Bird & Bird & data protection update

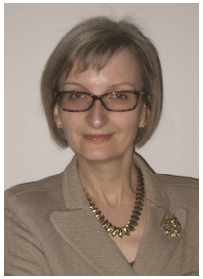
May 2014

Spring has seen a deluge of data protection developments.

Key points to note are:

- Two CJEU decisions:
  (1) Ruling the Data Retention Directive unlawful; and
  (2) On the Google case – confirming a right to be forgotten against search engines and giving guidance on applicable law;
- The Article 29 Working Party have released several documents and opinions, including important positions on anonymisation and reliance on legitimate interests; and
- The UK Government has signalled that it will consult on lowering the threshold for PECR monetary penalties to "nuisance and annoyance" from "substantial damage and distress".

As ever, please do not hesitate to contact us if you have any queries.



Ruth Boardman
Partner
ruth.boardman@twobirds.com

Ariane Mole
Partner
ariane.mole@twobirds.com

Title	Description
UK	
Information Commissioner's Office (ICO)	
1 April 2014	**ICO publishes complaints policy** The ICO has now published its finalised complaints handling policy following its consultation in December 2013. The policy outlines how the ICO will now handle the numerous requests for assistance it receives from individuals. The ICO will now: • only take action of its own where the data subject has first attempted to seek redress from the controller themselves; • base any decision on enforcement action on the context of a breach, including particularly how the controller has handled the data subject's complaint; and • take decisions, in some cases, based solely on correspondence provided by the individual, where appropriate. The new policy particularly emphasises the ICO's message that controllers need to take responsibility for their own data processing activities and respond to queries or complaints from data subjects rather than deferring judgment to the ICO. The policy does not include some of the more controversial content of the consultation version – there is no express focus on repeat offenders for enforcement action, for example, or any commitment to proactively publish the number of complaints it receives about particular organisations. **The complaints policy can be found here**
3 April 2014	**ICO provides update on its direct marketing enforcement strategy** The ICO's Director of Operations, Simon Entwisle, has blogged an update on the ICO's enforcement strategy against those responsible for nuisance calls and texts. The post discusses not only the concerted efforts that have been made by the ICO to bring about a change in the law (as reflected in the Government's Nuisance Calls Action Plan see below) but also the ICO's use of current powers to target this sector. The ICO is focusing on: • Seeking monetary penalties where ICO believes it can meet the substantial harm/distress hurdle, and pursuing an appeal

against the Tetrus Telecom decision (which concluded this test was not met);

- Seeking enforcement notices – which introduce criminal liability for directors if ignored – where companies are in breach; and
- Active pursuit of marketing companies that have failed to register their processing with the ICO.

The post also highlighted the role played by the online reporting tool in bringing repeat offenders to the ICO's attention.

The blog post can be read here.

12 May 2014

ICO security report

ICO has published a security report listing the 8 most common IT security failings which have been responsible for data breaches in an online context. The report has been compiled out of evidence collated during ICO's investigations. The top 8 vulnerabilities are:

1. Not keeping software up to date
2. Lack of protection from SQL injection
3. Use of unnecessary services
4. Poor decommissioning
5. Insecure password storage
6. Failure to encrypt online communications
7. Poor network design
8. Continued use of default credentials (including passwords).

The report explains why each issue raises a vulnerability and what the organisation can do to mitigate this. The report also contains a succinct and easy to read summary of encryption, hashing and salting: a good resource for lawyers looking at security!

Simon Rice, the ICO's Group Manager for security, has also published associated blogs on password storage and the heartbleed security flaw.

Enforcement

25 March – 7 May 2014

Enforcement for this month includes: one monetary penalty, five new undertakings, one follow-up undertaking, one enforcement notice and four prosecutions – another busy month for the ICO.

Please see attached Enforcement Table for more details.

Other

30 March 2014

Government publishes Nuisance Calls Action Plan including legislative proposals

The Department for Culture, Media and Sport has released a Nuisance Calls Action Plan detailing its legislative proposals to address the "growing problem" of nuisance calls. The Action Plan follows lobbying from the ICO and Ofcom for additional powers to address the difficulties they face in regulating the sector. The Action Plan proposes:

- Empowering Ofcom through Statutory Instrument (by October 2014) to share information without the consent of the regulated telecoms company (currently prohibited by s393 of the Communications Act 2003).
- Consulting over a change to the threshold required to impose monetary penalties under PECR, to lower it from a breach causing "substantial damage and distress" to one causing "nuisance, annoyance, inconvenience or anxiety."
- Considering the recommendations of a Which?-led taskforce examining the validity of consent where obtained through third parties.

Whilst targeted at nuisance calls, organisations should be aware that a change to PECR to lower the threshold for monetary penalties will be relevant to all direct marketing activities, not only those involving phone calls.

The Nuisance Calls Action Plan can be reviewed here.

16 April 2014

High Court confirms *Murray v Express Newspapers* test for misuse of private information and breach of the Data Protection Act 1998

The High Court has applied the tests set out in *Murray v Express Newspapers* [2008] EWCA Civ 446 to hold an online newspaper in breach of the claimant's right to privacy and the Data Protection Act, and has awarded a total of £10,000 in damages. The case was brought by three of Paul Weller's children (with him acting as their litigation friend) following the publication of un-pixelated photographs of the family's day out in California. As a result of the Murray test, the questions decided by the case were:

(a) whether the claimants had a reasonable expectation of privacy; and

(b) if so, how the balance should be struck between the claimants' right to privacy and the defendant's right to publish.

Interesting points from the case include:

- The ruling by the judge that the fact the photograph was taken lawfully in California, and could have lawfully been published in California, did not determine either question of the Murray test when the pictures had been published in England & Wales.

- The judge also concluded that the general interest in having a successful newspaper industry did not outweigh the interests of the children.

- Although the judge acknowledged that aggravated damages were possible in this area, none were awarded. The award given to the two younger children was lower, in reflection of the fact that, as babies, they did not suffer any "immediate embarrassment".

The case can be read here.

Title	Description
Europe	
EDPS (European Data Protection Supervisor)	
1 April 2014	**EDPS publishes 2013 report** The European Data Protection Supervisor (EDPS) has published his report of his office's activities in 2013. The report highlighted the EDPS' attention on the proposed revision to the data protection framework, a priority that will continue in 2014. The number of Opinions issued by the EDPS dropped as a result. The report also highlights the EDPS' key role in participating in the Article 29 Working Party, and contributing to the drafting of the group's opinions on data protection law in Europe. **The executive summary can be read here and the full report can be accessed here.**
CJEU	
8 April 2014	**CJEU rules Data Retention Directive unlawful** In the case of *Digital Rights Ireland* (C-293/12), the Grand Chamber of the CJEU declared the 'Data Retention

Directive' (Directive 2006/24) invalid on the basis that it is incompatible with the EU's Charter of Fundamental rights, namely the rights to respect for private life and protection of personal data. Under the provisions of the Directive, data relating to electronic communications (excluding the content of such communications) is retained by ISPs and Telcos and may be made available to law enforcement agencies for a period of 6 to 24 months.

In reaching its decision, the Grand Chamber considered whether the Directive's interference with fundamental rights is proportionate to the objectives of the Directive (combatting serious crime and terrorism). The Grand Chamber highlighted the following issues with the Directive:

- **Nature of the Data:** The data collected 'allow very precise conclusions to be drawn' about data subjects, such as social relationships and habits of everyday life.

- **Volume of the Data:** The pervasiveness of online communication means that the Directive 'entails an interference with the fundamental rights of practically the entire European population'.

- **Lack of Precision:** The provisions of the Directive indiscriminately apply to all individuals, all electronic communications and all traffic data, whether or not there is any evidence suggesting a link with serious crime. Further the Directive does not define 'serious crime' with sufficient clarity (which could lead to abuse by Member States) nor circumscribe the instances in which retained data can be accessed by security bodies, how the data can be used by security bodies, or with whom security bodies may share the data.

- **Generic Retention Period:** The 6 to 24 month retention period is not objectively justifiable and should be amended to reflect the objectives of the Directive.

- **Inadequate Safeguards:** The Directive does not ensure adequate protection of the retained data, taking into account the volume and nature of the data and the risk of unlawful access. Further, the Directive does not dictate that access to the retained data must be dependent upon prior review by a court or administrative body.

- **Transfer Outside the European Union:** The Directive does not require data to be retained within the EU.

The Grand Chamber concluded that the obligations set out in the Directive are 'wide ranging and particularly serious' and not 'sufficiently circumscribed' to limit interference to what is absolutely required. As such, the Directive was not deemed to be proportionate and was declared invalid.

However, it should be noted that the Directive has been implemented across the EU. Whether national laws are valid may depend on local considerations and the method of implementation. Slovakia is the first country to

review local law in response to the CJEU's decision, preliminarily suspending effectiveness of the Slovak implementation of the data retention elements of the Directive on 23 April 2014.

Reports suggest that the UK Government is assessing the consequences of the ruling but that it is reticent to make changes; a Home Office spokesperson has said: "we are considering the judgment and its implications carefully. The retention of communications data is absolutely fundamental to ensure law enforcement have the powers they need to investigate crime, protect the public and ensure national security."

The judgment can be read here.

---

13 May 2014

European Court's Google Spain judgement: privacy trumps all?

On 13th May 2014, the CJEU published one of the most anticipated privacy cases for 2014. The case, about a request from a Spanish citizen to be removed from Google's search index:

- takes a broad and purposive approach to interpreting the Data Protection Directive, repeatedly emphasizing the need to ensure effective protection for individuals and to avoid loopholes;
- states that a member state's data protection laws will apply when a company sets up sales offices selling advertising space in that country and otherwise focuses activities towards inhabitants of that member state;
- confirms the rights in the Directive to have personal data erased and to object to processing; and,
- at least in the case of search engines, concludes that there is no need for an individual to demonstrate prejudice to exercise these rights and that, absent special factors, these rights will prevail over the interests of the search engine to disseminate information and other users to receive information.

The strongly purposive approach to interpretation, emphasizing effective protection over other interests, will be of relevance to all organisations processing personal data.

In order to meet rights of erasure and objection, search engines will need to institute notice and take down style procedures. More worryingly for search engines, however, the Court also notes that operators must be able to justify their activities *from the outset* of the processing: in other words, a search engine which responds promptly to a notice from an individual, may still be faced with a claim for breach of data protection legislation for the period during which the linked material was available, even when such a claim could not be made against the original publisher.

The conclusions on rights to erasure and to objecting to processing could be seen as being specific to search engines, which are singled out by the Court as posing a specific threat to privacy. In the balance between the

---

democratisation of information and privacy, the Court has come down firmly in favour of privacy.

The facts

In 1998, Spanish newspaper, La Vanguardia, published an announcement for a real-estate auction connected with attachment proceedings for the recovery of social security debts owed by Mr Gonzalez. This was indexed by Google, making the page turn up when a user searched on González's name.

Mr González requested the newspaper to remove his personal data from the website or alter the pages so that this data would no longer be included by search engines. Subsequently, Mr González requested Google Spain or Google Inc. (California, US), to remove or conceal the personal data related to him so that they ceased to be included in the search results.

The Spanish data protection authority, AEPD, rejected the request made to La Vanguardia. The AEPD ruled that this publication was legally justified on order of the Ministry of Labour and Social Affairs, to give maximum publicity to the auction and secure as many bidders as possible. The AEPD did, however, uphold the complaint against Google and ordered it to remove Mr. Gonzalez's data. Google Spain and Google Inc each appealed to Spain's National High Court, which made a reference to the CJEU.

The Spanish Audiencia Nacional asked the CJEU preliminary questions on:

- the material scope of the Data Protection Directive: when search engines find, index, store and make available information, does this amount to *'processing of personal data'*;
- the territorial scope of Spanish law, i.e. whether Spanish data protection law applies to Google Spain or indeed directly to Google Inc; an
- whether search engine operators may be required to remove personal data from their indexes and to erase and block personal data – including in situations where the personal data has been lawfully published by third parties.

1: Search engines do process personal data

Google Spain and Google Inc did not dispute that the data indexed and made available related to identified or identifiable natural persons and so amounted to 'personal data'.

The Data Protection Directive defines processing as '*...collection, recording, ... storage, ... retrieval, ... disclosure... making available...*' The CJEU ruled that search engines engage in these specific activities when they index websites, record them and make them available. The CJEU followed its earlier 2008 decision (*Satakunnan Markkinapörssi and Satamedia*) and confirmed that the fact that this is processing (in unaltered form) of material which has already been published does not alter this. The CJEU also confirmed that the operator of the search

engine is the controller as it decides on the means and purposes of these activities.

The CJEU rejected the arguments put forward in the Advocate General's Opinion, by the Greek government and by Google that a search provider cannot be a controller as it searches indiscriminately (without differentiating between personal and other data) and does not exercise control over what personal data is published on the web pages of third parties. The CJEU emphasized the objective of the Directive is *'to ensure, through a broad definition... effective and complete protection of data subjects*' and excluding search engines from the scope of the Directive would be contrary to this aim.

The Court also ruled that the activities of search engines make information available to people who would not have otherwise found it and allow those searching to create a detailed profile of the data subject, acts which are liable to affect the right to privacy separately from the original website publication. Searching is, thus, seen as a significant act of processing in its own right.

2: Broad territorial scope

The Directive provides that an EU Member State's law will apply where *'processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State'*. Google has a subsidiary in Spain and is, therefore, established there. The activities of Google's establishment in Spain mainly related to selling advertisement-space: Google Spain was not involved with the actual functionalities of the Google search engine.

The CJEU held that the Directive does not require that the processing be undertaken 'by' the local establishment. There was sufficient connection between the activities of the Spanish branch and the search engine's data processing activities, *... the activities ... in [Spain]... are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine ... economically profitable and that engine is, at the same time, the means enabling those activities to be performed...'*.

The Spanish National High Court had also asked the CJEU to consider if Spanish law would apply because Google Inc had designated Google Spain as its representative for some purposes, because Google Spain forwards to Google Inc requests from individuals and authorities relating to data protection, or on the basis that Google Inc makes use of equipment in Spain when it crawls information contained on web servers in Spain. As the CJEU considered that Spanish data protection law applied by means of Google's Spanish establishment, it declined to consider these questions.

3: Search engines' responsibilities

The Directive grants individuals the right to have personal data corrected, erased or blocked (Art.12(b)) and to object to processing on 'compelling legitimate grounds' (Art.14).. The CJEU affirms that these rights can also be invoked against search engines acting as controllers.

When it comes to the application of those rights, the search engines' responsibility is distinct from the original websites and this could result in removing information on data subjects from search engine results, even where publication on the original pages might be lawful. According to the CJEU, search engines cannot rely on the journalistic exception in the Directive, whereas the original publisher may benefit from this. This could thus result in disparity between what is available on the web and what can be effectively found though search engines. This right to demand rectification, erasure or blocking of personal data applies to all situations of non-compliance with the Directive, including situations where the data is kept too long (data retention), not complete (data quality) or where the data subject has compelling legitimate grounds (substantial impact on his privacy or other legitimate interests).

Search engines, like other controllers, must also be able to show that their processing satisfies one of the legitimate bases for processing under Article 7 – the most relevant condition for search engines being Article 7(f) (that the processing is necessary for the legitimate interests of the search engine, or those to whom the personal data are disclosed, except where the interests or fundamental rights and freedoms of the data subject override these interests). On this balancing test, the CJEU noted that:

- Search engines are likely to significantly affect fundamental rights to privacy, as search plays an important role in society and makes information ubiquitous;
- The potential seriousness of the interference with privacy rights, is such that search engines 'cannot' justify this purely on their economic interests;
- The CJEU accepts that it is relevant to consider the legitimate interests of internet users who are interested in having access to search results;
- However, *'data subject's rights ... override as a general rule ... that interest of internet users [in having material communicated to them*]';
- This may be altered in specific cases – based on the sensitivity of the information for the individual and the interest the public have in accessing the information – for example, whether the individual has a role in public life.

4: A right to be forgotten?

The *'right to be forgotten'* has been a heavily debated part of the proposals for the draft General Data Protection Regulation.

The CJEU refrains from stating that there is an actual "right to be forgotten". However, it confirms that an individual does have a right to require his personal data to be removed from a list of results, without needing to show specific prejudice – which is substantially equivalent to a right to be forgotten. This right may be overridden in particular cases – eg where there is a strong interest in continued availability of information if the individual is a

public figure. In this case, the CJEU noted that there did not appear to be any particular reasons justifying continued inclusion of Mr Gonzalez's personal data in Google's search results – although this was a matter for the referring Spanish court to determine.

The CJEU has confirmed that the Spanish courts could, if they chose, grant Mr González's wish to be "forgotten. In the process, the case has likely secured Mr Gonzalez's literary immortality, at least in legal circles: a 'right' to be forgotten is easier to say than to deliver.

The judgment can be read here.

Art 29 Working Party

21 March 2014

Art 29 WP publishes Working Document containing "draft ad hoc contractual clauses" for Processor to Processor international transfers

The Article 29 Working Party has published draft ad hoc contractual clauses, intended for use when an EU processor subcontracts processing to a non-EEA sub-processor (a "P2P" transfer). The WP29 underlines that the proposed clauses are not approved by the Commission, and are not in their current form a finalised set of ad-hoc clauses that can be relied upon to meet data transfer requirements. The aim of the document is stated to be to "*provide advice to the Commission should [it] in future consider the possibility of amendments or supplementations to the existing model clauses*" as well as "*contributing to the uniform application of national measures authorising transfers of personal data*". It is notable that Spain has adopted its own approval scheme for P2P transfers.

The draft clauses contained both directions on the type of agreement that must be in place between the controller and the processor data exporter, and place obligations on the processor data exporter that effectively replicate typical data processing agreement provisions, such as:

- Detailed requirements on consent to sub-processing;
- Requirements to notify breaches or communications from law enforcement/data subjects;
- A requirement to include a detailed reference to the ad-hoc clauses within the agreement with the controller, such as use of an appendix; and
- Obligations on termination, depending on the choice of the controller as to whether it prefers return or destruction of data.

Much of the agreement is broadly similar to the Commission approved C2P SCCs – for example, the inclusion of rights of enforcement by data subjects, and provisions on data transfers. The two Appendices replicate those in the C2P SCCS (i.e. description of processing and detailed security measures).

The Opinion can be read here.

2 April 2014

Art 29 WP concludes that Microsoft Agreement can be considered "in line with C2P SCC" rather than ad-hoc clauses requiring specific authorisation

Following a collaborative process, the Article 29 Working Party has written to Microsoft to confirm that they consider the Enterprise Enrolment Addendum Microsoft Online Services Data Processing Agreement – together with its Annex 1 – to be in line with the Commission drafted C2P SCCs. This decision practically reduces the number of authorisations that will be required by Microsoft (although authorisation will still be required in countries where all SCCs must be approved, such as Spain).

The WP29 letter can be read here.

---

9 April 2014

Art 29 WP publishes Opinion on legitimate interests

When may a data controller process personal data on the basis that the processing is in its, or someone else's 'legitimate interests'? On 9th April 2014, the Article 29 Working Party adopted an Opinion giving guidance on this (WP217).

WP217 considers the role of 'legitimate interests' under the current Data Protection Directive. It also emphasizes the importance of this provision in the draft General Data Protection Regulation and recommends some additions to the Regulation.
The Opinion states that 'legitimate interests' 'should not be treated as a last resort for rare or unexpected situations'. However, nor should it be 'automatically chosen... on the basis of a perception that it is less constraining than the other grounds'.

If a controller wishes to rely on 'legitimate interests', it should carry out an assessment:

- identifying and evaluating the interests on which it is seeking to rely;
- the impact this will have on individual's interests;
- whether the processing may, in principle, be justified on this basis; and
- whether there are additional safeguards that the controller could implement that that would minimise this impact.

The Opinion recommends documenting this assessment and suggests that the draft Regulation should require a) such documentation and b) that controllers explain to individuals why processing is being justified on this basis.

Justification for processing Personal Data:

The Data Protection Directive provides that a data controller may only process personal data when it can satisfy one or more of the grounds for processing set out in Article 6 of the Directive. Aside from 'legitimate interests', these grounds relate to:

- individual consent;
- contractual arrangements with the individual;
- legal obligation of the controller;
- vital interests of the individual; and
- tasks performed in the public interest.

The Working Party offers some limited commentary on these other grounds. In particular, noting that for all grounds other than consent, processing must be 'necessary', which, in accordance with CJEU jurisprudence, is something less strict than 'indispensable', but more strict than 'reasonable' or 'desirable'. The Working Party notes that contractual necessity only justifies processing which is, in fact, necessary to perform the contract, not processing which the controller reserves a contractual right to perform. On 'legal obligations', the Working Party suggests that the obligations must be imposed by EU or member state law - so overseas legal obligations are not valid for this condition. Further, the condition would cover processing which the controller is specifically required to carry out: if the controller choses to process personal data, in order to better meet legal obligations or reduce risk of non-compliance, then this should be justified in another way.

Legitimate interests basis for processing: A balancing test

The legitimate interests condition requires the controller to balance its interests, or those of the third party to whom data is disclosed, with those of the data subjects. The Working Party notes that this risk assessment need not be particularly burdensome and it gives examples of relevant factors to be considered at each point of the assessment.

Identifying relevant interests:

- Is the processing necessary for a fundamental right (such as freedom of expression), or otherwise in the public interest?
- is it for a purpose which is recognised in the relevant community?
- other interests, which engage only 'private' interests can also be considered - however, they will weigh less heavily in the balance
- is the processing being carried out in accordance with regulatory guidelines?

Assessing the impact on the individual:

- what are the individual's reasonable expectations as to how their data will be used?
- what is the nature of the data?
- even individuals engaged in illegal activities are entitled to have their interests taken into account
- an adverse impact does not necessarily mean the processing cannot be carried out

Possible safeguards:

- have privacy enhancing technologies been deployed, has the data to be collected been minimised?
- what steps have been taken to raise awareness of the processing, can the individual opt-out?

The Working Party recommends against an attempt to include lists of conditions which do, or do not, satisfy this test in the text of the draft Regulation: one of the benefits of the legitimate interests test is its ability to develop over time and prescriptive lists may restrict this.

Sensitive data- Additional restrictions

The Working Party also looks at the relationship between Article 7 (conditions for processing personal data) and Article 8 (conditions for processing 'sensitive' data). It considers that the tests are cumulative - i.e. where sensitive personal data are processed, a controller must be able to satisfy a condition under both Articles - but that this is not clear from the face of the Directive. A possible counter argument is that Article 8 counts as 'lex specialis', such that these sensitive data specific conditions stand in place of the ordinary conditions for processing.

Examples

The Opinion contains many examples of processing that can/cannot be justified on the basis of legitimate interests. Readers may find the following of interest:

- employee monitoring: is unlikely to be justified as being contractually necessary, but may be justified based on legitimate interests;
- direct marketing can be justified based on legitimate interests, unless it involves extensive profiling, in which case the Working Party suggests that consent would be necessary;
- the Working Party also suggests that consent 'should' be necessary for data broking and for tracking based digital market research; and
- publication of salaries of officials or senior managers in the interests of transparency.

The Opinion can be accessed here.

---

10 April 2014

Art 29 WP publishes Opinion on surveillance of electronic communications for intelligence and national security purposes

The Article 29 Working Party has published an opinion in response to the Snowden revelations of the use of electronic communication data by national security services both within and outside the EU. The WP29 conducted

---

a survey of all national EU DPAs (plus Switzerland and Serbia) to establish the level of oversight from DPAs of intelligence services, and the extent to which general data protection laws were deemed to apply to their activities. The results of the survey showed that there was much diversity in the approach taken by member states, and DPAs in most EU countries had little to no oversight role. The Opinion also concludes that under no circumstances can surveillance programmes based on the indiscriminate, blanket collection of personal data meet the requirements of necessity and proportionality set out in the data protection principles, which apply through the ECHR and the EU Charter on Fundamental Rights even if exempt from Directive 95/46/EC.

The majority of recommendations relate to legislative or administrative measures that are directed at Member States. Recommendations in the report that are relevant to data controllers include:

- Taking measures to improve transparency including continued attempts to publish information on the number and types of requests received from public authorities; and
- Ensuring that data transfers outside of the EEA abide by the data protection principles – DPAs are encouraged to suspend transfer mechanisms if there is a substantial likelihood that the principles are being violated.

The Opinion can be found here.

---

10 April 2014

Art 29 WP publishes Opinion on Anonymisation Techniques

The Article 29 Working Party has published an Opinion on anonymisation techniques. The Opinion states that anonymity must be ensured with reference to three criteria:

- Is it possible to **single out** an individual by isolating some or all records relating to that individual in a dataset;
- Is it still possible to **link records** relating to an individual or group of individuals, whether in the same database or across databases;
- Can information still be **inferred** about an individual – can a value relating to an individual be deduced with significant probability from other values.

The Opinion then goes on to provide a detailed assessment of various anonymisation techniques with reference to these criteria (namely, noise addition, permutation, differential privacy, aggregation, k-anonymity, l-diversity and t-closeness). The Opinion makes the following important conclusions:

1. Processing data in order to anonymise it ought to be considered compatible with the original processing of that data.
2. Removing identifying elements is not in itself enough to ensure identification of a data subject is no longer possible, nor can any one of the anonymisation techniques discussed itself meet all three criteria – a combination of techniques ought to be adopted, as determined on a case-by-case basis.

---

3. Where a data controller does not delete the original identifiable data at "event-level", and the data controller hands over part of this dataset following the use of masking or deletion of identifiers, the resulting dataset is *not* considered anonymous.

This Opinion goes into greater technical detail than the ICO's Anonymisation guidance released last year. In seemingly concluding that information must be anonymous in all hands (including the original controller's), the WP29 appear to run counter to the established interpretation in the UK, where information that is anonymous in the hands of the recipients is not considered personal data in the hands of that recipient, even if the original controller retains the ability to re-identify that data. It remains to be seen whether the ICO will amend its own anonymisation guidance.

The Opinion can be accessed here.

UK Enforcement

UK				
Date	**Entity**	**Enforcement notice, undertaking, monetary penalty, or prosecution?**	**Description of Breach**	**Summary of steps required (in addition to the usual steps*)**
7 March 2014	Amber UPVC Fabrications Ltd	**Monetary Penalty and Enforcement notice under section 40 of the Act.**	The ICO has served a monetary penalty of £60,000 and an enforcement notice on Amber UPVC Fabrications Ltd (Amber Windows) after the company was found to be making unsolicited marketing calls to individual subscribers, all of whom had registered with the TPS at least 28 days prior to receiving the calls and had not previously notified Amber Windows that they were willing to receive calls from them. This was a breach of the Privacy and Electronic Communications Regulations 2003 (Regulation 21).	Amber Windows shall, within 35 days of the Enforcement Notice, neither use nor instigate the use of a public electronic communications service to make unsolicited calls for direct marketing purposes to: • Subscribers who have previously notified Amber Windows that calls should not be made on that line; and/or • Subscribers who have registered their number with the TPS at least 28 days previously and who have not notified Amber Windows that they do not object to such calls.
13 March 2014	Barry Spencer (of ICU Investigations Limited)	**Prosecution under s55 of the Act.**	Barry Spencer, who ran ICU investigations Limited (ICU), has been ordered to pay fines of £20,000 and is subject to a confiscation order of over £69,000. ICU traced individuals on behalf of clients and, in doing so, had tricked organisations (such as utility companies and GP surgeries) into revealing personal data on nearly 2,000	Order to pay fines and prosecution costs totalling £20,000 as well as a confiscation order of £69,327.37 under the Proceeds of Crime Act. Failure to pay the confiscation order will result in 20 months imprisonment. Disqualified from being a director for 8 years.

UK				
Date	**Entity**	**Enforcement notice, undertaking, monetary penalty, or prosecution?**	**Description of Breach**	**Summary of steps required (in addition to the usual steps*)**
			occasions. Spencer and his former business associate, Adrian Stanton were convicted at an earlier trial in 20 November 2013. Stanton, along with five other employees, were fined a total of £18,500 and ordered to pay over £15,000 in costs.	
14 March 2014	Allied Union Limited	**Prosecution under s17 of the Act**	Allied Union Limited, a pension review company, has been prosecuted by the ICO for failing to notify the ICO that it handled personal data.	Company to pay fines of £400, costs of £338.11 and a victim surcharge of £40.
25 March 2014	Help Direct UK Limited	**Prosecution under s17 of the Act**	A financial advisor has been prosecuted by the ICO for failing to notify. Help Direct UK Limited pleaded guilty.	The company was fined £250, ordered to pay costs of £248.83 and a victim surcharge of £25.
28 March 2014	Barking, Havering & Redbridge University Hospitals NHS Trust	**Undertaking to comply with the seventh data protection principle** (Part 1 Schedule 1 of the Act)	An undertaking to comply with the seventh data protection principle has been signed by the Barking, Havering & Redbridge University Hospitals NHS Trust (BHRUT) following a fax containing personal data being sent to the incorrect number of a member of the public. Neither of the employees involved had received Information Governance training. The ICO	Steps required to ensure: • That attendance for its mandatory Information Governance training is properly enforced; and • That it maintains a full and accurate record of who has received the training.

UK				
Date	**Entity**	**Enforcement notice, undertaking, monetary penalty, or prosecution?**	**Description of Breach**	**Summary of steps required (in addition to the usual steps*)**
			discovered that the overall attendance rate at BHRUT for this training was only 35 to 40%.	
11 April 2014	Royal Borough of Windsor and Maidenhead	**Follow up review of undertaking (originally signed 24 September 2013)**	A follow up has been completed to provide an assurance that the Royal Borough of Windsor and Maidenhead (RBWM) has appropriately addressed the actions agreed in its September 2013 undertaking. This undertaking was in relation to disclosure of the details of 257 employees on RBWM's intranet. The ICO has concluded that appropriate steps are being taken, but work needs to be completed for requirements to be fully addressed.	Further action to be taken: • Finalise and gain ratification for the information handling policy; and • Complete data protection training for all staff, implement annual refresher training, and implement initial training of new starters.
15 April 2014	Wirral Borough Council	**Undertaking to comply with the seventh data protection principle (Part 1 Schedule 1 of the Act)**	An undertaking to comply with the seventh data protection principle has been signed by Wirral Borough Council (WBC) following social work information being sent to the wrong address, resulting in disclosure of sensitive personal data relating to two families. WBC did not have adequate provisions in its IT Security policy nor overarching data protection guidance. Further, social workers had not received any specific data protection or data handling training.	WBC must ensure that: • Processes are put in place to ensure documents are sent to the correct address and staff receive practical guidance on these processes; • Further steps are taken to promote the use of locked printing functions, or prompt collection of paperwork where locked printing is not used; • Completion of the mandatory data protection training for all staff is

UK				
Date	**Entity**	**Enforcement notice, undertaking, monetary penalty, or prosecution?**	**Description of Breach**	**Summary of steps required (in addition to the usual steps*)**
				monitored and enforced, with training material updated and reiterated at regular intervals (not exceeding two years); and • Review of data protection policies and procedures generally, to ensure that sufficient practical guidance is provided to staff in how to comply with the Act, and communicated such revised guideline effectively to staff by 30 June 2014.
15 April 2014	Wokingham Borough Council (WBC)	**Undertaking to comply with the seventh data protection principle (Part 1 of Schedule 1 of the Act)**	Documents containing sensitive personal data, released in response to a SAR, were left on a door step by a delivery driver (employed by WBC). The documents subsequently disappeared. The ICO was aware of previous cases in which advice had been provided to WBC on, *inter alia*, training and employee awareness of data protection, rather than formal regulatory action being taken. The ICO's recommendations had not been properly implemented.	• Staff must be made aware of WBC's policy and procedures for storage and use of personal data, and appropriately trained how to follow these, by 31 July 2014; • Training in data protection and information security (including WBC's policy and procedures) shall be carried out prior to initially granting access to WBC's systems for all staff whose roles involve regular access to personal data; • A refresher training structure shall be implemented; training to be regularly updated and refreshed at regular intervals not exceeding two years, by 31 July 2014; • Procedures shall be drafted and implemented to cover issues such as transporting paper records containing

UK				
Date	**Entity**	**Enforcement notice, undertaking, monetary penalty, or prosecution?**	**Description of Breach**	**Summary of steps required (in addition to the usual steps*)**
				personal data outside the office, no later than 30 June 2014; and • Compliance with policies on data protection and completion of training shall be monitored and appropriate steps taken to ensure failings are rectified with minimal delay.
25 April 2014	Dudley Metropolitan Borough Council	**Undertaking to comply with the seventh data protection principle** (Part 1 Schedule 1 of the Act)	An undertaking to comply with the seventh data protection principle has been signed by Dudley Metropolitan Borough Council (DMBC) following a case file containing sensitive personal data being left at a client's home by an agency social worker. The contents were read by a child in the house and then communicated to family members. The documents outlined child welfare concerns raised by another family member. The agency social worker had not completed Information Governance training upon induction.	DMBC must ensure that: • Staff (permanent and temporary) use consistent standards in relation to handing personal data and are made aware of any changes promptly; • Completion of mandatory induction data protection training (on the requirements of the DPA 1998 and DMBC's data protection policies) is enforced for all staff (permanent and temporary). Completion of training must be recorded and monitored; and • Guidance regarding taking personal information out of the office should be available to all social workers conducting home visits (covering removal, transport, security and safe return).
12 May 2014	The Moray Council	**Undertaking to**	A bundle of papers relating to a	• MC must ensure that a policy or

UK				
Date	**Entity**	**Enforcement notice, undertaking, monetary penalty, or prosecution?**	**Description of Breach**	**Summary of steps required (in addition to the usual steps*)**
	(MC)	**comply with the seventh data protection principle** (Part 1 Schedule 1 of the Act)	permanence panel hearing were left in a local café by an employee of MC. The employee in question had signed a confidentiality agreement requiring that the papers were kept safe and secure in lock fast facilities. However, the ICO found that MC had not implemented any policies or procedures to assist staff in keeping data secure outside the office, nor had any general training on security of personal data been provided.	procedure is implemented ensuring the security of data taken outside of the office. Staff must be made aware of this policy/procedure; • MC must ensure data protection training is mandatory for all staff handling personal data and that completion is monitored; and • MC must review the content of its data protection training to ensure it is adequate.
13 May 2014	QR Lettings	**Prosecution under s17 of the Act**	A property company has been prosecuted by the ICO for failing to notify. QR Lettings pleaded guilty.	Company to pay a fines of £250, costs of £260 and a victim surcharge of £30.