ICO releases updated direct marketing guidance

The ICO has updated its guidance on direct marketing. At first sight, it looked like the revision was more extensive than, in reality, it was. The key changes are as follows:

1. **ICO enforcement**
   - Monetary penalty notices: New and up-to-date examples are provided for such notices issued in respect of breaches of the direct marketing rules. The ICO has also divided such examples into notices issued for: (i) making live marketing calls without prior consent; (ii) making automated marketing calls without prior consent; (iii) sending marketing emails without consent; and (iv) sending marketing text messages without consent.
   - Marketing lists: The ICO changes the wording from "likely to" to "will" take enforcement action under the DPA against organisations who sell marketing lists without people’s knowledge or consent.

2. **Market research**
   - The ICO now provides an example of ‘genuine market research’: "(for example, the purpose is to use market research to make decisions for commercial or public policy)."
   - The ICO now also provides an example of what ‘promoting their products’ is in the context of explaining what an organisation cannot ask a market research firm to do: "(this will include asking the research firm to use the organisation's goods/services as a way to incentivise participation)."

3. **Not-for-profit organisations**
   The ICO has tightened up the wording in this section to ensure that it is clear that all not-for-profit organisations must comply with the direct marketing rules, and not just charities and political parties. The ICO reiterates the direct marketing rules as applied to not-for-profit organisations.

4. **Consent**
   - The ICO now provides examples for each element of valid consent i.e. "freely given, specific, informed and an indication specifying agreement."
   - The guidance given in respect of what constitutes 'freely given' consent has changed. Previously, the ICO stated that consent simply cannot be a condition of subscribing to a service or completing a transaction. The
position in the revised guidance is that consent can be a condition of subscribing to a service, provided that the organisation demonstrates how this indicates that the consent was freely given. i.e. this is no longer an absolute prohibition in respect of subscribing to a service.

- Implied consent: In this context, the ICO provides more information on what an organisation must demonstrate if it makes consent a condition of subscribing to a service and the considerations the ICO will take into account when assessing whether such consent is valid. An organisation must, in addition to the above, demonstrate why consent cannot be sought separately; and the ICO will take the following factors into account: (i) whether there is a choice of other services; (ii) how fair it is to couple consent to marketing with subscribing to the service; and (iii) whether this approach creates an imbalance between the individual and organisation.

- Methods of obtaining consent: The ICO reiterates that best practice for obtaining consent is to present a customer with an opt-in box requesting that they wish to receive marketing messages "via specific channels (e.g. post, email, live phone call etc.).", i.e. reiterating its recommendation that an opt-in box should be provided after each means of communication.

5. Indirect consent

- It is no longer sufficient to simply "describe a specific category of organisation" that may send the customer direct marketing. Indirect consent will only be considered valid if the consent "very clearly describes precise and defined categories of organisations and the organisation wanting to use the consent clearly falls within that description." Further, the names of categories must be "tightly defined", "understandable to individuals" and "sufficiently specific that individuals could reasonably foresee the types of companies that they would receive marketing from, how they would receive that marketing and what the marketing would be".

- New guidance is given on the presentation by an organisation of marketing material relating to third parties. The ICO recommends that, while the organisation is not passing on its customers' contact details to a third party, it must ensure that it has appropriate consent from its customers to receive such marketing material.
3 March 2016
ICO releases new encryption guidance

The ICO has updated its guidance on encryption, providing several example scenarios of when an organisation should consider encrypting data and indicating that regulatory action could occur where the lack of encryption has led to a loss of data. While the DPA does not oblige data controllers to encrypt personal data, there is a general principle that "appropriate technical and organisational measures shall be taken against unauthorised loss or unlawful processing of personal data".

The scenarios featured in the guidance include the transfer of personal data by CD or DVD, sending personal data by email, encryption of mobile devices, CCTV and drones. The guidance also provides basic information on the different types of encryption and how organisations can implement encryption.

The full ICO guidance is available here.

16 February 2016
ICO publishes new guidance on Wi-Fi location analytics

With a growing number of organisations offering free Wi-Fi to customers or installing Wi-Fi networks on their premises for use by employees, the use of data obtained from, or via, Wi-Fi enabled devices to monitor individuals is becoming increasingly common.

An activated Wi-Fi enabled device will continually broadcast 'probe requests' to discover Wi-Fi networks. When a Wi-Fi transmitter is within range of the device, the two will communicate and the MAC address of the device (theoretically, a unique identifier) will form part of these communications. The strength of the signal received by the transmitter can be used to estimate how far away the particular device is situated (which, in turn, can be used to monitor the location and movements of the device). Organisations can use this information to determine, for example, volume of visitors to the premises or how individuals typically move around the premises.

In February, the ICO published guidance for operators of Wi-Fi networks, which contained the following key recommendations for ensuring compliance with the DPA:

1. Conduct a privacy impact assessment ('PIA') to identify and reduce privacy risks.

2. Define purposes to ensure that the reasons behind collection of personal data and the intended processing activities are clear.

3. Notify individuals of the purpose of processing, potential data sharing and the identity of the date controller. The ICO suggests achieving this:
4. Remove identifiable elements by, for example, anonymising the MAC address so that individuals cannot be identified, where this would still enable a data controller to achieve the specified purpose of data collection (e.g. where the data controller's intention is to measure the number of visitors to a store only).

5. Define the bounds of collection to ensure that individuals are provided with information on the data collection before it occurs. Organisations should remember that certain locations may be more sensitive than others (e.g. bathrooms and first aid rooms) and should consider ways of minimising the amount of personal data collected, or degree of intrusion to privacy caused (e.g. by sampling data, or limiting data collection to specific times of day).

6. Define a data retention period to ensure that data are not kept for longer than necessary (in light of the purpose of collection).

7. Establish control mechanisms to provide individuals with a simple and effective way to opt-in or opt-out of data collection.

8. The ICO provides examples of:
   - installing, at the entrance, an instrument which identifies a device's MAC code then offers an opt-in or opt-out to the individual;
   - including URL or QR codes in privacy notices, websites or Wi-Fi sign-up pages (or similar) which direct users to a webpage into which they can enter their MAC address and indicate their opt-in or opt-out preference; and
   - providing regular visitors (e.g. employees) with briefings.

9. Contracting out – where an organisation would like to use a third party to perform Wi-Fi analytics on its behalf, it will need to ensure that the third party also processes the personal data appropriately.

The full ICO guidance is available [here](#).
New Investigatory Powers Bill for UK

The UK’s new Investigatory Powers Bill, currently making its way through Parliament, is the first major revision of intelligence agency and law enforcement powers over communications for over 15 years. It will put existing interception, equipment interference and communications data acquisition capabilities, including some only recently acknowledged to exist, on a more explicit statutory footing, and introduce judicial approval for the exercise of some powers. It also extends existing powers, such as by introducing mandatory retention by service providers of users’ site browsing histories. This article summarises the likely changes and provides a business by business analysis of the Bill’s implications.

The article can be viewed in full [here](#).

With thanks to Graham Smith (Partner (IP), Bird & Bird).

Liberalisation of citizen data held by public bodies – UK law changes planned

On 1 March, the Cabinet Office announced that the Government, in order to "improve the welfare of the individual in question", would alter the law to make it simpler for public sector organisations to share citizens’ personal data.

To enable data sharing, a "single gateway" will be established. Only under certain circumstances will disclosure be allowed, and the new laws will give UK ministers the ability to "modify or add objectives for which information may be disclosed".

The Cabinet Office has stated that, "The objective must have as its purpose the improvement or targeting of a public service provided to individuals of a particular description, or the facilitation of the provision of a benefit (whether or not financial) to individuals of a particular description, and the improvement of the well-being of individuals." Further detail is provided on what is meant by well-being of individuals, which might be, for example, physical, emotional or social well-being.

Disclosures will not be permitted if objectives can be attained without data sharing. Furthermore, only if "it is not realistic and practicable to use consent to achieve the intended outcome or use of consent would not meet the criteria of free and informed decision making", will data be shared. Lastly, only if the "sharing and analysis of de-identified data would not achieve the intended outcome", will the sharing of personal data be permitted.

Two new codes of practice that are to be presented to Parliament will govern the proposed arrangements. Under the
proposals, if a public body shares or uses data in a way that does not conform to the codes, it could be prohibited from disclosing or receiving data.

According to the Cabinet Office, "...the code will reinforce the need for authorities using the power to follow the data protection principles as well as guidance issued by the Information Commissioner...Each code will reinforce the data protection principle of proportionate usage and will challenge proposed data sharing arrangements, questioning whether aggregate, general or de-identified data would meet needs rather than using identified data....Where it is determined that identified data is required for the purposes of the data share, the challenge will then be whether binary checks/data matching will suffice. Bulk data transfers will only take place where there is a strong case to do so and where objectives cannot be met through other methods, and only then with the condition that there are appropriate secure processes, systems and data transmission methods to ensure that transfers can take place safely."

A new criminal offence of unlawful disclosure of personal data has additionally been proposed. If a person is found guilty of unlawful disclosure, they could be sentenced to up to two years in jail and also receive a fine.

The Cabinet Office’s consultation paper can be viewed in full here

Consultation on the plans ended on 22 April 2016.

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 February – 16 May 2016</td>
<td>Enforcement for the period includes: 14 monetary penalties, 5 new undertakings (and 10 follow-up reviews of existing undertakings), 9 enforcement notices, and 3 prosecutions. Please see the Enforcement Table below for more details.</td>
</tr>
</tbody>
</table>

**Cases**

<table>
<thead>
<tr>
<th>Date</th>
<th>Case</th>
</tr>
</thead>
</table>

This is an interesting subject access case. Warby J rejected overly broad claims, by a firm of private investigators, that the firm should not have to respond to a subject access request, on the basis that all of the information they held would be covered by exemptions, or that the request was an abuse of process (as it was linked to separate, private, criminal proceedings in Cyprus).

The defendants failed, in part, because they had not tried to sift and analyse the information they held - so that they could not demonstrate that all of the information they held would be covered by an exemption, or that release of the requested
information would be likely to cause prejudice.

The decision contains some interesting, more general comments:

1) about the way the courts should exercise discretion in subject access cases (pro-data subject unless the defendant can show reasons why discretion should not be exercised); and

2) about the approach to cases where subject access requests are used as a way of obtaining advance disclosure of documents (that there is nothing wrong with using the Act in this way).

The facts

The case concerned 3 Russian nationals, who had been involved in the same company. One (Alexander Gorbachev) asserted that the others (the claimants) had improperly defrauded him of his shares in the company. Mr Gorbachev instructed investigators (the defendants) in connection with this matter. He also brought a private prosecution against them in Cyprus. The investigators approached the matter in a way which the claimants were likely to consider threatening. The claimants made a subject access request to the investigators. The investigators declined to deal with the request arguing that it was procedurally invalid and that any material they held would be exempt - either on the basis of the crime prevention exemption, or the legal professional privilege exemption. The investigators also invited the court to exercise its discretion not to order them to comply with the access request, on the basis that it was an abuse of process as it was solely being made in connection with the Cypriot proceedings.

The judgment

Evidence of authority:

Where the request comes from a solicitors' firm, which states that it is instructed by the data subject to make the access request, there will ordinarily be no need to check this assertion of authority.

Crime prevention/detection exemption:

Private persons can rely on the prevention/detection of crime exemption: it is not restricted to public bodies.

However, on this occasion, the defendants failed to demonstrate to the judge's satisfaction, and on the basis of a civil standard of proof, that they were in fact processing the claimant's personal data for this purpose.

They also failed to demonstrate that disclosure of the claimants' personal data would, or would be likely, to prejudice this
purpose, as required for the exemption to apply. The defendants were trying to make a blanket claim that, given the nature of their investigations, all the material they held must be exempt: the judge confirmed the approach taken in *R (on the application of Alan Lord) v Secretary of State for the Home Department* [2003] EWHC 2073, and set out in ICO guidance, that the exemption must be applied on a case by case basis and does not apply to all information held by an organisation as a matter of principle.

Legal privilege:

Lawyers who claim privilege for documents are, in effect, judges in their own cause (or rather the cause of their clients). For this reason, courts must approach claims of privilege cautiously. The onus is on the person claiming privilege to prove (to a civil standard) that it is likely to apply.

Again, the judge held that the claimants had failed to prove this. They had also attempted to make a blanket claim that all data they held must be privileged, without providing any analysis as to why this should be the case. The judge accepted the claimants’ arguments that it was highly unlikely that all of the personal data held by the investigators would be protected by privilege: for example, they would likely have obtained pre-existing documents for analysis, which would not suddenly become privileged.

Discretion:

Irrespective of the points above, the defendants invited the judge to exercise his discretion not to require them to respond to the access request (on the basis that the sifting required would be disproportionate and that the request was made for an improper purpose).

The judge noted that there were two divergent lines of approach as to how discretion should be exercised:

1) some comments suggest that the court’s discretion was "general and untrammelled" (*Durant v Financial Services Authority* [2003] EWCA Civ 1746; [2004] FSR 28, but obiter); and

2) others suggest that, to remain faithful to the purposes of the Directive, discretion should be exercised "to require disclosure, unless good reason is shown why it should not be disclosed" (part of Ward LJ’s reasoning for granting permission for the appeal in *Durant v Financial Services Authority*, which followed a failed claim in the court of first instance).

On balance, Warby J preferred the second approach - but he noted that he would have found for the claimants on either test.
Proportionality:

Warby J rejected claims that analysis of the documents to assess privilege would be disproportionate. He felt this was the kind of analysis that was regularly carried out. He distinguished Dawson-Damer & Ors v Taylor Wessing LLP & Ors [2015] EWHC 2366 (Ch), on the basis that that involved consideration of whether a claim to privilege could be maintained as a matter of Bahamian law, where there was evidence that such law operated differently to English law.

Abuse of process:

The judge also rejected the defendant’s argument that the claimants request should be rejected because it was solely made as an (improper) attempt to access material relevant to the Cypriot proceedings which should be handled in the course of those proceedings. The claimants relied on a passage from Durant v Financial Services Authority which suggested that the purpose of s. 7 is not to allow applicants early access to discovery of documents which may assist in litigation. They also referred to cases (such as Dawson-Damer v Taylor-Wessing LLP) which considered whether requests should be refused where there were mixed or collateral motives and where the request would not have been made but for the improper litigation motive.

Warby J did not think that the Court of Appeal comments on this should be treated as authority for the fact that the purpose of a subject access request is relevant to determining whether or not to accept the request. Instead, he referred to an alternate Court of Appeal case, Dunn v Durham County Council [2012] EWCA Civ. 1654, where the Court of Appeal noted that subject access rights would likely be used prior to proceedings and where the Court of Appeal “did not doubt” that an individual would be entitled to do this.

In any event, even if the collateral or mixed motive approach were followed, the judge preferred the claimants’ approach: the defendants had made intimidating approaches to them and had also insinuated that the claimants might present a physical threat to their client. In this situation, the claimants would reasonably be concerned about the material held by the defendants and would likely want to check its accuracy (a bona fide purpose).

19 February 2016  R (on the application of G) v Chief Constable of Surrey Police and others [2016] All ER (D) 201

This case involved a challenge by way of judicial review to the disclosure of records of a police reprimand in response to an enhanced disclosure request made under the Police Act 1997 to the Disclosure and Barring Service (DBS).

The Court upheld the applicant’s claim that the disclosure by DBS of data relating to a police reprimand accepted by the applicant when he was 13 years old, amounted to an unjustified interference with his rights under Article 8 of the European Convention on Human Rights and declared the statutory regime governing enhanced disclosure incompatible with the applicant’s human rights.
The statutory scheme

The Police Act 1997 imposes a duty on the DBS to issue a certificate recording ‘all relevant matters’ in response to a valid request for enhanced disclosure (e.g. a disclosure request made in connection with a position that will involve caring for, training, supervising or being in sole charge of children or vulnerable adults). ‘Relevant matters’ include not only recorded convictions but also cautions and reprimands. Enhanced checks may also result in the disclosure of police ‘intelligence data’ which does not form part of the subject’s central criminal record. This intelligence data is included on enhanced disclosure certificates only where it is considered by the Chief Constable concerned to be relevant to the position that has been applied for.

The facts

In 2006, the claimant (then aged 13 years) was issued with two reprimands for offences of sexual activity with two children. The CPS prosecutor at the time had recommended a reprimand rather than a prosecution on the basis that the behaviour constituted "sexual experimentation" and was "not something sinister and serious - just misguided." In 2011, the claimant applied for an enhanced disclosure check because he intended to take up a role at the library of a local college. The Criminal Records Bureau (CRB) (the predecessor body of the DBS) notified the claimant that the two reprimands would appear on his enhanced disclosure certificate and proposed adding an explanatory comment about the circumstances of the offences. At this point, the claimant wrote to the Chief Constable asking her to erase the record, arguing that, in view of the circumstances of the offence, the reprimand should never have been issued. The Chief Constable refused on the grounds that the reprimands had been lawfully administered and there was insufficient reason, within the terms of the applicable policy, to erase the records.

The claimant issued judicial review proceedings, seeking an order quashing the Chief Constable’s decision refusing to erase the data. In the event his claim against the Chief Constable failed, the claimant sought declaratory relief in the form of a declaration of incompatibility under the Human Rights Act 1998 on the basis that the regime of statutory disclosure under the Police Act 1997 (specifically the automatic disclosure of ‘all relevant matters’) resulted in an unjustified interference with his right to respect for private life, pursuant to Article 8 of the European Convention on Human Rights.

The judgment

The challenge to the lawfulness of the Chief Constable’s refusal to delete the record of the 2006 reprimand failed; the Court found that the reprimand had been lawfully issued and that the exercise of discretion by the Chief Constable in relation to the deletion of the record was not therefore flawed.

However, in relation to the requirement under the Police Act that any caution or reprimand for any offence included in Schedule 15 of the Criminal Justice Act 2003 must be included in an enhanced disclosure certificate, irrespective of the
nature of the offence, the age of the offender at the time of the caution, the subsequent passage of time and good behaviour, and the relevance of the data to employment sought, the Court found that the absence of a review mechanism that would allow assessment of whether disclosure was relevant or necessary, meant there were insufficient safeguards for the claimant’s Article 8 rights.

In reaching this conclusion the Court took a series of considerations into account. Having regard to international law relating to the welfare of the child, the Court noted that disclosure of a child’s reprimand can have a deleterious effect on subsequent social life, and that disclosure should only take place where strictly necessary and proportionate. The Court also noted that the claimant’s 2006 offence had been a borderline case for a reprimand, that the CPS had not thought it in the public interest to give him a criminal record and that at the time of the offence it was not the practice of the police to retain central records of reprimands given to a juvenile for more than a short period. The Court found there was a compelling case for saying that a review mechanism, allowing all relevant considerations to be taken into account, was needed and was practicable. It suggested that this might be achieved by adjusting the statutory scheme so that spent convictions and cautions are no longer recorded automatically on enhanced disclosure certificates but instead are treated as ‘intelligence data’ that should be disclosed only where relevant and proportionate to the specific disclosure application. The Secretary of State will now have to consider whether to revise the statutory scheme for enhanced disclosure checks in line with the Court’s judgment.

**EU News**

4 May 2016  
**General Data Protection Regulation (GDPR) published in the Official Journal of the EU**

On 4 May, the GDPR was published in the Official Journal of the European Union. The GDPR is effective now, and will apply to organisations on 25 May 2018.

Bird & Bird’s comprehensive guide to the GDPR is available [here](#).

Please contact us if you would like further information on how we might be able to help you with any queries relating to the GDPR.
14 April 2016

**Article 29 Working Party publishes opinion on EU-US Privacy Shield**

More information on this development can be found [here](#).

12 April 2016

**Joined cases C-698/15 R (Davis, Watson, Brice & Lewis) v Secretary of State for the Home Department and C-203/15 Tele 2 Sverige AB v Post-och Telestyrelsen**

On 12 April, the CJEU heard oral submissions from various Member State governments in response to challenges to national legislation mandating retention of data produced by public electronic communication service providers, and access to such data by intelligence and law enforcement agencies. The Advocate General will deliver his opinion on 19 July 2016.

In 2014, the CJEU ruled that the Data Retention Directive (EU Directive 2006/24/EC) was invalid because it was contrary to Articles 7 and 8 of the EU Charter of Fundamental Rights. In these two joined cases, the CJEU has been asked to rule on the application of Articles 7 and 8 on Member States’ data retention and data access regimes – including the lawfulness of the current UK regime.

11 April 2016

**Online public consultation for the revision of Directive 2002/58/EC, the "ePrivacy Directive"**

On 11 April 2016, the European Commission announced the launch of an online public consultation regarding the revision of Directive 2002/58/EC on privacy and electronic communications as amended (the "ePrivacy Directive"). This text provides specific rules for the telecommunications industry but also general provisions (applicable to any organisation) in areas such as (i) electronic direct marketing and (ii) the use of cookies or similar technologies.

Following the launch of the public consultation, the European Commission organised a kick-off workshop on 12 April 2016 where the following was discussed:

**From a Directive to a Regulation?**

There seems to be a growing consensus around the idea that the revised ePrivacy rules should be produced by way of a regulation (i.e. a text directly applicable to all EU Member States) instead of a directive (i.e. a legal instrument which can only be deployed into the national legal framework of each Member State by way of implementing legislation). The recurring arguments in favour of such an approach are as follows: (i) the necessity to avoid a “regudirective”; (ii) to prevent confusion similar to that experienced during the implementation of the cookie rules; and (iii) to follow the path used for the revision of Directive 95/46/EC on Data Protection (the "Data Protection Directive"), due to be replaced by the General Data Protection Regulation (the "GDPR") as from 25 May 2018.
At present, the ePrivacy Directive needs to be read in conjunction with the Data Protection Directive as the two texts work together. With the replacement of the Data Protection Directive by the GDPR, the ePrivacy Directive will need to be revisited so as to be in line with the new rules. One illustration of this can be found in the growing importance of the role and type of consent under the GDPR rules. For instance, Art 7.1 of the GDPR provides that “where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data”. The European Commission will have to clarify whether this would require organisations using electronic direct marketing to implement a so-called “double opt in” procedure as already exists in Germany (i.e. under German laws, companies are currently required to obtain a prior express consent from individuals when conducting electronic direct marketing activities. As a result, email addresses in Germany must be confirmed before they are added to a distribution list. A request for confirmation must be sent to the submitted address and the recipient must take some action to confirm that he indeed wants to be added to the distribution list. Most often, the confirmation action is as simple as replying to the confirmation request or clicking on a link).

**OTT and semi-public Wi-Fi operators to be caught and telco-specific breach notification regime to be abolished?**

The public consultation is also aimed at getting the European Commission into line with today's technologies. There is an open question as to whether over the top (“OTT”) actors (e.g. messenger applications provided by social media or application providers) and semi-public Wi-Fi operators (e.g. the provision of Internet access in coffee shops or stores) should be subject to the various telco-specific obligations provided in the ePrivacy Directive. The workshop was used as a platform by many attendees to relay the message that the current telco-specific breach notification obligations provided in the ePrivacy Directive and Regulation 611/2013 should be abolished. Affected telco-organisations should instead be subject to the general breach notification regime provided under the GDPR where a longer period of time for notification applies.

**Cookies and similar technologies**

The European Commission is seeking views as to whether the current cookie rules should be amended. It has, for instance, been argued that requesting users' consent to the storage/access of information on their devices, in particular tracking cookies, may disrupt the Internet experience. The European Commission would like to know if new options should be considered (e.g. effective browser settings, Do-Not-Track standard, a self-regulatory regime and others).
The European Commission invites all interested parties to respond to the online public consultation before 5 July 2016. The European Commission intends to (i) review all expressed comments and (ii) carry out the necessary impact assessments over summer and autumn 2016. The plan is that a first draft proposal will be presented by the European Commission in December 2016. Whether this ambitious deadline will be met remains to be seen. However, organisations should take the online public consultation as an opportunity to express their views and contribute to the debate. Should you need assistance in this respect or would like to be represented, our data protection experts in over 14 EU countries will be happy to help.

**European Commission publishes draft "adequacy decision" and texts for EU-US Privacy Shield**

More information on this development can be found [here](http://example.com)

On the same day the ICO issued an updated blog post, ‘Safe Harbor: Calmer waters on the horizon’. This confirmed that the ICO’s position remains the same as that stated in October, namely that the ICO will not be seeking to expedite complaints about Safe Harbor while the process to finalise its replacement is still ongoing. They also refer to their interim guidance which consolidates their views to date.

**ECtHR**

**31 March 2016**

*Santare and Labaznikovs v Latvia 34148/07 (Court (Fifth Section)), [2016] ECHR 315*

The applicants brought proceedings relating to the use of intercepted phone conversations in criminal proceedings. Their complaint about fairness of proceedings was inadmissible due to lapse of time. Their complaint about breach of privacy rights was partly successful – however, the case is another reminder that the ECtHR is inclined to view the decision itself as sufficient remedy and that damages will be low – here EUR 1,500 to each applicant for non-pecuniary damage.

**The facts**

The applicants in this case were two Latvian nationals, Mrs Lilija Santare (the "first applicant"), a board member of the second applicant’s company, and Mr Vladimirs Labaznikovs (the "second applicant"), the owner of a chain of pharmacies in Latvia at the time.
Earlier trial

After an undercover operation involving the Bureau for the Prevention and Combating of Corruption (the "KNAB"), on 15 July 2015 a criminal case concerning both applicants was brought. The second applicant was found guilty of bribing a State official by attempting to prevent any further investigation into his business and corrupt State officials connected with it. He was given a two year suspended custodial sentence. The first applicant was acquitted.

On 8 November 2005, the prosecutor submitted an appeal which disputed the acquittal of the first applicant and which asked for an upgrade to the second applicant's sentence. The second applicant's suspended sentence was withdrawn on 31 October 2006 (at which point he was imprisoned). The first applicant was thereafter found guilty of aiding and abetting by the appellate court and given a one year suspended custodial sentence. In an appeal, the first applicant argued that tapped phone conversations should not have been admitted as evidence, since they had been obtained without the correct authorisation. The second applicant argued that the appellate court had not assessed the lawfulness of the phone tapping and had ignored the fact that the criminal case had contained no reference to any authorisation to carry out the above activity (as prescribed by Article 176 of the Code of Criminal Procedure). On 19 January 2007, the Senate of the Supreme Court dismissed the appeal.

In 2012, the applicants decided to bring their case to the European Court of Human Rights (the "Court"). They alleged that the covert interception of their telephone conversations via phone-tapping had not been carried out in compliance with Article 8 of the European Convention on Human Rights ("ECHR"). In addition, they complained under Article 6 ECHR that comments made by the Minister of Justice regarding the lower court's judgment had been "prejudicial" to the "fairness" of the appeal.

The judgment

Article 8(1) ECHR provides that, "Everyone has the right to respect for his private and family life, his home and his correspondence." Article 8(2) ECHR provides that, "There shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others."

The Latvian Government argued that the applicants had not exhausted their domestic remedies and had failed to comply with the six-month rule (the six-month time-limit in which a case can be brought). The applicants challenged the Government's arguments, and the Court agreed with the applicants, finding that their complaints under Article 8 "could not be inadmissible for non-exhaustion of domestic remedies" and were "not manifestly ill-founded" in relation to the six-month rule.
As regards the applicants' Article 8 rights, the Government did not dispute that there had been an interference with the applicants' rights to respect for private life. Nevertheless, they argued that the interference had been "lawful" and had "pursued a legitimate aim", and that the contested interception of the applicants' telephone conversations had been "carried out in accordance with the Law on Operational Activities". The applicants, meanwhile, maintained that in their criminal proceedings there had been no Supreme Court decision authorising the interception of their phone conversations (as required by Article 176 of the Code of Criminal Procedure). They argued that the information provided by the Government did nothing more than show the existence of an entry in the register.

The Court did not dispute that the covert interception of the applicants' telephone conversations amounted to an interference within the meaning of Article 8 ECHR. However, when deciding whether the interference was justified in light of paragraph 2 of Article 8 ECHR, the Court had to assess whether the authorities acted "in accordance with the law" (pursuant to one or more legitimate aims), and whether the measure in dispute was "necessary in a democratic society".

The Court established that the interception of the applicants' phone conversations had "a legal basis in domestic law", and that the legal basis was "accessible" to the applicants. The Court was then required to assess whether the retrospective judicial review of the lawfulness of the phone tapping was carried out "in accordance with the law", and whether "the judicial review provided additional safeguards against arbitrariness during the adjudication of the criminal proceedings against the applicants." The Court determined that in the course of the criminal proceedings, the applicants could not be sure that the interference with their rights under Article 8 ECHR had been carried out on the basis of previous judicial authorisation.

A violation of Article 8 ECHR had therefore occurred, and the court did not need to further assess whether the measure in dispute was "necessary in a democratic society".

As regards the alleged violations of Article 6 ECHR, the applicants' complaint was lodged out of time and was rejected.

In accordance with Article 41 ECHR, the Court decided on an equitable basis to award each applicant EUR 1,500 in respect of non-pecuniary damage as a result of the violation of their Article 8 ECHR rights. EUR 800 was also awarded to the second applicant to cover legal and postal expenses.
## Enforcement Table

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity</th>
<th>Description of breach</th>
<th>Summary of steps required (in addition to the usual steps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 May 2016</td>
<td>Check Point Claims Ltd</td>
<td>Monetary penalty notice of £250,000.</td>
<td>Monetary penalty notice of £250,000.</td>
</tr>
</tbody>
</table>

In June 2015, the Commissioner's office identified that a number of complaints had been received about the receipt of automated marketing calls relating to hearing loss claims. The recorded message did not identify the sender or instigator of the calls. However, on further investigation it was discovered that two of the CLI's identified by the complainants were allocated to Check Point Claims Ltd (the "Company").

The ICO wrote to the Company on 9 September 2015, and on 1 October 2015, the Commissioner's office received a response from the Company stating that it had purchased “opted-in” data from a data provider. The Company was also unaware of the requirement to comply with regulation 24 of the PECR.

Following additional correspondence between the ICO and the Company, evidence of freely given consent by subscribers was not forthcoming. The relevant communications service provider subsequently confirmed that the Company had sent or instigated 17,565,690 automated marketing calls between 30 March 2015 and 30 September 2015, although the calls were connected to approximately 6,388,122
subscribers.

During this period, the Commissioner's office received 248 complaints about automated marketing calls made at inconvenient times such as evenings and weekends.

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 May 2016</td>
<td>Better for the Country Ltd</td>
<td>Monetary penalty</td>
<td>Better for the Country Ltd (the &quot;Company&quot;) campaigns for the UK to leave the European Union, formerly under the name The Know and now as Leave.EU. As part of this campaign, it sent unsolicited direct marketing text messages. Between 1 May 2015 and 7 October 2015, 134 complaints were made to the 7726 spam text reporting service about the receipt of unsolicited direct marketing text messages sent by the Company. In the same period 6 complaints were made direct to the Commissioner. The ICO contacted the Company and it replied on 30 October 2015 and explained that some text messages had been sent to individuals who had registered as supporters of the campaign on the Company's website. However, the remainder were sent to individuals whose details had been obtained from a third party data supplier. The Company explained that the data obtained from the third party supplier was “double opt-in consented for government and local government marketing”. The Company subsequently confirmed that it had sent a total of 501,135 text messages between 1 May 2015 and 7 October 2015 to individuals whose details had been obtained from the third party supplier.</td>
</tr>
<tr>
<td>Date</td>
<td>Organization</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------</td>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 10 May 2016| **Sirona Care and Health**            | Undertaking follow-up       | This action concerned an ICO “follow-up” assessment of the actions taken by Sirona Care and Health (the "Provider") in relation to an undertaking it signed in November 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented. The review demonstrated that the Provider had taken the following appropriate steps to address the requirements of the undertaking:  
- ensured that mandatory annual data protection refresher training is in place for all staff who routinely process personal data;  
- ensured that the completion rate of data protection training sessions is monitored;  
- reviewed its policies to ensure that appropriate advice is provided to staff on email checking procedures and that these are readily accessible to its employees; and  
- implemented other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage. | N/A                         |
| 9 May 2016 | **Chelsea and Westminster Hospital NHS Foundation Trust** | Monetary penalty            | 56 Dean Street (Soho) (the "Clinic") is a clinic within the Chelsea and Westminster Hospital NHS Foundation Trust (the "Trust"). In March 2010, a member of staff in the Trust’s Pharmacy Department sent a questionnaire to 17 patients in relation to their access to HIV treatment. The email addresses were entered into the “to” field instead of the blind carbon copy. Monetary penalty notice of £180,000. | N/A                         |
The recipients of the email could therefore see the email addresses of all the other recipients.

The Trust put in place some remedial measures following this security breach. However, there was no specific training to remind staff to double check that the group email addresses were entered into the correct field. In addition, the Trust did not replace the email account it was using with an account that could send a separate email to each service user on the distribution list.

On 1 September 2015, a member of staff in the Clinic sent a newsletter to the 781 subscribers of the Option E service. The email addresses were again entered into the “to” field instead of the blind carbon copy (“bcc”) field in error. The recipients of the email could therefore see the email addresses of all the other recipients. The Commissioner understands that 730 out of the 781 group email addresses contained the full names of service users.

<table>
<thead>
<tr>
<th>4 May 2016</th>
<th>Blackpool Teaching Hospitals NHS Foundation Trust</th>
<th>Monetary penalty</th>
<th>Blackpool Teaching Hospitals NHS Foundation Trust (the &quot;Trust&quot;) is required to publish equality and diversity metrics annually on its website.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>On 30 January 2015, the equality and diversity lead in HR asked the electronic staff records team for metrics held on the electronic staff records system. A team member searched the Trust’s website to check the format of the Excel spreadsheets for 2013 so that they could be replicated. He clicked on a pivot-table and it was discovered that the associated data to the ‘protected groups’ and ‘equality pay bands’</td>
</tr>
</tbody>
</table>
spreadsheets could also be accessed via a pivot table.

The spreadsheets contained confidential and (sensitive) personal data relating to 6,574 employees (past and present) including the employees’ name, pay scale, NI number and date of birth. They also contained their ‘disabled’ status, ethnicity, religious belief and sexual orientation.

It subsequently transpired that the spreadsheets had been publicly available on the Trust’s website for 11 months. During that time, the pivot tables were accessed at least 59 times by 20 visitors. The associated data was also downloaded by persons unknown on several occasions.

| 29 April 2016 | Doncaster Metropolitan Borough Council | Undertaking follow-up | This action concerned an ICO “follow-up” assessment of the actions taken by Doncaster Metropolitan Borough Council (the "Council") in relation to an undertaking it signed on 27 July 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented.

The review demonstrated that the Council had not taken appropriate steps to address the requirements of the undertaking.

It had neglected to:

- conduct a training need analysis for all roles within the organisation to ascertain the level of data protection awareness required for the role, and the frequency at which the individual should receive refresher training;

The Council should take further action as follows:

- establish a suitable method of delivering data protection training to all staff who handle personal or sensitive personal data on a regular basis;
- ensure that all staff receive data protection training, to be refreshed at regular intervals; and
- implement a method for monitoring the completion of mandatory records management training.
• deliver mandatory data protection training to the relevant individuals, and at the intervals agreed; and

• ensure all staff required to undertake mandatory training complete the training within the timescales identified.

### 29 April 2016

**Martin & Company**

**Undertaking follow-up**

This action concerned an ICO “follow-up” assessment of the actions taken by Martin & Company (the "Company") in relation to an undertaking it signed on 14 September 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented.

The review demonstrated that the Company had taken appropriate steps to address some of the requirements of the undertaking.

However, further work will need to be completed by the Company to fully address the agreed actions.

In particular, the Company confirmed that it had taken the following steps:

• implemented procedures relating to the collection of paper and electronic media containing sensitive and personal data from third parties; and

• staff have been made aware of these policies and provided with guidance on how to follow them via a staff training memo.

The Company should take further action as follows:

• work on addressing the issue of encrypting portable media used to store and transfer personal data;

• stop permitting company emails to be forwarded to users’ Hotmail accounts which is considered bad practice by the ICO;

• proof read staff policy documents; and

• introduce a more comprehensive data protection training such as the National Archives free ‘Responsible for Information’ e-learning training course.
<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
</table>
| 28 April 2016 | West Dumbartonshire Council            | Enforcement notice       | The Commissioner's office completed a consensual audit of West Dumbartonshire Council (the "Council") in January 2013. This audit provided “reasonable assurance”. It then carried out a follow-up audit in November 2013. This audit showed that some progress had been made, but that certain recommendations had not been fully implemented. Following a security breach on 21 July 2014, a further investigation was carried out. The Commissioner's Office subsequently determined that the Council had failed to comply with the requirements of section 7 of the Data Protection Act. The Council shall, within 6 months of the Notice, ensure that:  
- there is a mandatory data protection training programme for all staff (including new starters) and refresher training on an annual basis;
- completion of such training is properly documented and monitored to ensure training is completed within an appropriate timeframe; and
- a home-working policy is implemented to provide sufficient guidance for staff working remotely. |
<p>| 27 April 2016 | Nevis Home Improvements Ltd            | Monetary penalty          | Nevis Home Improvements Ltd (the &quot;Company&quot;) is a company that sells products designed to improve energy efficiency in the home. Between 21 May and 27 August 2015, the Commissioner’s office received 175 complaints via the online reporting tool. The TPS received 8 complaints. The gist of the complaints was that automated marketing calls had been received. On further investigation, it transpired that between 21 May and 27 August 2015, the Company had sent or instigated 2,530,549 automated marketing calls, 1,538,682 of which were connected. When questioned, the Company informed the Commissioner’s office that it had purchased “opt-in” data from a reputable supplier and that the Monetary penalty notice of £50,000. |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Company/Individual</th>
<th>Action</th>
<th>Details</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 April 2016</td>
<td><strong>Getwork2day Ltd</strong></td>
<td>Prosecution</td>
<td>Getwork2day Ltd, a company involved in web based recruitment, was prosecuted at Worthing Magistrates’ Court for failing to notify with the ICO. Getwork2day Ltd was found guilty of a section 17 non-notification offence and fined £500. It was also ordered to pay £951.79 costs and a £50 victim surcharge.</td>
<td>Getwork2day Ltd was found guilty of a section 17 non-notification offence and fined £500. It was also ordered to pay £951.79 costs and a £50 victim surcharge.</td>
</tr>
<tr>
<td>21 April 2016</td>
<td><strong>Chief Constable of Kent Police</strong></td>
<td>Monetary penalty</td>
<td>The Commissioner has found that Kent Police processed (sensitive) personal data in contravention of the seventh data protection principle in Part I of Schedule 1 to the DPA. Monetary penalty notice of £80,000.</td>
<td>Monetary penalty notice of £80,000.</td>
</tr>
<tr>
<td>20 April 2016</td>
<td><strong>Health and Social Care Information Centre (HSCIC)</strong></td>
<td>Undertaking</td>
<td>The Health and Social Care Information Centre (&quot;HSCIC&quot;) has signed an undertaking committing the Trust to ensure that personal data are processed in accordance with the First Data Protection Principle in Part I of Schedule 1 to the Act, and in particular:</td>
<td>The data controller shall ensure that personal data are processed in accordance with the First Data Protection Principle in Part I of Schedule 1 to the Act, and in particular:</td>
</tr>
</tbody>
</table>

Data had been screened against the TPS list before it was added to its database. However, it was subsequently unable to provide any evidence of freely given consent by subscribers.
The ICO has found that patients were offered an opportunity to opt out from their data being shared with other organisations, but that the opt-outs were not implemented. HSCIC have agreed a series of steps to remedy this.

- HSCIC should establish and operate a system to process and uphold Type 2 objections;
- HSCIC should ensure that any patients affected by this incident can be made aware that it is possible that their personal data has been shared with third parties against their wishes;
- HSCIC should ensure that any patients who have previously registered a Type 2 objection, or patients who register a Type 2 objection in the future, are provided with clear fair processing information that enables them to understand how the Type 2 objection will be applied and how their data will be used;
- HSCIC should contact recipients of data sets it provided in the period January 2014 – April 2016 and make them aware that the datasets may include records relating to patients who have chosen to opt out;
- HSCIC should contact recipients of data sets it provided in the period January 2014 – April 2016 and where the agreement allowed the recipient to onwardly disseminate the data, to make them aware that this data should no longer be disseminated further;
HSCIC should contact recipients of data sets it provided in the period January 2014 – April 2016 to inform them that, where possible, the data sets should be destroyed or deleted and replaced with a new data set, which reflects patient opt outs, provided by HSCIC in its place; and

HSCIC should revisit the matter of objections following the completion of the National Data Guardian review and consider whether its systems and processes can be modified to allow the Type 2 objection to be applied in circumstances where this is not currently possible.

| 15 April 2016 | Croydon Health Services NHS Trust | Undertaking follow-up | This action concerned an ICO “follow-up” assessment of the actions taken by Croydon Health Services NHS Trust (the “Trust”) in relation to an undertaking it signed on 14 December 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented. The review demonstrated that the Trust had taken appropriate steps and put plans in place to address some of the requirements of the undertaking. However, further work will need to be completed by the Trust to fully address the agreed actions. In particular, the Trust confirmed that it had taken the following steps: |
|---------------|---------------------------------|----------------------|-------------------------------------------------|-------------------------------------------------|

The Trust should take further action as follows:

- ensure that the work around training continues to improve IG training figures and meet training targets; and
- ensure that legacy record destruction continues.
- key priority has been given to achieving IG training targets and staff awareness;
- all staff on the complaints team have completed data protection training in addition to the mandatory IG training;
- the ICO were informed that attendance at data protection training sessions is monitored and there are appropriate follow up procedures in place to ensure completion;
- information assets were reviewed for data flows and information risk assessments were conducted;
- a records disposal option for legacy records was implemented;
- a correspondence checking procedure was implemented and brought to the attention of all staff;
- the implementation of the recommendations from the data protection incident investigation report were monitored;
- the ICO was supplied with evidence in relation to progress against the objectives in the undertaking within the allotted time; and
- reviewed and updated a number of documents.

11 April 2016  Brunel University London  Undertaking follow-up  This action concerned an ICO “follow-up” assessment of the actions taken by Brunel University London (the “University”) in relation to an undertaking it signed on 28 July 2015 to A few additional points were, however, raised. The University should:
* ensure the data protection training
provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented.

The review demonstrated that the University had taken appropriate steps and put plans in place to address the requirements of the undertaking.

- ensure that completion of refresher training once a staff member has passed probation is robustly monitored.

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 April 2016</td>
<td>David Barlow Lewis</td>
<td>Prosecution</td>
<td>Former Liverpool Victoria employee David Barlow Lewis was prosecuted at Bournemouth Magistrates’ Court for attempting to commit a section 55 Data Protection Act offence, by attempting to obtain personal data without the data controller’s consent.</td>
<td>Mr Lewis pleaded guilty to the offence and was fined £300, ordered to pay £614.40 costs and a £30 victim surcharge.</td>
</tr>
<tr>
<td>5 April 2016</td>
<td>Flybe Limited</td>
<td>Undertaking</td>
<td>This action concerned an ICO “follow-up” assessment of the actions taken by Flybe Limited (the &quot;Company&quot;) in relation to an undertaking it signed on 16 February 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented.</td>
<td>A few additional points were, however, raised. The Company should:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The review demonstrated that the Company had taken appropriate steps and put plans in place to address the requirements of the undertaking.</td>
<td>- ensure that all employees that access personal data complete information security training before they are given access to personal data;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- display their new data protection awareness posters, as planned; and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- roll out the DPA e-learning module, as planned.</td>
</tr>
<tr>
<td>5 April 2016</td>
<td>Keurboom Communications Limited</td>
<td>Prosecution</td>
<td>Keurboom Communications Limited and its Director, Gregory Rudd, were prosecuted at Luton Magistrates’ Court for failing to comply with a third-party information notice issued by the Commissioner in relation to an ongoing investigation for PECR breaches.</td>
<td>Keurboom Communications Limited pleaded guilty to the offence and was fined £1500, ordered to pay £435.95 costs and a £120 victim surcharge. Mr Rudd was fined £1000, ordered to pay £435.95 costs and a £100 victim surcharge.</td>
</tr>
<tr>
<td>Date</td>
<td>Company</td>
<td>Type</td>
<td>Description</td>
<td>Monetary penalty</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>1 April 2016</td>
<td>Advice Direct Ltd</td>
<td>Monetary penalty</td>
<td>The business of Advice Direct Ltd (the &quot;Company&quot;) involves calling people to try to generate leads for potential claims in relation to hearing loss as a result of working in loud environments. Between 7 April 2015 and 31 July 2015, the ICO received 57 complaints about the Company. During the same period, the TPS received 160 complaints about the Company.</td>
<td>Monetary penalty notice of £20,000.</td>
</tr>
<tr>
<td>29 March 2016</td>
<td>M I Wealth Management Ltd</td>
<td>Enforcement notice</td>
<td>M I Wealth Management Ltd (the &quot;Company&quot;) has been ordered to respond to a subject access request after the ICO ruled that it had failed to comply with the requirements of section 7 of the Data Protection Act.</td>
<td>The Company shall, within 30 days of the Notice: • inform the complainant whether the personal data processed by the data controller includes personal data of which the complainant is the data subject and shall supply him with a copy of any such personal data so processed in accordance with the requirements of section 7 of the DPA and the Sixth Data Protection Principle in that respect, subject only to the proper consideration and application of any exemption from, or modification to, section 7 of the DPA provided for in or by virtue of Part IV of the DPA which may apply.</td>
</tr>
<tr>
<td>24 March 2016</td>
<td>Direct Choice Home Improvements Ltd</td>
<td>Enforcement notice &amp; monetary penalty</td>
<td>The ICO first wrote to Direct Choice Home Improvements (the &quot;Company&quot;) in June 2014 following a number of complaints about unsolicited direct marketing calls. Since the volume of complaints was relatively low, the Commissioner provided the Company with advice and guidance on compliance with the PECR</td>
<td>The Company shall, within 35 days of the Notice: • neither transmit, nor instigate the transmission of, communications comprising recorded matter for direct marketing purposes by means of an automated calling system except:</td>
</tr>
</tbody>
</table>
rather than take regulatory action at that time.

However, in May 2015, the Company was in the top 20 list of companies about which the TPS received the most complaints. The Commissioner therefore wrote to the Company on 15 July 2015, providing a list of the complaints made to the TPS in May 2015 and asking for evidence that it had the consent of the subscribers to make those calls.

The Company subsequently maintained that the ICO's letters had not been received. On 26 August 2015, the Commissioner sent further letters to the Company.

On 3 September 2015, the Company replied to the Commissioner by returning a copy of the list of TPS complaints marked with the name of the third-party who had supplied it with the data it had used to make marketing calls. The Company later explained that it had received assurances from the third-party that the data provided had been screened against the TPS register.

Between 29 April 2015 and 29 September 2015, 167 complaints were made about unsolicited direct marketing calls made by the Company. 118 of those complaints were made to the TPS, with a further 49 made direct to the ICO. All of these complaints were made by individual subscribers who were registered with the TPS.

(a) where the called line is that of a subscriber who has previously notified the Company that for the time being he consents to such communications being sent by, or at the instigation of, the Company; and

b) where the communication includes the name of the Company and either the address of the Company or a telephone number on which the Company can be reached free of charge.

AND

Monetary penalty notice of £40,000.

The Company shall, within 35 days of the Notice:

- neither transmit, nor instigate the transmission of, communications comprising recorded matter for direct marketing purposes by means...
Between 26 June 2015 and 31 October 2015, the ICO received 5,535 complaints about automated direct marketing calls made by the Company. The recorded messages sent did not always identify the sender or instigator of the call.

On 26 August 2015, the ICO wrote to the Company to remind it of its obligations and asking it to provide evidence that the recipients of the calls had consented to receiving automated marketing calls from the Company.

The Company informed the ICO that the automated calls had been made on its behalf by a third party, which also provided the data.

Despite informing the ICO that it had ceased making automated calls by the end of June 2015, complaints about such calls continued to be received.

The Commissioner subsequently established that between 26 June 2015 and 7 September 2015, the Company made 2,475,481 automated direct marketing calls.

of an automated calling system except:

(a) where the called line is that of a subscriber who has previously notified the Company that for the time being he consents to such communications being sent by, or at the instigation of, the Company; and

b) where the communication includes the name of the Company and either the address of the Company or a telephone number on which the Company can be reached free of charge.

AND

Monetary penalty notice of £140,000.

24 March 2016 Age International Voluntary undertaking Age International has signed an undertaking committing the charity to best practice around fundraising calls.

This action follows an article published in the Daily Mail on 7 July 2015, as a result of which the Commissioner launched an investigation into the direct marketing practices of the charity sector.

N/A

23 March 2016 Anxiety UK Undertaking follow-up This action concerned an ICO “follow-up” assessment of the actions taken by Anxiety UK (the “Charity”) in relation to an undertaking it

The Charity should take further action as follows:
signed on 3 August 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented.

The review demonstrated that the Charity had taken appropriate steps and put plans in place to address some of the requirements of the undertaking. However, further work will need to be completed by the Charity to fully address the agreed actions.

In particular, the Charity confirmed that it had taken the following steps:

- commissioned a new website that has been designed to reduce exposure to vulnerabilities; and
- implemented appropriate retention, review and disposal controls.

The Charity has also taken other measures to develop information security:

- an external data security review was undertaken in January 2016;
- information security policies have been updated;
- the Anxiety UK Board of Trustees is monitoring an Information Governance Project plan; and
- staff data protection training has been rolled out which was tested by a quiz.

- a key recommendation was that the Charity enters into data sharing agreements with all partners in the supply chain. Agreements are in place with all partners except Zen Desk. It appears that this outstanding agreement will be completed shortly.
The South Eastern Health & Social Care Trust (the "Trust") has signed an undertaking committing the Trust to ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I Schedule 1 to the Act.

This action follows two separate incidents involving the disclosure of personal data in error which led the Commissioner to undertake a formal investigation into the Trust’s compliance with the Act.

One incident concerned a breach of confidentiality by a locum doctor who left unsecured patients’ records in a private rental property they had vacated. It became apparent that the doctor had removed significant personal sensitive information from the Trust without approval from senior medical colleagues or management.

Another incident was reported to the Commissioner in which a staff member emailed a confidential document to her personal email account and on review of the email address realised that she had entered it incorrectly. Enquiries revealed that the information disclosed in this case was extremely sensitive. However, it is noted that the Trust has a suite of policies in place which cover the use of email, Trust equipment and remote working standards. Despite a lack of appropriate training, the member of staff confirmed their awareness of Trust policies and their responsibilities in this regard and breached these policies by emailing sensitive personal data to a non-Trust email and to a non-Trust issued encrypted device.

The data controller shall ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

- all staff, including locum doctors, 3rd party contractors, temporary (agency/bank staff) and volunteers, whose role involves the routine processing of personal and sensitive personal data, undertake mandatory training;
- the provision of such training shall be recorded and monitored with oversight provided at a senior level against agreed KPIs to ensure completion;
- staff, including locum doctors, 3rd party contractors, temporary (agency/bank staff) and volunteers are aware of the content and location of its policies and procedures relating to the processing of personal data; and
- the data controller shall implement such other security measures as are appropriate.
<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Action/Notice</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 March 2016</td>
<td><strong>Cambridgeshire Community Services NHS Trust</strong></td>
<td>Undertaking follow-up</td>
<td>This action concerned an ICO “follow-up” assessment of the actions taken by the Cambridgeshire Community Services NHS Trust (the “Trust”) in relation to an undertaking it signed on 20 July 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented. The review demonstrated that the Trust had taken appropriate steps and put plans in place to address the requirements of the undertaking.</td>
</tr>
<tr>
<td>17 March 2016</td>
<td><strong>FEP Heatcare Ltd</strong></td>
<td>Enforcement notice &amp; monetary penalty</td>
<td>FEP Heatcare Ltd (the “Company”) initially came to the attention of the ICO in February 2015 when it appeared in the Telephone Preference Service’s twenty most complained about organisations making unsolicited direct marketing calls to TPS subscribers. The ICO wrote to the Company alerting it to the complaints, and reminding it that making unsolicited direct marketing telephone calls to individuals who have subscribed with the TPS was a contravention of regulation 21 of PECR. The Company explained that it relied on data provided by a third party supplier which it was assured was compliant. The ICO advised the Company that, as the instigator of marketing calls, it was responsible for ensuring compliance with PECR. The Company was subsequently placed under a period of monitoring for 3 months. In June 2015, the ICO identified that a number of complaints had been received about the receipt of automated direct marketing calls relating to boiler replacements. The recorded message did not identify the sender or instigator of the call. The Company shall, within 35 days of the Notice: • neither transmit, nor instigate the transmission of, communications comprising recorded matter for direct marketing purposes by means of an automated calling system except: (a) where the called line is that of a subscriber who has previously notified the Company that for the time being he consents to such communications being sent by, or at the instigation of, the Company; and (b) where the communication includes the name of the Company and either the address of the Company or a telephone number on which the Company can be reached free of charge.</td>
</tr>
</tbody>
</table>
However, on further investigation it was discovered that the CLI identified by the complainants was allocated to the Company.

The relevant communications service provider subsequently confirmed that 2,692,217 automated calls were instigated by the Company between 6 April 2015 and 15 July 2015.

Between 18 June 2015 and 5 September 2015, the ICO received 94 complaints about unsolicited automated direct marketing calls made from the CLI allocated to the Company.

AND

Monetary penalty notice of £180,000.

Monetary penalty notice of £5,000.

On 19 August 2015, the ICO became aware that David Lammy MP had made automated telephone calls for the purpose of seeking support for his bid to become the Labour Party’s London Mayoral candidate. On 24 August 2015 the ICO wrote to Mr Lammy to remind him of the requirements of regulation 19 of PECR and to give him an opportunity to provide an explanation for the automated calls that had been made.

Mr Lammy replied on 14 September 2015, confirming that he had instigated a total of 35,629 automated calls that were made on 17 and 18 August 2015. The calls had been made to registered members of the Labour Party. The Labour Party provides membership data to elected representatives or candidates in elections or selections, on the condition that it is only used for the purpose of promoting the candidate in that campaign and not used or disclosed for any other purpose.

When registering to join as a member of the Labour Party, individuals are required to agree to its terms and conditions, which include
acceptance of its privacy policy (www.labour.org.uk/pages/privacy).

The privacy policy contains no indication that information about members will be used to make automated direct marketing calls. Further, prospective members are not asked for consent to the receipt of automated marketing calls from the Labour Party or its elected representatives or candidates.

<table>
<thead>
<tr>
<th>10 March 2016</th>
<th>Chief Constable Wiltshire Constabulary</th>
<th>Undertaking</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Chief Constable of Wiltshire Constabulary has signed an undertaking committing the Constabulary to ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I Schedule 1 to the Act.</td>
<td>The data controller shall ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:</td>
</tr>
</tbody>
</table>

- a suitable method of delivering data protection training to all staff who handle personal or sensitive personal data on a regular basis be introduced;
- data protection training provided to staff be refreshed at regular intervals;
- appropriate records management training be delivered to all staff who are regularly involved with the processing of files containing personal or sensitive personal data;
- the completion of mandatory records management training for such staff and the results reported into a central location to ensure
<table>
<thead>
<tr>
<th>Date</th>
<th><strong>Company</strong></th>
<th>Type</th>
<th><strong>Enforcement notice</strong></th>
<th><strong>Undertaking follow-up</strong></th>
</tr>
</thead>
</table>
| 7 March 2016 | **Wainwrights Estate Agents Limited** | Enforcement notice | Wainwrights Estate Agents Limited (the "Company") has been ordered to respond to a subject access request after the ICO ruled that it had failed to comply with the requirements of section 7 of the Data Protection Act. | The Company shall, within 30 days of the Notice:  
- inform the complainant whether the personal data processed by the data controller includes personal data of which the complainant is the data subject and shall supply him with a copy of any such personal data so processed in accordance with the requirements of section 7 of the DPA and the Sixth Data Protection Principle in that respect, subject only to the proper consideration and application of any exemption from, or modification to, section 7 of the DPA provided for in or by virtue of Part IV of the DPA which may apply. |
| 2 March 2016 | **General Dental Council**            | Undertaking        | This action concerned an ICO "follow-up" assessment of the actions taken by the General Dental Council (the "Council") in relation to an undertaking it signed on 7 September 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented. | The Council should take further action as follows:  
- the data protection training needs of all staff including any role specific training should be clearly documented in a relevant policy of which staff are aware. |
address some of the requirements of the undertaking. However, further work will need to be completed by the Council to fully address the agreed actions.

In particular, the Council confirmed that it had taken the following steps:

- an initial online 'Introduction to Data Protection' SkillBites learning module has been rolled out;
- the Council have worked with an external training provider to develop the content of a classroom based data protection training course;
- Fitness to Practice and Investigating Committee members have received data protection training from key Council staff; and
- data protection training attendance is recorded on the HR system and monitored by the Council.

Further work is yet to be completed by the Council with the following actions planned for 2016:

- all staff will be required to complete data protection refresher training;
- a project to review the content and delivery of the corporate induction to new starters will be presented commenced in February 2016;
- a longer 2.5 hour version of the data protection course has been designed for specific groups;
a wider review of the training requirements of Fitness to Practise panellists, Registration staff and Investigating Committee members is due to take place during 2016; and

the Council will also explore the feasibility of not providing new starters with write-access to the Microsoft Dynamics CRM system until there is an auditable record of a member of staff having completed training.

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 February 2016</td>
<td><strong>Prodial Ltd</strong></td>
<td>Monetary penalty</td>
<td>Prodial (the &quot;Company&quot;) was a company which generated leads in relation to individuals making a claim for a PPI refund.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Between 30 January and 4 September 2015, the Commissioner’s office received 1,122 complaints via its online reporting tool. 719 of those reports were received after 6 April 2015.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The gist of the complaints was that a significant number of automated marketing calls had been received by subscribers in relation to claiming a PPI refund.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>On further investigation, it was discovered that between 6 April and 21 August 2015, the Company sent or instigated 40,204,838 automated marketing calls that were all connected.</td>
</tr>
</tbody>
</table>

Monetary penalty notice of £350,000 to act as a deterrent - the largest fine ever issued for a cold calling operation.
<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Notice Type</th>
<th>Description</th>
<th>Required Action</th>
</tr>
</thead>
</table>
| 28 February 2016 | **Preferred Pension LLP** | Enforcement Notice | Between June 2014 and 23 July 2015, the Commissioner received complaints from individuals who alleged that they had received unsolicited automated marketing calls. The Commissioner subsequently established that Preferred Pension LLP (the "LLP") had instigated the sending of millions of nuisance calls.                                                                                                                                                                                                                       | The LLP shall, within 35 days of the Notice:  
- neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of an automated call unless the recipient of the automated call has previously notified the LLP that he consents for the time being to such communications being sent by, or at the instigation of the LLP; and  
- neither transmit, nor instigate the transmission of a communication for the purposes of direct marketing by means of an automated call unless the particulars mentioned in paragraph 2(a) and (b) of Regulation 24 of the Regulations are provided with that communication. |
| 28 February 2016 | **Advanced VoIP Solutions Ltd** | Enforcement Notice | Between June 2014 and 23 July 2015, the Commissioner received complaints from individuals who alleged that they had received unsolicited automated marketing calls. The Commissioner subsequently established that Advanced VoIP Solutions Ltd (the "Company") had instigated the sending of millions of nuisance calls.                                                                                                                                                                                                                       | The Company shall, within 35 days of the Notice:  
- neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of an automated call unless the recipient of the automated call has previously notified the Company that he consents for the time being to such communications being sent by, or at the instigation of the Company; and |
Between June 2014 and 23 July 2015, the Commissioner received complaints from individuals who alleged that they had received unsolicited automated marketing calls. The Commissioner subsequently established that Money Help Marketing Ltd (the "Company") had instigated the sending of millions of nuisance calls.

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Notice Type</th>
<th>Details</th>
<th>Undertaking</th>
</tr>
</thead>
</table>
| 28 February 2016 | **Money Help Marketing Ltd** | Enforcement notice | The Company shall, within 35 days of the Notice:  
- neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of an automated call unless the recipient of the automated call has previously notified the Company that he consents for the time being to such communications 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 means of an automated call unless the particulars mentioned in paragraph 2(a) and (b) of Regulation 24 of the Regulations are provided with that communication. | British Red Cross has signed an undertaking committing the charity to best practice around fundraising calls. |
| 26 February 2016 | **British Red Cross** | Voluntary undertaking | British Red Cross has signed an undertaking committing the charity to best practice around fundraising calls.                                                                                       | N/A                                                                          |
This action follows an article published in the Daily Mail on 7 July 2015, as a result of which the Commissioner launched an investigation into the direct marketing practices of the charity sector.

24 February 2016 \textbf{Western Health and Social Care Trust} \hspace{1cm} \textbf{Undertaking follow-up} \hspace{1cm} This action concerned an ICO “follow-up” assessment of the actions taken by Western Health and Social Care Trust (the “Trust”) in relation to an undertaking it signed on 28 April 2015 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented.

The review demonstrated that the Trust had taken appropriate steps and put plans in place to address some of the requirements of the undertaking. However, further work will need to be completed by the Trust to fully address the agreed actions.

In particular, the Trust confirmed that it had taken the following steps:

- the Trust’s ICT Disposal Policy was reviewed. The amended policy now sets out conditions for redistribution of ICT equipment. The policy is currently going through the Trust’s approval process and final Trust Board approval is expected in March 2016;

- PCs and laptops that are scheduled for disposal will now have their hard disks removed; the Trust will use two different waste management companies for the disposal of hard disks; and

- the Trust will develop a bespoke training package to address the SAR issues highlighted.

The Trust should take further action on the following:

- current records show that Trust wide completion rates for DP training year to date (Quarters 1-3) stand at 16.5%. The Trust is aiming for an end of year completion rate of 25%. The Trust should aim to have all members of staff, whose role involves the routine processing of personal data, appropriately trained as soon as possible.
MyIML’s (the "Company") business involves making unsolicited marketing calls to individual subscribers in order to sell solar panels and other green energy saving equipment.

In November 2013, the Company was identified by the ICO as being the subject of a large number of complaints about unsolicited marketing calls.

Despite discussions with and warnings given to the Company, between 9 October 2013 and 17 July 2015, the ICO has now established that the Company used a public telecommunications service for the purposes of making 1048 unsolicited calls for direct marketing purposes to subscribers where the number allocated to the subscriber in respect of the called line was a number listed on the register of numbers kept by OFCOM in accordance with regulation 26, contrary to regulation 21(1)(b) of PECR.
17 February 2016  **Direct Security Marketing Ltd**  Monetary penalty  Direct Security Marketing Ltd (the “Company”) provides a range of marketing services to its clients.

The Commissioner’s office received 49 complaints via the online reporting tool. The gist of the complaints was that automated marketing calls were received by subscribers early on 24 August 2015, inviting them to purchase a security system. The calls were made from a withheld number and did not identify the sender.

Subsequently, the Commissioner’s office established that the Company instigated 39,214 automated calls on 24 August 2015, although the calls were only connected to approximately 12,000 subscribers. The Company instigated 9,775 of those calls between the hours of 01:00 and 06:00 in the morning.

Monetary penalty notice of £70,000.