

# Information rights report Quarter 3 2016/17

## Contents

1. Important policy issues
2. Data breaches and other high profile cases
3. Ongoing investigations
4. Enforcement action
5. Consultations
6. Other



## 1. Important policy issues

### **Investigatory Powers Legislation:**

[Redacted]

### **Police use of surveillance technologies –**

[Redacted]

### **Criminal records (retention and disclosure)**

[Redacted]

### **Medical General Practitioner (GP) Systems Providers**

[Redacted]

### **National Data Guardian Review into data security standards, consent and opt outs**

The Secretary of State for Health commissioned the National Data Guardian (NDG) to review and produce a report detailing whether the NHS should offer an opt out of data being used for purposes other than direct care. During the review we participated in the review panel and hosted a meeting to provide them with information on security incidents in the health sector.

Outcomes:

We have responded to the subsequent Department of Health consultation and attended speaking engagements to ensure that NHS bodies are well aware of our views relating to the consent model, in particular.

There has been a significant amount of work relating to anonymisation in the health sector which seems to be emerging from the recommendations of the NDG review.

Future Work:

Now that the consultation has closed we are waiting for the government response. We have also asked to be represented on the working group that has been put together to look at the practicalities of implementing the recommendations of the NDG review around the consent model.

We continue to engage regularly with NHS England and NHS Digital on anonymisation issues. This is something we have been involved with and will remain involved with going forward.

Contact: Strategic Liaison: Stacey Egerton, Victoria Cetinkaya, Ian Inman

### **Digital Economy Bill: data sharing and age verification**

The Digital Economy Bill has completed its progress through the House of Commons and received its Second Reading in the Lords on 13 December 2016. The main elements of ICO interest are provisions for a statutory direct marketing code, data sharing powers and age verification for access to online pornography.

Data sharing powers cover delivery of public services such as fuel poverty and troubled families; research and statistics; fraud; debt and the General Register Office data (births, deaths).

The Commissioner in her oral and written evidence to the Commons Bill Committee called on the government to strengthen safeguards on data sharing and recommended placing references to the ICO's codes on data sharing; privacy impact assessments and privacy notices and transparency on the face of the Bill. She also encouraged the government to undertake further work on the codes of practice accompanying the data sharing powers to improve consistency and align them more closely with ICO codes. The Commissioner has continued to make these points to Ministers in meetings and correspondence. There have also been meetings at official level with the Cabinet Office on developing the codes of practice.

#### Outcome:

Following the Commissioner's appearance before the Commons Committee, the government tabled an amendment that the codes of practice established by the Bill must be consistent with the ICO's statutory data sharing code. The government is listening to our advice on the need for further safeguards on the face of the Bill. During the Lords Second Reading debate a number of Lords called for enhanced safeguards on data sharing and emphasised the importance of adopting privacy by design approach to age verification for access to online pornography.

#### Future work:

The Lords Committee Stage is expected in late-January or February. We shall provide interested Lords with an updated briefing and monitor the Bill's progress through Parliament. We shall continue to engage with the Cabinet Office and DCMS as they develop proposals arising from the Bill

and respond formally when consultations on the codes are launched. We will remain alert to civil society concerns over the data sharing proposals.

Contact: Strategic Liaison: Judith Jones, Jonathan Bamford

### **Electoral arrangements and political parties**

The data protection and privacy issues arising from electoral arrangements continue to feature in our work this quarter. We have provided advice on these issues to a range of organisations and stakeholders.

Outcomes:

In December 2016 we responded to a Cabinet Office consultation on a number of draft Statutory Instruments relating to canvass pilots and other arrangements in England, Wales and Scotland. Also in December we spoke at a meeting of Cabinet Office, Electoral Commission and representatives from the main political parties on issues covered in the ICO's Guidance on Political Campaigning also on GDPR issues relevant to the group.

We have continued to monitor commentary and developments following the publication in August 2016 of Sir Eric Pickles' report 'Securing the ballot' to which the Government issued a formal response in December.

Future work:

We expect to receive further requests for a formal response to the Cabinet Office on electoral arrangements going forward in 2017 and beyond. It is clear that there is an intention to further refine the Individual Electoral Registration arrangements so as to reduce the burden on local authority electoral registration staff whilst at the same time achieving higher levels nationally of registration.

We have been invited to speak again to the group of representatives from the main political parties later in 2017. We will continue to monitor those of Sir Eric Pickles' recommendations that government has indicated it will be taking forward where data protection and privacy issues may arise.

Contact: Strategic Liaison: Judith Jones, Sue Markey

### **HMRC employment history subject access requests**

[Redacted]

## **Energy competition remedies**

[Redacted]

## **Criminal Finances Bill**

The Fourth EU Money Laundering Directive (4MLD) is due to take effect in June 2017, and the Criminal Finances Bill is currently being scrutinised in Parliament. Clauses in the Bill relating to data sharing between regulated entities and the National Crime Agency (NCA) have been introduced which would amend the DPA by creating an additional condition for processing personal data and absolve regulated entities from liability in the event they act in good faith. There is a danger that the proposals would fail to provide sufficient protection for individuals' personal data, and not take into account the requirements of the General Data Protection Regulation.

Outcome:

We have made our concerns clear with officials across government, and have offered to meet with industry to work through and better understand their concerns regarding the existing law.

Future work:

We will be meeting with industry in January 2017 and will continue our engagement with officials from DCMS, HM Treasury and the Home Office. Contact: Strategic Liaison: Garreth Cameron, Meagan Mirza

## **Consumer access to their energy supply data: midata**

[Redacted]

## **Fundraising and Regulatory Compliance Event**

On 21 February the ICO will co-host an event with the Charity Commission and the Fundraising Regulator. The aim of the event is to ensure fundraisers understand their requirements under current laws, explain what measures are in place to help them comply and outline future direction of travel. A handout has been drafted for the event which confirms specific policy positions and will be explained in detail at workshops during the day. The content of the handout will be incorporated into the new Direct Marketing Code of Practice later in 2017.

Next steps: Following the event we will draft a report to be submitted to parliamentary bodies explaining our work on this issue as a whole and how it will improve compliance and reassure the public about fundraising practices.

Contact: Robert Parker/Ian Inman/Richard Marbrow

## **Embedding information rights in higher education**

[Redacted]

## **Research and grants programme**

We are developing the grants and research programme; aiming to launch in the first quarter of 2017. Approval has been given to making available a fund of £200,000 per year for this programme. Applicants will be able to apply for funding to support research and development of privacy enhancing solutions that align with ICO policy priorities.

Next steps: We are developing the governance framework and documentation for the programme. We will also start to put together a communication plan with input from our communications team.

Contact: Jo Pedder/Steve Wood/Lisa O'Brien

## **CCTV and domestic processing**

As mentioned in the 'other' section below, complaints and enquiries about domestic CCTV are growing. We are reviewing our guidance to clarify new policy positions on emerging issues. However, in view of the volume of cases coming in and the nature of the issues we have identified a need to take another look at the overall policy direction in this area. An initial meeting has been held within policy areas and the issues scoped.

Next steps: we are in the process of compiling a report outlining the relevant issues and setting out policy options and recommendations. We are aiming to submit this to SMT (or the appropriate alternative forum once SMT ceases) in February.

## **GDPR**

### **Working Party 29(WP29) Guidelines published**

In late December 2016, the Article 29 Working Party adopted guidelines on data portability, the concept of main establishment and identifying the lead supervisory authority and the role of the Data Protection Officer (DPO). All the guidelines are available for public comment until 31 January. The ICO Overview of the GDPR has been updated to incorporate links to this guidance.

Next steps: Where necessary key concepts from the WP29 guidelines will

be added to the text of the Overview document. We are also in the process of reviewing whether we can develop additional ICO guidance to build on any of the WP29 guidelines, particularly in relation to the provisions related to DPOs.

Contact: Jo Pedder/Hannah McCausland/Carl Wiper

### **Working Party 29 work plan 2017 agreed**

The Working Party has agreed its work plan for 2017. The ICO has been instrumental in influencing the Working Party to adopt a more deadline focussed approach to the production of guidelines. Specifically, our suggestion of a meeting of sub group coordinators to identify dependencies between work streams, develop a year's timetable for meetings and adopt a consistent approach to outputs via the use of templates was adopted. The meeting was held in Brussels on 10 January.

Next steps: In 2017 the ICO will take lead responsibility for WP 29 guidelines on profiling. We will also contribute as co-rapporteurs on guidelines on consent and the concepts of transparency and certification (with the European Data Protection Supervisor (EDPS)). In many of these areas we have already developed our policy thinking, having produced policy papers on profiling and consent and via our work on Privacy Seals. We will feed this in to the Article 29 Working Party process.

A number of guidelines that were started during 2016 have rolled over to 2017. Draft guidelines on the concept of high risk processing and Data Protection Impact Assessments (DPIAs) and the first part of the work on administrative fines (which we are leading together with Norway) will hopefully be agreed in the first part of 2017.

Contact: Jo Pedder/Hannah McCausland/Carl Wiper

### **ICO guidance/policy outputs**

As mentioned above, we have produced policy papers on the concepts of risk, consent and profiling under the GDPR. These are currently under review and will feed into the work being undertaken by the WP29 in 2017.

We have updated the EUDPR reform area of the ICO website to include a revised outline of what guidance to expect in the coming months. We have also updated the Overview of the GDPR document not only to include links to the new WP29 guidelines but also to flag forthcoming work stakeholders can expect in particular areas. And we have added a 'Whats new' section to the Overview so that stakeholders can continually refer back to the site to keep track on developments. We will update this document regularly and we have publicised these changes with a blog.

Next steps: We are evolving the Overview of the GDPR into the Guide to the GDPR which we will use as the spine for all of our guidance in data protection going forward.

We are in the process of drafting guidance on consent which we aim to publish early in 2017. We are also considering what content from the profiling paper we can publish as a means of external consultation. This will feed into the WP29 guidelines and to the European stakeholder event (FabLab) scheduled for April 2017.

We intend to publish our second Big Data paper in February. The paper includes some content about the GDPR and is currently being amended to incorporate detail about artificial intelligence and machine learning.

As the WP29 work plan for 2017 is now clearer we will review and prioritise other outstanding areas in which we can develop our policy thinking on the GDPR. This will include reviewing existing DPA guidance in priority areas to identify what can be retained and amended and where we will need to develop new content. Some of this work is dependent on the work DCMS is doing to develop domestic legislative changes needed, for example in relation to the derogations in Article 23 of the GDPR.

Contact: Jo Pedder/Hannah McCausland/Carl Wiper

### **Technology output**

We published a blog *Being held to ransom?* (<https://iconewsblog.wordpress.com/2016/12/15/being-held-to-ransom/>) which explains the rising threat of ransom-ware, a type of malware which can lead to a permanent loss of data unless a ransom demand is paid. A version of the blog was also published on the Huffington Post with advice for individuals ([http://www.huffingtonpost.co.uk/dr-simon-rice/cybersecurity\\_b\\_13647998.html](http://www.huffingtonpost.co.uk/dr-simon-rice/cybersecurity_b_13647998.html)).

Contact: Simon Rice

### **The International Working Group on Data Protection and Telecommunications (IWGDPT)**

A Working Paper on the topic of Privacy and Security Issues in Internet Telephony (VoIP) and Related Communication Technologies was published ([https://datenschutz-berlin.de/attachments/1237/675.52.10\\_WP\\_Update\\_VoIP\\_2016.pdf?1470059412](https://datenschutz-berlin.de/attachments/1237/675.52.10_WP_Update_VoIP_2016.pdf?1470059412)) following adoption for written procedure at the IWGDPT meeting in Oslo.

Contact: Simon Rice

## **International engagement**

### **International Conference of Data Protection and Privacy Commissioners (ICDPPC)**

The ICDPPC adopted the ICO's Resolution on International Enforcement Cooperation with unanimous support from a wide range of other privacy and data protection authorities from around the globe. This will be a first step in improving the privacy enforcement authorities' collective response to cross-border cases. The ICO also continues this work in cooperation with the Executive Committee of the Conference which will help to strengthen the numbers of other authorities participating in the Global Cross-border Enforcement Cooperation Arrangement and explore other pragmatic cooperation possibilities. The theme of the ICDPPC in 2016 was on artificial intelligence and robotics.

Outcome: The main outcome of the Resolution was the establishment of the Group of Experts on Legal and Practical Cooperation. This was launched in December with the British and Dutch data protection authorities appointed as Co-chairs. The Group is committed to develop a proposal for key principles in legislation that facilitates greater enforcement cooperation between members. The principles could be adapted by individual members according to their national, regional and local needs. The ICO is also working with the Canadian Office of the Privacy Commissioner on developing a work stream within this project on other practical ways to improve cooperation.

The ICO and Canada's Office of the Privacy Commissioner (OPC) also raised the ICDPPC members' awareness of the newly updated Handbook on International Enforcement Cooperation. This helps the ICO to identify ways to cooperate with other authorities more easily and generally more swiftly which in turn helps us to be more efficient in dealing with individuals' complaints about cross-border processing. The ICO learned from the invited international experts presenting cutting edge thinking on artificial intelligence and robotics.

Next steps: The Group of Experts has identified an Action Plan for delivering its output by the next ICDPPC in September 2017. The expertise gained from the sessions on Artificial Intelligence and Robotics will help to inform the ICO's technology policy strategy and Corporate Plan priorities.

Contact: Hannah McCausland

## **Common Thread Network – relations with Commonwealth counterparts**

The data protection authorities participating in the Common Thread Network or CTN (the network for data protection authorities of the Commonwealth) met for the Annual General Meeting in October 2016 in the margins of the 38<sup>th</sup> International Conference. Members of the Network reiterated their commitment to continue fostering sharing of knowledge and good practices and enabling capacity building.

Outcome: Canada OPC and UK ICO Commissioners both extended their role as joint co-chairs of the network for another year, until October 2017. They also took the opportunity of the Annual General Meeting to officially launch the CTN website ([www.commonthreadnetwork.org](http://www.commonthreadnetwork.org)). A platform for the CTN projects, it will also help showcase the activities of the network to any Commonwealth governments and other interested entities from the civil society and the public at large.

This network helps to inform the ICO's emerging International Strategy and has further potential to maintain the ICO's relevance as a leader in information rights in a changing international policy environment.

Next steps: The CTN work plan will be discussed at the next Quarterly Call on 20 January. Among its priorities, the CTN will resume discussions with the Commonwealth Secretariat to ensure that data protection remains high on the agenda list of the Heads of Government.

Contact: Hannah McCausland/Alain Kapper

## **Visitors**

In October, the South Korean Personal Information Protection Commission visited the ICO to discuss defining and disclosing personal data, as well as anonymisation. The delegation also explained their certification scheme to the ICO.

Outcome: Both authorities established good contacts on the aforementioned topics that will help to facilitate outreach in the everyday work the ICO does on information rights.

Next steps: The ICO will maintain its contacts with the South Koreans in view of the fact that the European Union is imminently opening a new phase of active engagement with the South Korean authorities. The South Koreans are the first among a number of key trading partners of the EU across East and South-East Asia to enter into this dialogue with the EU, as the EU seeks to establish adequacy findings for jurisdictions in that region. This will be useful in particular, seeing as the Article 29 Working

Party will be asked by the Commission to provide its assessment of South Korean law in due course.

Contact: Alain Kapper/Naomi Osborne-Wood

### **Case Handling Workshop**

ICO staff participated in the 28<sup>th</sup> European case handling workshop, which took place in Podgorica, Montenegro, on 13 and 14 October. The audience of European data protection case officers devoted particular attention to the challenges posed by new technologies, notably with the rise of affordable mobile recording technology and the changing European data protection laws in mind.

Next steps: At the end of last year, the ICO expressed its interest in hosting the 2017 Case Handling Workshop. Our application was favourably received by Cyprus which will be the host of this year's European Spring Conference. In the coming weeks, we will start making arrangements to host the event in Manchester on 20-21 June 2017. We will also facilitate the organisation of GPEN's first ever Enforcement Practitioners' Event, which will take place adjacent to the workshop and assist enforcement colleagues through dialogue in overcoming common cooperation challenges.

Contact: Alain Kapper

### **BIIDPA – British, Irish and Islands Data Protection Authorities Network**

On 5 October 2016, the ICO hosted a half-day GDPR-themed workshop with the commissioners and senior staff from the data protection authorities of Gibraltar, the Channel Islands, the Isle of Man and Malta. The discussion also benefitted from the presence of senior DCMS officials. Half a year after the adoption of the new data protection package, the meeting proved an ideal opportunity for partners around the table to share their ongoing efforts in transposing the new requirements of the GDPR into data protection legislation, notably in relation to the national derogations and exemptions introduced by the GDPR. The group also intends to hold further discussions on more specific sections of the GDPR, which may include the future rules governing international transfers and the adequacy process or the change to the notification system, to be decided later.

Next steps: Gibraltar will host the 2017 BIIDPA Conference on 30 June 2017, where discussions on the implementation of the GDPR as well as of the EU Law Enforcement Directive will continue.

Contact: Alain Kapper

## **EURODAC**

Eurodac is the European information system established for the comparison of fingerprints of asylum applicants and irregular immigrants, which came into use in January 2003. The system required an overhaul to keep up with the developments of the asylum legislation, notably to allow access to it by law enforcement agencies. The original Eurodac Regulations were recast in 2013 and the new system became operational on 20 July 2015. The ICO participates in the European Eurodac Supervision Coordination Group ("SCG") which supervises the application of the Eurodac Regulations by Member States. The SCG had a Standardised Inspection Plan for national inspections under the previous system but in light of the new Eurodac legal framework, the document had to be adjusted in 2016 to meet the new legal requirements of the Recast Regulation.

Outcome: The ICO, supported by the Romanian Data Protection Authority, chaired the review of the standardized Inspection Plan, which was formally adopted by the SCG at its meeting on 23 November 2016.

Next steps: The new Plan will be used by the SCG with immediate effect.

Contact: Alain Kapper

## **Freedom of Information**

In a Ministerial Statement in response to the Burns Commission report on FOIA, the government committed to provide additional guidance for public authorities to assist them in complying with their obligations under the Act. It opted to do this by revising the section 45 Code of Practice. In December the ICO provided comments about the draft code as part of the government's consultation.

Next steps: we await any further requests for input from the government.

## 2. Data breaches and other high profile cases

The inflow of data breach cases retained its momentum throughout the quarter, with new cases totalling in excess of 590. Based on current projections new cases will exceed 2,100 by year end, a potential increase of 150 cases on the total received in 2015/2016.

We continue to categorise cyber incidents into specific descriptors in order to enable more detailed statistical to be provided. In Q3 60 cyber incidents were recorded, compared with 73 in Q2, suggesting a slight dip in intake.

Cyber incidents continue to dominate the media, with several high-profile incidents reported this quarter. The ICO is presently corresponding with several household names in relation to potential cyber-incidents.

The introduction of a specialist technical team is progressing and we expect to recruit three Technical Investigators in the next quarter. We are continuing to develop our response to cyber-security incidents to ensure the timely management, oversight and investigation of this type of reported incident.

We have strengthened our position to managing and investigating cyber security incidents by working in partnership with the National Cyber Security Centre and through participation in national cyber-security exercises coordinated by the Home Office, aimed at testing the ability of policing and law enforcement agencies to prioritise and coordinate the response to large scale cyber crime nationally, regionally and locally; and collaborate with partners, including the private sector, in order to ensure an effective multi-agency response and sharing of capabilities. Learnings from the exercise will inform the development of the response procedure.

We also continue to work with international counterparts and with domestic law enforcement agencies to progress our investigations into multinational companies affected by cyber-incidents. This work has been complemented by a two month secondment of a member of staff to the OPC in Canada.

We continue to promote awareness of the risks of data breaches. In Q3 we delivered three Webinars: two focussing on the cost of a data breach, and one on the need for organisations to take preventive measures to reduce the risk of an incident with particular reference to working out of the office.

The first data security incident trends report was published covering Q1 2015/2016, and has now been produced for just over 12 months. Our aim is to reach three sets of audiences to highlight the trends we see and the

work we do - stakeholders who are interested in the overall picture of data protection; people within named sectors, who are perhaps less aware of the ICO, but who could be influenced by the statistics to take action to improve their compliance with the law, and finally; ICO staff to be aware of the report and use it for campaigns and initiatives. A recent review has highlighted some changes necessary to meet these aims and these will be actioned in the next quarter.

[Redacted]

### 3. Ongoing investigations

In Q3 we opened 49 cases into potential criminal breaches, 48 of which are section 55 Data Protection Act enquiries, and 1 section 77 Freedom of Information Act case. By comparison with the previous quarters this year this is down on Q2 (89), but up on Q1 (42).

We have also assessed 105 'provide advice' requests in Q3, compared to 103 in Q1 and 125 in Q2. We have completed 2 requests for case reviews in Q3 – both with the original decision upheld.

We have submitted eight prosecution files to the ICO Prosecutor in Q3 of which seven were for section 55 offences, the other being a section 47 Data Protection Act offence. As noted in section 2 above; one file has been submitted for Operation SPRUCE in addition to these cases. Six further files await a prosecution decision.

[Redacted]

We continue to investigate the extent of criminal breaches associated with the collection, trade and sale of personal data. Operation PELHAM is a criminal investigation into the unlawful obtaining and sale of data from accident repair centres, which has then been used to make nuisance calls to customers of those centres. Three search warrants were executed in Q3 relating to this enquiry, and a large amount of relevant documents and computer equipment was seized. This is now undergoing forensic assessment.

[Redacted]

In respect of non-notification work, we have received 55 referrals with three cases being referred for a prosecution decision for section 17 Data Protection Act offences. In this quarter we closed 13 cases, with 31 data controllers subsequently notifying as processing personal data. We continue to investigate the Royal Free Hospital Trust's sharing of patient data with Google Deepmind in support of the development of a healthcare application.

We have completed the investigation into the disclosure of CCTV footage by Virgin Trains East Coast of Jeremy Corbyn and unrelated third parties. We expect to report early in 2017.

[Redacted]

## 4. Enforcement action

This quarter we prosecuted six criminal cases – one for a section 56 Data Protection Act offence, concerning Minera Tyres. They were found not guilty after a trial. Four cases were for section 55 offences, and one was a section 47 offence – all these entered guilty pleas. Fines totalled £1,845, with costs of £2,657.98 and victim surcharges of £145. A total of £4,647.98.

We cautioned one person for a section 55 offence this quarter.

We issued five civil monetary penalties totaling £250,000 for contraventions of the Privacy and Electronic Communication Regulations (PECR), by organisations making or sending unsolicited marketing calls and messages.

The largest fine this quarter was £100,000 against Silver City Tech Limited. Other fines included £70,000 against Nouveau Finance Limited, £30,000 against Assist Law Limited, £30,000 against Oracle Insurance Brokers Limited and £20,000 against Rainbow (UK) Limited. In the year to date we have now issued 14 monetary penalties for marketing contraventions for £1,120,000 in total.

We also served three Enforcement Notices; one to Nouveau Finance Limited to accompany the monetary penalty above, one against Silver City Tech Limited, again to accompany the monetary penalty, with an Enforcement Notice issued against Key Insolvency Service Limited to compel their compliance with the Regulations. Three further Preliminary Enforcement Notices were issued against organisations in this period. Representations are due from the organisations in the next quarter in respect of those notices.

We issued one fixed penalty notice under the PECR against a communications service provider for failing to report an unauthorised disclosure of personal data as a result of a security breach. Kcom Limited discharged their liability by paying £800 on receipt of the Notice of Intent.

We monitored seven organisations this quarter which we believe represent risks in relation to compliance with PECR. We held nine meetings with organisations to tell them to improve their direct marketing practices. In the year to date we have monitored 15 organisations and held 21 compliance meetings.

The ICO's investigation into a number of charities and their fundraising activities has been completed and we progressed the cases to enforcement action. The first decisions were made in this quarter; monetary penalties were issued against the RSPCA for £25,000 and

British Heart Foundation for £18,000 for serious and widespread breaches of the first and second data protection principles. The monetary penalties have been paid and both organisations have confirmed cessation of the unlawful activities identified by the ICO. The Charity Commission subsequently opened compliance investigations into both charities.

This quarter we have also issued one further civil monetary penalty notice totaling £500 for a serious contravention of principle seven of the Data Protection Act 1998 after an unencrypted laptop containing sensitive personal data was stolen. The notice is subject to publishing and reporting restrictions, and the name of the data controller is therefore redacted from public view.

A total of nine notices of intent relating to serious data protection compliance failures have been served this quarter. The notices were served on a variety of organisations, including private sector businesses and public sector organisations.

The total number of monetary penalty notices served to organisations found to be in breach of the Data Protection Act 1998 this year to date totals eleven and the number of notices of intent (NOIs) totals fifteen.

Also in this quarter, commitments to improve compliance were obtained from Cornwall Council and the London Borough of Ealing, with both organisations signing undertakings setting out the steps they will take to ensure that they meet the requirements of the Data Protection Act. Both undertakings require improvements to be made to each Council's delivery of staff training. We also issued an undertaking to the Royal Bank of Scotland, which required the organisation to improve its fax procedures.

[Redacted]

Any further decisions will be publicised in the usual way, and according to our policy on Communicating Regulatory Activity.

## 5. Consultations

Responses to formal consultations –

Independent Parliamentary Standards Authority - *Review of the MP's Scheme of Business Costs and Expenses and IPSA's publication policy*

HM Revenue and Customs - *Making Tax Digital: Transforming the tax system through the better use of information*

HM Revenue and Customs – *Tackling the hidden economy: conditionality*

HM Revenue and Customs – *Tackling the Hidden Economy: Extension of Data-Gathering Powers to Money Service Businesses*

HM Revenue and Customs – *Tackling offshore tax evasion: a requirement to correct*

HM Revenue and Customs – *Strengthening tax avoidance sanctions and deterrents*

Responses to parliamentary calls for evidence –

House of Commons Public Bill Committee – *Digital Economy Bill*

## 6. Other

### Performance Improvement

The third quarter of 2016/17 has been productive but there has been no let-up in terms of complaints received. It remains a risk that we won't be able to deal with all of the complaints made to us this year, and our outstanding caseloads continue to rise.

DP complaints/concerns cases are up 19% when compared to intake at the same time last year and FOI cases are up 9%.

The Department has continued to increase output and at the end of the year have closed over 1,600 more DP cases than at the same point in 2016 (that equates to a 14% productivity increase, or an additional full month's work of intake). FOI casework output is also up on last year, by 220 cases (a 6% increase).

Despite this, the DP caseload has risen by some 900 cases since the start of the financial year. The FOI caseload is up by 150.

The situation is a challenging one, but we expect that significant case officer recruitment in quarter 2 should start to boost case resolution numbers in the next month, which will continue to climb toward year end. We continue to offer overtime at weekends, both in the office and for those available to homework, in an attempt to mitigate the impact for those that require our help.

As well as our routine data protection and freedom of information casework we have continued to assess search engine cases for those that want the results to be removed. There were 93 new cases this quarter and we were able to conclude 105. The majority of our decisions are supporting Google's approach to removal.

[Redacted]

FOI monitoring continues. Following the latest round of statistical reporting the London Borough of Lambeth was put on formal monitoring for the period Jan/Feb/Mar 2017. Three other public authorities were also identified as potential monitoring candidates however as we have decided to work with two, informally, to improve performance. Further investigation and consultation with the third organisation meant that additional intervention was not required.

The Metropolitan Police Service has had a number of issues in terms of FOI delivery, although there has been some improvement in turn around time recently. A further review meeting is scheduled for February 2017.

As every quarter, the department deals with thousands of individual issues and we attempt to use this experience to improve information rights practices in the organisations we contact. Some examples of this are included below.

We picked up on a media report that a high street retailer is using WhatsApp to share images of suspected shoplifters lifted from CCTV systems with other retailers. When contacted they were of the view that this was acceptable under s29 – we have clarified that this isn't the case and the practice must cease. Other intelligence gathered via the Intel Hub suggested that other large retailers are also doing this. We have made contact with the British Retail Consortium and will explore how we can get messages to retailers about this matter more widely.

We continue to see ongoing issues raised by Claims Management Companies (CMC) about the handling of information requests by major lenders generating large volumes of concerns being brought to our attention. Due to the increasing volume of concerns raised we have met with the CMC Regulator and one of the most complained about lenders. The lender has committed to making changes to process to ensure compliance and reduce concerns raised.

Concerns about domestic CCTV cameras remain high with a further 159 Request for Assessment concerns raised in Q3. We have engaged with some of the larger retailers who sell CCTV systems to explore whether their buying guides could include a link to our website/guidance to advise buyers of the potential responsibilities when operating such equipment.

A number of concerns were raised with us about a major high street optician and the display of personal data on screen when in private consulting rooms at the store. The organisation has now made major IT alterations so this no longer happens. Search results, when trying to identify patients, have been significantly improved and the amount of data displayed and stored has been revised. Alongside this measure it has also issued guidance to its stores relating to vigilance of the screen content and the data visibility.

We attended a meeting with UK Visas and Immigration following receipt of a number of concerns raised with us by solicitors and charities representing asylum seekers about the ID requirements UKVI was imposing on data subjects making SARs. Our view was that the requirements were disproportionate. UKVI agreed and have now introduced less stringent requirements whilst still ensuring that they received adequate ID verification.

The above examples are not exhaustive and simply provide a sample snapshot of the improving practice activity undertaken in the quarter.

Contact: Andy Laing

## **Training**

### **Internal GDPR training**

In November we launched a new desk based learning package for ICO staff to convert them from the DPA to the GDPR. This is the first phase of our internal training programme to introduce staff across the ICO to the new legislation. A manager's brief highlighted the training and drop in sessions for managers were held to talk them through the new resource.

Feedback and delegate assessment results have been extremely positive.

Next steps: work is now underway on developing the introduction to GDPR for new staff joining the ICO with no data protection knowledge.

Contact: Lisa Atkinson/Jo Pedder

### **Other internal information rights training**

Since September a total of 86 delegates have attended internal information rights training. We have run 1 Introduction to Data Protection and 4 Introduction to FOI courses. In addition we have delivered 1 full core FOI course, 2 DPA/PECR courses and 2 complete BCS courses.

Contact: Lisa Atkinson/Jo Pedder

The technology team delivered know about sessions covering Know abouts covering coding, TOR and passwords held for staff.

Contact: Simon Rice

### **External training/events**

The technology team delivered a Cyber security webinar (<https://ico.org.uk/about-the-ico/news-and-events/events-and-webinars/cyber-security-webinar/>) attended by more than 600 delegates. The webinar focused on current cyber security trends and issues, such as ransomware and phishing, some of the biggest cases the ICO has been involved in, and what firms can do to improve cyber security within their organisation. Following the webinar, questions received were answered in a blog.

Contact: Simon Rice

## **Good Practice**

We hosted a visit from two senior investigators from the Office of the Privacy Commissioner of Canada (OPC). The OPC is considering pro-active compliance activities, such as privacy check-ups, and they have been learning from the experiences of their counterparts who, like ourselves, have active programs in this area.

During their time here, the OPC met with managers to go through our established audit processes and the audit services we offer. On day two, our visitors observed a pre audit meeting held at a local health trust. This helped them gain an oversight of one of the key stages in our audit planning process. The visit concluded with a round table workshop, with the OPC and ICO, which gave both authorities the chance to ask questions and share experiences of both good practice and data protection compliance services.

This visit has opened up the lines of communication between the two offices facilitating ongoing engagements and the development of services around the world.

## **Central Government breach reporting**

The NAO's report 'Protecting information across government' identified inconsistencies in the data breach reporting practices of 17 (now 16) central government departments. As a result we have instigated a programme of consensual information risk reviews to these departments. To date all but one of the departments has responded positively to the proposed engagement and we have now received the majority of documentation requested for the pre visit review of policies and procedures. The first on site reviews are scheduled for Q4 and planning for the remainder is in progress.

## **ICO Regions**

The integration of the three Regional Offices has continued to develop over the quarter led by the Regional Management Team comprising the Head of ICO Regions and the three Regional Managers. The new working relationships are now well established. Given the increased demand for RO services, in November 2016 a case was made for the creation of a Lead Policy Officer post in each office; successful candidates will take up their positions in January 2017.

## **Preparing devolved administrations for GDPR**

*Work includes:* A series of GDPR workshops were delivered to the Departmental Knowledge Information Managers (DKIMs) from a range of service areas across the Welsh Government in which aspects of the GDPR likely to impact on the areas were highlighted. Workshops have also been held in Northern Ireland and a briefing was given to the NI Civil Service Information Governance Innovation Board. In Scotland, regular updates were provided to the Scottish Government and its agencies through the ICO's attendance at the Government's DP Practitioners Forum.

*Future action:* Further targeted working with all three devolved administration will take place in accordance with local delivery strategies.

*Outcomes:* Assisting the devolved administrations with their preparation for GDPR, and accordingly improving information rights for their citizens.

*Contact:* Shauna Dunlop, Rachael Gallagher (Northern Ireland)  
Maureen Falconer (Scotland)  
David Teague, Helen Thomas (Wales)

## **Child Protection**

*Work Includes:* Engagement has continued with the Scottish Child Abuse Inquiry which is investigating both historical instances of abuse and more recent cases occurring up to the end of 2014. In Northern Ireland, and in conjunction with the Irish Data Protection Commissioner, work is ongoing with the National Board for Safeguarding Children in the Catholic Church which has a cross-border remit.

*Future Action:* Awareness raising sessions will be delivered to the staff of the Scottish Child Abuse Inquiry. A response to a consultation on its Safeguarding Policy and Procedure will be submitted to the Safeguarding Board for Northern Ireland

*Outcomes:* Greater awareness of privacy concerns by staff handling the information relating to extremely vulnerable individuals.

*Contact:* Shauna Dunlop (Northern Ireland)  
Maureen Falconer (Scotland)

## **Child Death Review Project Board**

*Work Includes:* The Scottish Government is currently seeking to establish a review process for every child death in Scotland and the ICO is represented on the Project Board. Our focus is on issues relating to the processing of personal and sensitive personal data relating to relatives,

professional practitioners and others whose involvement with the child/family is relevant to the review.

*Future action:* The Project is at a very early stage so it is envisaged that attendance at Board meetings will continue with specific advice provided in respect of the recommended PIA.

*Outcomes:* Ensuring that data protection obligations are met at all stages of the Project as well as making the resultant process as privacy friendly as possible. Reinforcing the ICO's reputation as an authoritative source of data protection advice and guidance.

*Contact:* Maureen Falconer (Scotland)

### **Improving information rights compliance within the community and voluntary sectors**

*Work Includes:* All three offices had continuing engagement with third sector organisations throughout the quarter. Following the successful #Data Friday programme held in conjunction with the NI Council for Voluntary Action (NICVA) which ended in December, preparations for further engagement began. In addition, a series of data protection blogs were produced for publication by the Scottish Council for Voluntary Organisations and awareness raising sessions, including webinars, were held for the Wales Council for Voluntary Action.

*Future action:* Further engagement with the umbrella bodies and their membership will take place focussing on fund-raising and the preparation for GDPR

*Outcomes:* Improved information rights compliance across the voluntary and community sector in the ICO Regions.

*Contact:* Shauna Dunlop (Northern Ireland)  
Maureen Falconer (Scotland)  
Dave Teague (Wales)

### **Embedding an 'individual rights' approach across priority sectors**

*Work includes:* Further developing the NI successful partnership strategies to ensure organisations and the ICO work together strategically to inform individuals of their rights. To date, a stakeholder panel has been established to tackle nuisance calls. The next panels to meet include the legal sector, the technology sector and the voluntary and community sector. In addition, a work plan has been agreed with Libraries NI, to work together on information awareness across the 90+ libraries in NI.

*Future action:* Establish and agree all terms of reference for the stakeholder panels and successfully complete the Libraries NI pilot – ‘MyData’

*Outcomes:* Working in partnership with stakeholders to deliver key strategic outcomes and inform individuals of their rights

*Contact:* Shauna Dunlop, Rachael Gallagher (Northern Ireland)

### **Nuisance Calls Commission**

*Work Includes:* The Scotland Act 2016 devolved to the Scottish Parliament a number of powers relating to consumer advocacy and advice. Subsequently, the Cabinet Secretary for the Economy, Jobs and Fair Work established the Nuisance Calls Commission comprising representatives from various interested bodies, to examine how these powers may be used to help reduce the detriment arising from nuisance calls. The Information Commissioner attended the first meeting in November along with the Head of ICO Regions and the manager of the Anti-Spam Investigation Team.

*Future Action:* The ICO will maintain membership of the Commission throughout its lifetime and participate in any appropriate and relevant actions arising from its work.

*Outcomes:* Reduction in nuisance calls received. Greater consumer awareness about preventative measures.

*Contact:* Ken Macdonald (Head of ICO Regions)  
David Clancy (Enforcement)

### **Identifying risk in multi-agency data sharing**

*Work includes:* Our attendance at the NHS Wales Information Governance Managers Group enabled us to identify a potential risk involved in the development of the Welsh Community Care Information System (WCCIS), a new collaborative solution for Health and Social Care in Wales. We invited key stakeholders to a round-table meeting which we chaired, and were able to clarify the risks involved for all parties.

*Future action:* We will continue to monitor the development of WCCIS, and offer input where appropriate.

*Outcomes:* Data controllers involved in the WCCIS now understand our view of the risk, and are better placed to take appropriate mitigation.

*Contact:* Helen Thomas (Wales)

## **Independent Schools and Alumni Associations**

*Work Includes:* Providing a series of presentations to various Fora and Conferences on the forthcoming provisions of the GDPR, especially in respect of alumni contact, fundraising and wealth profiling.

*Future action:* Advisory Visits to individual schools and work with the Scottish Council for Independent Schools to promote GDPR. Work with alumni associations on profiling in particular.

*Outcomes:* Assisting the independent school sector and alumni associations in preparing for GDPR. Reinforcing the ICO's reputation as an authoritative source of data protection advice and guidance.

*Contact:* Maureen Falconer (Scotland)