 ("HRA"). **Judgment** HHJ Luba QC considered potential remedies for: (a) breaches of the DPA (which was conceded by the Defendants); (b) breaches of the HRA (which was conceded by the Defendants); and (c) the tortious interference with the right to privacy/ misuse of private information (which was made out on the facts). Following a global assessment of remedies for all such breaches, HHJ Luba QC awarded £9,000 in damages, to be apportioned between the Defendants as 2/3: 1/3, reflecting *"primary responsibility as laying with the MPS and the fact that it made two disclosure requests, only one of which concerned GMP"*. This award was made on the following bases: 1. *"Compensating for the shock, distress and upset caused by the discovery that a person's personal information or data (and some material relating to their child) has been wrongly accessed and disseminated cannot be an exact science"*; 2. As noted above, HHJ Luba QC agreed with the point made in the case of *Gulati* that *"in addition to compensating for distress, the award of general damages should embrace compensation for the fact that the Claimant has lost control of personal information";* 3. In considering various competing factors, among other things, HHJ Luba QC cited that, on the one hand, *"of the two Defendants…one was the Claimant's own employer…and both were police forces which might have been expected to know and obey relevant legal requirements rather than transgress them"*, and on the other, *"the Court is not dealing with the wide dissemination of highly sensitive or highly personal information for profit or gain…";* 4. HHJ Luba QC distinguished the court's finding in *Gulati* that, *"the starting point for general hacking was £10,000 for each year of serious levels of hacking",* on the basis of the latter point made in paragraph 3: *"Gulati was concerned with carefully organised and frequently repeated hacking of highly*

Date	Description
	personal and sensitive information for gain"; and 5. This being said, the judge agreed that the award must be substantial: despite not mirroring the facts of *Gulati, "the personal information disclosed…was wrongly sought, obtained and disclosed by state authorities…and the Claimant did lose control over her personal information…"* **The full judgment is available here.**
19 October 2016	***R (on the application of Ingenious Media Holdings plc and another) (Appellants) v Commissioners for Her Majesty's Revenue and Customs (Respondent)* [2016] UKSC 54** **Summary** HMRC is subject to a statutory duty to keep taxpayer information confidential. A senior HMRC official leaked information to the press. The case concluded (i.a.) that disclosure of confidential information, 'in confidence', is still a breach of confidence. The rest of the case is specific to revenue confidentiality legislation, but this point may have general relevance to the law of confidence. On 19 October 2016, the Supreme Court ("SC") overturned the Court of Appeal's ("CA") decision that disclosure of information about an individual taxpayer by the former Permanent Secretary for Tax at the HMRC – Mr David Hartnett – to *The Times* journalists was justified under Section 18 (2) (a) of the Commissioners for Revenue and Customs Act 2005 (the "Act"). It, therefore, allowed the applicants' appeal against the decisions of the lower courts dismissing their claim for a judicial review of Mr Hartnett's decision to so disclose this information. **Facts** On 14 June 2012, Mr Hartnett gave an 'off the record' interview to two *The Times* journalists about tax avoidance. More specifically, this case concerns the discussion they had about film investment schemes involving film production partnerships. Among other things, Mr Hartnett provided the journalists with information about the tax activities of Mr Patrick McKenna, who devised such schemes and utilised their associated tax relief, and Ingenious Media Holdings plc ("Ingenious"), of which Mr McKenna is the founder and CEO. Mr Hartnett gave the following reasons for disclosure: i. It was in the interests of HMRC to *"establish good relations with the financial press"*; ii. Newspaper publication was an effective means of conveying HMRC's views on *"elaborate tax avoidance*

Date	Description
	schemes"; and iii. The journalists may have had information which was useful to HMRC. Ingenious and Mr McKenna brought an application for the judicial review of Mr Hartnett's decision to disclose information about their tax activities to *The Times*. Both Sales J at first instance and the CA were reluctant to approach Mr Hartnett's decision as if they were the 'primary decision makers', dismissing the application. **Judgment** The SC decided the three main issues as follows: i. **Interpretation of disclosure permitted under section 18 (2) (a) of the Act and, in particular, the definition of 'function' under section 18 (2) (a) (i):** Section 18 (2) (a) permits disclosure by HMRC officials of information held in connection with a function of HMRC if such disclosure is *"made for the purposes of a function of"* HMRC. Lord Toulson interpreted 'function' narrowly and stated that, *"I take section 18 (1) to be intended to reflect the ordinary principle of taxpayer confidentiality…* [i.e. that stated in the case of *Marcel v Commissioner of Police of the Metropolis* [1992] Ch 225] *to which section 18 (2) (a) (i) creates an exception by permitting disclosure to the extent reasonably necessary for HMRC to fulfil its primary function"* i.e. the collection and management of revenue only. ii. **The courts' approach to reviewing HMRC's conduct:** Here, Lord Toulson disagreed with the decision of the lower courts, *"that it was not for them to approach the disclosures made by Mr Hartnett as if they were the primary decision makers…the question of breach of confidentiality is one for the court's judgment"*. iii. **'Off the record' interview:** The message was clear from Lord Toulson – *"…an impermissible disclosure of confidential information is no less impermissible just because the information is passed on in confidence…"* **The full judgment is available here.**
20 October 2016	***Norman, R v* [2016] EWCA Crim 1564** **Summary** The Article 10 rights of a journalistic source under the European Convention on Human Rights ("ECHR") are likely not engaged where a media corporation discloses the identity of said source to the police. Even if the source's Article 10 rights are engaged, if the source has committed a criminal offence by disclosing information, the right can be interfered with

Date	Description
	and the media corporation is under no obligation to protect the source's identity. **Facts** This case was an appeal by Robert Norman (the "Appellant"), a former prison officer, against his conviction for misconduct in a public office. The criminal conviction related to the corrupt relationship between the Appellant and the tabloid journalist Stephen Moyes, who was working during the period of this relationship for the Daily Mirror and subsequently News of the World. Both newspapers had paid the Appellant sums totalling around £10,000 in return for information supplied to Mr Moyes about the prison, which formed the subject matter of numerous published articles. The information included stories about named high-profile prisoners and bad practices within the prison. Before the Court of Appeal, the Appellant argued that the original criminal proceedings against him were an abuse of process. This was on the ground that the police had applied improper pressure to the newspapers in order to obtain from them the Appellant's identity, and the material which was used to bring the proceedings against him. The Appellant argued further that this was a violation of Article 10 of the ECHR. **Judgment** Sitting in the Court of Appeal, Lord Thomas CJ, Popplewell J and Goss J found that the newspapers had voluntarily agreed to assist the police with their investigation, and therefore that no improper pressure was used by the police to obtain the Appellant's identity and the materials used to bring proceedings against him. The Court also found that the Appellant's Article 10 rights had not been interfered with: • The Court found that it was doubtful whether Article 10 rights were engaged at all in the case of a source whose identity is voluntarily disclosed by a newspaper. Although Article 10 protects the right of journalists to withhold journalistic material from the police, the Court found that under European law, journalists are under no obligation to do so unless such an obligation is imposed by national legislation. There are no UK laws imposing such an obligation on journalists; • Even if the Article 10(1) right was engaged, it is a qualified right under Article 10(2) and thus would not protect the Appellant in these circumstances. This is because the Appellant had committed a criminal offence (misconduct in a public office). This meant that the revelation of his wrongdoing was necessary and proportionate for the important public interest of prosecuting a crime and the right could be interfered with on this basis.

Date	Description
	Analysis The Court acknowledged that different considerations may arise in the case of a 'genuine whistleblower' seeking to act in the public interest *"where the only wrongdoing might lie in a breach of obligations to the employer rather than the circumstances of the communication to the journalist."* However, given that some of the information disclosed by the Appellant to Stephen Moyes covered stories such as the consequences of prison cuts in conjunction with increased prisoner numbers, suicides within the prison and the misconduct of prison officers, the distinction between a 'genuine whistleblower' making a disclosure in the public interest and an individual whose disclosure constitutes a criminal offence may be difficult to make in practice. Media corporations will need to find effective ways of making this distinction in order to ensure that any co-operation with the police does not constitute a breach of a source's Article 10 rights. **The full judgment is available here.**
Other News	
December 2016	**UK Government publishes review of UK cyber security landscape** In December 2016, the Government published its conclusions of a review (*'Cyber Security Regulation and Incentives Review'*) of the adequacy of the current UK cyber security landscape in the context of the wider economy (i.e. not essential service sector-specific). The headline to take from this report is that it seems very likely that the UK will implement the Network and Information Security (NIS) Directive notwithstanding the result of the 23 June 2016 referendum, stating that *"[whilst the] Government is separately considering whether additional regulation might be necessary for critical sectors, including in the context of the NIS Directive due to be implemented in 2018 as well as wider national infrastructure considerations…The detailed scope and security requirements for NIS implementation will be set out by Government in 2017, informed by the work of the NCSC and lead Government departments with relevant sectors alongside broader Government consideration of critical infrastructure"*. This being said, the focus of this report was essentially whether the Government needed to introduce additional regulation above that which will be imposed on businesses (generally) under the General Data Protection Regulation ("**GDPR**") when it comes into force on 25 May 2018. The Government's conclusion is clear: *"For now, Government will not seek to pursue further general cyber security regulation for the wider economy over and above the GDPR. It should ultimately be for organisations to manage their own risk in respect of their own sensitive data (e.g. intellectual property) and online presence"*. The Government states that there is a *"strong justification for regulation to secure personal data as there is a clear public interest in protecting citizens from crime and other harm, where it may not otherwise be in organisations' commercial interests to do so"*. However, it reserves its role to improving/ enhancing this protection by means of its implementation of the GDPR. The reasons for not adding to the GDPR's red-tape are as follows:

Date	Description
	1. It is satisfied that both the data breach notification obligations which will be imposed on both controllers and processors, and the *"aggravating and mitigating factors affecting the size of fines imposed for cyber security-related breaches"*, under the GDPR are sufficient means of effectively incentivising *"organisations to adopt good cyber security practices"*. 2. Various measures will be implemented in due course which are designed to connect the field of data protection with the field of cyber security, for example, the collaboration of the ICO and the National Cyber Security Centre on relevant projects. 3. Government intervention must be proportionate: *"It does not want to overburden businesses and organisations with unnecessary regulatory requirements"*. This does not mean that businesses should become complacent: in addition to beginning to devise and implement data breach detection and notification procedures and policies, they must devise and implement *"formal incident response plans to deal with hackers and the consequences"* i.e. procedures dealing with the full 'life cycle' of a breach and its consequences **The review is available here.**
EU	
European Commission	
10 January 2017	**European Commission publishes proposed draft e-Privacy Regulation text** **More information is available here.**
A29WP	
13 December 2016	**Article 29 Working Party publishes data portability guidelines** Guidance on the right to data portability was issued by the Article 29 Working Party in December 2016 (WP242). The guidance tackles some of the uncertainties posed by the right: • What data does it apply to? (*unsurprisingly the Working Party suggests a broad interpretation*) • To what extent does the service provider have to build inter-operable and compatible systems? (*inter-operability*

Date	Description
	is encouraged but not a hard-law requirement; compatibility is not required) • Does a service provider have a responsibility to ensure how the data will be used? (*no*) **Data portability extends subject access and makes data more usable for individuals** Data controllers already have to tell individuals what data they process about an individual and (in most member states) to provide a copy of that data to the individual. The General Data Protection Regulation strengthens the access right – if an individual makes a request electronically, the data has to be provided in a commonly used electronic format. Portability is a stronger right: it is a right for the individual to receive the data in a commonly used, machine-readable format. This extended right will allow the individual to make more use of the data, allowing them to switch service providers more easily for example. The individual can either require the service provider to provide data to them, or direct to another provider. **Data portability applies to a narrower set of data than subject access** Whereas subject access rights apply to all personal data, portability applies to a narrower set of data. Data portability applies to personal data concerning the data subject: • Which is processed automatically (so not paper records) • Which is provided by the individual • Which is processed based on consent or pursuant to a contract with the individual WP 242 gives examples of occasions when portability would apply: data held by a music streaming service; titles of books held by an online bookstore; data collected from a smart-meter; emails held by an email service provider. Portability raises many tricky questions. Predictably, the approach of the Article 29 Working Party is to answer these in ways which maximise the usefulness of the right to the data subject making the portability request. **What if the data relates to more than one person?** One tricky question is what to do if the data requested relates to the person making the request and to others as well: emails relate to sender and recipient; bank details relate to payer and payee; information in a social media account

Date	Description
	relates both to the individual and to their friends and connections. WP242 suggests that the fact that the data relates to multiple individuals does not stop it all being data which concerns the person making the request: all such data should be provided. However, helpfully, the Working Party states that the original service provider is not responsible for ensuring that the new provider, or the person making the request, respects the data protection rights of these individuals. This is a matter for the new provider, who is independently obliged to comply with data protection law. The Working Party suggests that this limits the new provider to processing data to deliver a service to the data subject who has ported the data – it would not, for example, be able to use data about friends or contacts for direct marketing purposes. The Working Party does, however, consider that the original provider is responsible for the security of the data whilst it is being ported to the data subject or the new provider. **What does 'data provided by the individual' mean?** Where a user has an email account, is the data that person provides to the email service provider just the account opening information and emails they send – or does it also include emails sent to the individual? On a literal reading, emails sent to the data subject are not data provided 'by' that individual to the email service provider. This makes portability of little use. A more purposive interpretation would be that, as the individual has chosen to use this provider, they have authorised the provider to receive this information on their behalf, so that this is all information provided by the individual. The Working Party takes this broader approach. 'Provided by' includes data actively and knowingly provided by the individual (e.g. in filling a form). It also includes observed data which is 'provided' by the individual in a more purposive interpretation – this includes search history, traffic and location data and information learnt from fitness trackers. Data which the service provider infers from this data – for example, personalisation or recommendations, or profiles – are not 'provided by' the individual. A distinction between data which is directly provided or collected and subsequent inferences is drawn. **Portability could extend to meta data – but need not include all data in an organisation's systems relating to the data subject** The Working Party notes that a data controller should consider what data the data subject needs to receive to meet GDPR's objective - of allowing users to move data more easily from one service to another.

Date	Description
	This could mean that metadata has to be provided (so not just emails sent and received – but also timestamp information; information about whether emails have been opened etc.). However, passwords would not have to be ported. Payment information would also not be covered. **Limits to portability** GDPR provides that portability '*shall not adversely affect the rights and freedoms of others*'. Businesses also have rights – including rights to protect trade secrets and intellectual property rights. The WP acknowledges that portability should not grant individuals rights to misuse information in an unfair way. However, GDPR provides that these rights should not result in '*a refusal to provide all information to the data subject*'. Further the WP notes that a perceived potential business risk does not justify companies refusing to provide portability. The Working Party suggests that the answer could be to provide information in a form that does not release information covered by trade secrets or IPRs. This may help in some situations. However, the form in which the information is stored may not be the most likely area where IPRs or trade secrets are relevant. For example, in some cases, the actual questions asked by the provider and so the data fields collected (when taken over a large number of data subjects and where they vary by data subject) may be where the innovation and trade secret applies. The paper only gives 2 short paragraphs to considering this issue: more thought is needed here. **Best practice guidance** The Working Party also makes a number of recommendations for organisations – all from the perspective of ensuring that portability is more useful for individuals or minimises risks to third parties whose data is swept up in a portability request. These include: • Development of interoperable formats • Development of APIs to allow easy porting from one provider to another • Explaining to individuals the differences between the data available to them as part of an access request and a portability request • Providing portals or tools, to allow individuals to select data for porting and to exclude data about others • Tools to obtain consent from others whose data are included in a portability request

Date	Description
	You can find the guidelines here.
13 December 2016	**Article 29 Working Party publishes lead supervisory authority guidelines** The Article 29 Working Party adopted guidelines for identifying a controller or processor's lead supervisory authority and related FAQs on 13 December 2016 (the "**Guidelines**"). Identifying a lead supervisory authority is only relevant where a controller or processor is carrying out the *"cross-border processing of personal data"* (defined in Article 4(23) GDPR). This is the case where: (i) the processing of personal data takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (ii) the processing of personal data takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State. The Guidelines consider what is meant by *"substantially affects or is likely to substantially affect data subjects"*. The A29WP states that this will be considered on a case by case basis, taking into account the context of the processing, the type of data, the purpose of the processing and a range of other factors, including (among other things) whether the processing causes, or is likely to cause, damage, loss or distress to individuals, whether the processing affects, or is likely to affect individuals' health, well-being or peace of mind and whether the processing creates embarrassment or other negative outcomes, including reputational damage. The A29WP provides guidance on how to identify the lead authority in three scenarios: (i) where the cross border processing involves a controller; (ii) where the cross border processing involves a controller and a processor; and (iii) where the cross border processing involves a processor. Where the processing only involves a controller and the controller has a single establishment in the EU, the lead supervisory authority is the supervisory authority of the place of that single establishment. Where an organisation has several establishments in the EU, the lead authority will be the supervisory authority of the country where the place of central administration in the EU is located, unless the decisions on purposes and means of the processing are taken in another establishment in the EU. The A29WP asks organisations to consider if there are other establishments: (i) where decisions about business activities that involve data processing are made; (ii) where the power to have decisions implemented effectively lie; (iii) where director(s) with overall management responsibility for the cross-border processing activity are located; and (iv) where the controller is registered as a company, if in a single territory. The A29WP recognises that there can be situations where more than one lead authority can be identified, i.e. in cases where a multinational company decides to have separate decision making centres, in different countries, for different

Date	Description
	processing activities. The Guidelines state that *"the GDPR does not permit 'forum shopping'"* – there must be an effective and real exercise of management activity in the member state identified as the organisation's main establishment. Organisations should be able to demonstrate to supervisory authorities where decisions about data processing are actually taken and implemented, as they may be asked to evidence their position. The A29WP emphasises informal cooperation between lead and concerned supervisory authorities to reach a mutually acceptable course of action, noting that the formal consistency mechanism should only be invoked where co-operation does not reach a mutually acceptable outcome. **You can find the guidelines here.**
16 December 2016	**Article 29 Working Party publishes guidance on DPO provisions of the GDPR** In February 2016, as part of its action plan of activities for the implementation of the General Data Protection Regulation ("**GDPR**"), the Article 29 Working Party ("**A29WP**") promised to publish guidance on the operation of the GDPR's provisions regarding the requirement for controllers and processors to appoint a Data Protection Officer ("DPO"). That guidance was published on 16th December – a copy is available **here** (the "**Guidance**"). Some of the key points raised by the A29WP in its Guidance are as follows: 1. ***When is a DPO appointment obligatory?*** – The Guidance unpacks some of the GDPR's terminology so it is worth starting with a reminder about when the Regulation says that a DPO appointment is obligatory. Three scenarios are mentioned (and the Guidance goes on to summarise what the words in bold/italics below mean), namely where: i. Processing is carried out by a ***public authority*** (other than certain courts); ii. The ***core activities*** of a controller or processor consist of processing which require: a) ***regular and systematic monitoring*** of individuals on a ***large scale*** given their nature, scope, and/or purpose; or b) ***large scale*** processing of sensitive data or criminal records; or iii. A Member State's law requires a DPO to be appointed (likely in countries such as Germany).

Date	Description

- ***"Public authority":*** The Guidance says that each Member State's laws should define what constitutes a public authority, and also that bodies which are subject to public law should also fall within this definition. So providers of utility services, transport infrastructure and public broadcasting services in many countries are likely to have to appoint a DPO under the GDPR.

- ***"Core activities":*** Activities which are '*an inextricable part*' of the controller's/ processor's pursuit of its goals are cited. Reassuringly the Guidance confirms that a company's processing of staff information (which will inevitably include sensitive data) is ancillary to its activities, not core. Examples of core activities given include, a security company's surveillance where it is hired to safeguard a public space, a hospital's processing of patient health data and an outsourced provider of occupational health services processing of employee data.

- ***"Regular and systematic monitoring":*** All forms of on-line tracking and profiling are called out as examples, including for the purpose of behavioural advertising and email retargeting. Other interesting examples cited include: scoring (e.g. for credit scoring, fraud prevention or for the setting of insurance premiums); location tracking; fitness and health data tracking; CCTV; and processing by connected devices (smart meters, smart cars etc.).

- ***"Large scale":*** The A29WP is not currently keen on precise numbers being used as a benchmark for this term, although the Guidance notes that plans are afoot to publish thresholds. Instead the Guidance lists some fairly obvious factors to be considered in defining large scale (e.g. the number of individuals affected and geographic extent of processing). Examples of large scale processing cited include: a bank or insurance company processing customer data; and processing of an international fast food chain's customer geo-location data in real time for statistical purposes by a specialist processor.

2. ***What about voluntary DPO appointments*** – The A29WP encourage these, although given the prescriptive nature of the requirements for the DPO role which the Guidance sets out (summarised below) it remains to be seen how comfortable organisations will be to follow this lead. The Guidance confirms that where a DPO is appointed on a voluntary basis the same requirements as set by the GDPR to mandatory DPO's will apply to them (e.g. regarding independence, freedom from unfair dismissal, obligation to publish their contact details etc.). Interestingly, the Guidance recommends that an organisation which decides not to voluntarily appoint a GDPR DPO documents why it think that it is not subject to the mandatory DPO appointment criteria (as summarised above).

3. ***Will DPOs be personally liable if their organisation fails to comply with the GDPR?*** – No. The Guidance is clear on this point. Controller and processor organisations are obliged to ensure that they comply with

Date	Description
	the GDPR not individual DPOs. 4. ***Can an external DPO be appointed?*** – Yes, so long as the GDPR's requirements including regarding impartiality, knowledge of the organisation to which the DPO is appointed and accessibility are met. The Guidance stresses that the terms of an external DPO's appointment should be clearly laid out in a service contract and that the external DPO's title, status, position and tasks be clearly agreed. 5. ***Can a group of companies appoint a single DPO?*** – Yes, again so long as the GDPR's requirements mentioned at 4) are met. The Guidance makes an interesting point in relation to accessibility. DPO's are required to be accessible to data subjects and regulators. The Guidance makes the point that this is will not be possible unless the DPO can communicate in the languages which the data subjects (for instance customers and staff) and regulators which the organisations which he/she represents are likely to speak. It seems that the A29WP expect DPOs in multi-national groups to be data protection experts and multi-linguists (or at least to have access to good translation mechanisms). 6. ***What skillsets are required of a DPO?*** – The Guidance repeats the list included within the GDPR (e.g. expert knowledge of data protection laws and practices). Interestingly it notes that a higher level of expertise is required the more complex and/ or sensitive the personal data which is processed by the organisation, or the greater the volume of data processed. 7. ***Publication of the DPO's contact details*** – This is required by the GDPR. The Guidance clarifies that the name of the DPO does not need to be made publicly available but that it should be published to all relevant regulatory authorities and members of staff. Other members of the public need only to be given sufficient information to enable communications to easily reach the DPO, e.g. a dedicated email address published on a website. 8. ***The DPO's role*** – The A29WP stress that organisations which appoint a DPO must ensure that the DPO is involved in all issues relating to data protection at the earliest stage and that the DPO's primary concern should be enabling GDPR compliance of the organisation. In so doing the DPO must be involved in key decisions (access to senior management is mentioned) and be given necessary resources (including support, budget, facilities and training). If a security breach occurs the Guidance says that the DPO must be promptly consulted. 9. ***What if management disagree with the DPO?*** – The Guidance states that no instruction must be given to the DPO regarding how to deal with a matter, what results should be achieved or whether or not to consult with a regulatory authority. As a matter of good practice, should management disagree with a DPO then the reasons for not following the DPO's advice should be documented. DPOs should not be dismissed or penalised (including indirectly via, for instance, prevention of career development) for performing their tasks – to do so would constitute a breach

Date	Description
	of the GDPR. 10. ***What about conflicts of interest?*** – The GDPR does not restrict DPOs from holding other posts but expressly requires that organisations ensure that such other tasks do not give rise to a conflict of interest for the DPO. The Guidance goes further and states that a DPO cannot hold a position which leads him/her to *"determine the purposes and the means of the processing of personal data"*. It remains to be seen whether regulators feel that CISOs or CIOs can perform the DPO role.
Cases	
21 December 2016	**Joined Cases *Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v Watson, Brice, Lewis*** On 21 December 2016, the ECJ delivered its judgment in this case. **A summary of the decision 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)**
11 November 2016	**An historical society**	Monetary penalty	An administrative officer who worked for an historical society (the "Society") (name and other details redacted) left a laptop in a location from which it was then stolen. The laptop was unencrypted and never recovered, despite the theft having been reported to police. The purpose of the laptop was to allow the officer to transfer details of artefacts from a paper ledger to digital format. Among other things, the laptop contained a list of individuals who had donated or loaned artefacts to the Society.	Monetary penalty notice of £500.
11 November 2016	**Kayleigh Billington & Lesley Severs**	Prosecution	Kayleigh Billington and Lesley Severs pleaded guilty to offences under section 55 Data Protection Act. At the time of the offences, the pair worked at a claims management company, UK Claims Organisation Ltd. They obtained their initial data unlawfully from a car hire company and used this data as leads in order to try to "blag" insurance companies into giving them further information. This information they then sold on to solicitors as personal injury claims.	Kayleigh Billington: £320 fine, £250 costs, £20 victim surcharge Lesley Severs: £250 fine, £400 costs, £20 victim surcharge
15 November 2016	**London Borough of Ealing**	Undertaking	The London Borough of Ealing (the "Borough") has signed an undertaking committing it to ensure that personal data are processed in accordance with the First Data Protection Principle in Part I	The Borough shall, as from the date of the Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are

of Schedule 1 to the Act.

In February 2016, a Social Worker, after attending court for care proceedings, placed an envelope containing important documents relating to the proceedings on the top of her car. She then drove off. On arriving home, she realised that she did not have the envelope. Having returned to the car park where she lost the envelope, she was not able to locate it, and further enquiries came to nothing. The envelope was never recovered.

Previously, between 13 and 15 May 2013, the ICO conducted an audit of the Borough's data protection compliance. A lack of periodic data protection refresher training was highlighted. A follow-up audit was conducted in 2014. Following consideration of the remedial action taken in light of these audits and in lieu of the ICO exercising its powers to serve an Enforcement Notice, the Borough has agreed to sign an undertaking.

processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular:

- the Borough shall continue to work towards achieving their stated target for 100% completion of mandatory online data protection refresher training for all permanent, locum and temporary Social Care staff by 3 April 2017;

- the Borough shall record and monitor initial and refresher data protection training for non-permanent staff employed in all other council departments;

- the Borough shall ensure that the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher DP related training;

- the Borough shall ensure that the report recommendations by LBE Management Investigation are progressed; and

- the Borough shall implement other security measures as appropriate to ensure that personal data are protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

23 November 2016	**Key Insolvency Services Limited**	Enforcement notice	Key Insolvency Services Limited (the "Company") sent 136 unsolicited communications by SMS to individual subscribers between 24 November 2015 and 2 April 2016. The messages were sent by Key Lead Solutions Ltd, which did so on behalf of the Company. It is believed that many more messages may have been sent.	The Company shall, within 35 days of the Notice: • except in the circumstance referred to in paragraph (3) of Regulation 22 of PECR, neither transmit, nor instigate the transmission of, unsolicited communications for the purpose of direct marketing by means of electronic mail, unless the recipient of the electronic mail has previously notified the Company that he or she consents for the time being to such communication being sent by, or at the instigation of the Company.
29 November 2016	**Silver City Tech Limited**	Enforcement notice & monetary penalty	Silver City Tech Limited (the "Company") was found to have instigated the sending, via third parties, of 3,074,331 unsolicited communications by SMS between 11 November 2015 and 16 April 2016. The ICO found that the Company did not have the consent of the subscribers to whom the messages were sent.	The Company shall, within 35 days of the Notice: • except in the circumstance referred to in paragraph (3) of Regulation 22 of PECR, neither transmit, nor instigate the transmission of, unsolicited communications for the purpose of direct marketing by means of electronic mail, unless the recipient of the electronic mail has previously notified the Company that he or she consents for the time being to such communication being sent by, or at the instigation of the Company; and • neither transmit, nor instigate the transmission of, a communication for the purposes of direct marketing by electronic mail unless the particulars of paragraphs (a)

				and (b) of Regulation 23 of PECR are provided with that communication. AND Monetary penalty notice of £100,000.
30 November 2016	**Oracle Insurance Brokers Limited**	Monetary penalty	Oracle Insurance Brokers Limited (the "Company") generates leads for its business by instigating the sending of direct marketing text messages. Between 5 May 2015 and 21 December 2015, 659 complaints were made to the 7726 Spam Reporting Service or directly to the ICO, and it was subsequently determined that 136,369 unsolicited communications for the purposes of direct marketing had been sent without the consent of subscribers.	Monetary penalty notice of £30,000.
2 December 2016	**Keketso Monnapula**	Prosecution	Keketso Monnapula, a former agency admin worker at Tees Esk & Wear Valleys NHS Foundation Trust, was prosecuted for accessing the sensitive medical records of people that she knew, such as an old school friend and a family member, without the consent of the data controller.	£45 fine, £405.98 costs, £20 victim surcharge
9 December 2016	**Wiltshire Police**	Undertaking follow-up	This action concerned an ICO "follow-up" assessment of the actions taken by Wiltshire Police (the "Force") in relation to an undertaking it signed on 3 March 2016 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented. The review demonstrated that the Force had taken appropriate steps and put plans in place to address some of the requirements of the undertaking. However, the Force will need to	The Force should take further action as follows: • Create a records management training programme to be delivered to staff involved in processing personal and sensitive personal data; and • determine more clearly who is responsible for ensuring that

			complete further work to fully address the agreed actions. In particular, the Force confirmed that it had taken the following steps: • A mandatory online data protection training programme has been developed and is included in the induction programme to be completed by new police officers; • new police staff will also continue to receive face to face data protection training; • a data protection information sheet has been created and is provided to all new starters prior to their start date; and • existing Wiltshire Police staff are also required to view an online data protection video and complete an online data protection course.	mandatory training is refreshed and completed by staff every 2 years.
9 December 2016	**Royal Society for the Prevention of Cruelty to Animals**	Monetary penalty	The first part of the contravention relates to a company, one of whose activities includes "list-broking", and which organises a scheme called "Reciprocate". This scheme enables participating charities to share or swap the personal data of donors or prospective donors. The Royal Society for the Prevention of Cruelty to Animals (the "RSPCA") participated in this scheme from 1998 to 2015 inclusive. In each of those years, the RSPCA disclosed batches of records containing items of personal data. The number of records disclosed in each of those years ranged from between 105,697 to 794,768. The ICO found that the RSPCA failed to process data fairly and contravened DPP1, as the terms of its fair processing notice were unduly vague and/or	Monetary penalty notice of £25,000.

ambiguous.

The second part of the contravention relates to the first. On 19 November 2015, the RSPCA reported to the ICO that the personal data of 15,028 supporters had been shared with a third party or third parties via the scheme outlined above, despite those supporters having opted out of their personal data being shared with other organisations. Between April 2014 and June 2015, groups of records such as these were shared on 12 occasions. The RSCPA told the ICO that this occurred because the wrong dataset had been made available.

The third part of the contravention relates to the RSPCA's use of a number of wealth management companies to analyse the financial status of some of its supporters in order to estimate the likely financial support which those supporters could potentially be persuaded to provide. The RSPCA informed the ICO that this was common practice and, indeed, that it was equally common practice to provide such companies with its entire database, which included the personal data of more than 7 million data subjects. This kind of activity has been undertaken by the RSPCA since 2010, and the ICO determined that the RSPCA's fair processing notices did not indicate that personal data may be processed for such purposes.

The fourth part of the contravention relates to data-matching, which is the use of personal data to obtain and use other items of personal data which data subjects may have chosen not to provide to the data controller, such as email addresses or dates of birth. Tele-matching is data-matching, by which telephone numbers, which

			data subjects may have chosen not to provide, are obtained and used. The RSPCA has used the services of a number of external companies to undertake such practices since 2009. While the RSPCA does not hold records of the numbers of data subjects involved, this number is likely to exceed one million.	
9 December 2016	**British Heart Foundation**	Monetary penalty	The first part of the contravention relates to the "Reciprocate" scheme (please see details of the Monetary Penalty received by the RSPCA on 9 December, which relates to this and all future references). The British Heart Foundation (the "BHF") participated in this scheme for a number of years. Between January 2015 and July 2015, it disclosed batches of records containing items of personal data. The number of records disclosed over this period was 1,047,544, relating to 552,092 individuals. The ICO found that the BHF failed to process data fairly and contravened DPP1, as the terms of its fair processing notice were unduly vague and/or ambiguous. The second part of the contravention relates to the BHF's use of a number of wealth management companies to analyse the financial status of some of its supporters. This kind of activity has been undertaken by the BHF since 2009, but the BHF does not have any intention of undertaking this kind of activity for any longer. The ICO determined that the BHF's fair processing notices did not indicate that personal data may be processed for such purposes. The third part of the contravention relates to data-matching and tele-matching. The BHF has used the services of a number of external companies to undertake such practices since 2009.	Monetary penalty notice of £18,000.

20 December 2016	**Wainwrights Estate Agents Ltd**	Prosecution	Wainwrights Estate Agents Ltd (the "Company") was prosecuted for failing to comply with a third party Information Notice. The ICO received a complaint from an individual for non-compliance with a subject access request. The Company was subsequently served with an Information Notice to enable the ICO to make an assessment of the complaint, and the company failed to respond to this notice.	£250 fine, £500 costs, £30 victim surcharge
4 January 2017	**Minty, Leong and Craddock**	Prosecution	The defendants, Andrew Minty, Jamie Leong and Michelle Craddock were, at various times, employees of Enterprise Rent A Car (the "Company"). They unlawfully obtained personal data from the Company's systems, and these data were then forwarded to claims management companies ('ambulance chasers'), so that they could use them to pursue personal injury claims. Tens of thousands of records were extracted over a two and a half year period and sold for hundreds of thousands of pounds. The Company previously issued civil proceedings against the defendants, which resulted in the defendants having to pay it £400,000 in compensation between them. The ICO subsequently prosecuted the defendants, all of whom pleaded guilty to Conspiracy to commit section 55 Data Protection Act offences.	Andrew Minty: £7,500 fine, to be paid within 2 years (with a period of 3 months in default). Jamie Leong: Conditional discharge for 12 months, and prosecution costs of £3,000, to be paid within 2 years. Michelle Craddock: Conditional discharge for 12 months, and prosecution costs of £1,200, to be paid within 2 years.
10 January 2017	**Royal & Sun Alliance Insurance PLC**	Monetary penalty	Royal & Sun Alliance Insurance PLC (the "Company") is a multinational general insurance company. At some time between 18 May and 30 July 2015, a portable network attached storage ("NAS") device was stolen by a member of staff or contactor who had access to the data server room ("DSR") at the company's premises in Horsham, West Sussex.	Monetary penalty notice of £150,000.

	Both a key and an access card were required to access the DSR, and 40 of the company's staff and contractors had unaccompanied access to the room. The NAS device was unencrypted, but did have password protection. It held, among other items, personal data of 59,592 customers (comprising customer names, addresses, bank account and sort code numbers), and personal data of 20,000 customers (comprising customer names, addresses and credit card primary account numbers, but not CVV numbers or expiry dates).	