Information rights report
Quarter 2 2016/17

Contents

1. Key Developments

Some key developments expected in the next quarter are:

- [Redacted]
- Several key Article 29 working party opinions on the GDPR including on the concept of main establishment, the role of the Data Protection Officer and the right to Data Portability.
- Publication of the ICO's refreshed Big Data paper
- Further details of the Privacy Shield processes and procedures
- Proposed ICO technology strategy

2. Cross Sectoral Work

Good Practice

Following a review of the current sectoral audit outcomes analysis and reporting processes, new opportunities to adapt and evolve our approach were identified. The new approach includes working closely with our Communications Team to develop communications strategies based on key themes or challenges for organisations in complying with the current DPA that we have identified through our audit activities.

Two managers from Good Practice visited the Office of the Personal Data Protection Inspector in Tbilisi, Georgia, as part of a project to support institutional capacity building. We shared our knowledge and experience of conducting audits, including methodology, resources and communication of outcomes and met with officials from the British Embassy, the Prosecution Service and the Ministry of Internal Affairs. The visit was extremely well received.

External guidance

Data protection

The revised Privacy Notice code of practice was published in early October together with a blog explaining the importance of transparency to consumer confidence and the growth of the digital economy. The code addresses compliance with the DPA and outlines the additional requirements of the GDPR. It has had 10,000 views to date and received positive social media coverage. It is the first ICO code of practice to be published on a multipage document platform and to contain interactive examples of different techniques to engage individuals with privacy information.

Next steps: additional detail about the requirements of the GDPR will be added as our policy positions develop as part of the ICO implementation plan. This will include detail on transparency requirements where children's data is involved. We will also consider the feasibility of developing a privacy notice generator and tools to assist data controllers with the extra documentation requirements the GDPR imposes.

Contact: Jo Pedder/Carl Wiper

Privacy and Electronic Communications Regulations

The refreshed cookies guidance will be published imminently. It does not introduce different policy approaches but addresses recent activities and highlights the need for organisations to consider the use of mobile and

other types of device when considering consent mechanisms and information resources.

Contact: Simon Rice

Freedom of Information

Detailed guidance on the exemptions in sections 26 (Defence) and 44 (Statutory and other prohibitions on disclosure) of the Freedom of Information Act was also published.

Contact: Carl Wiper

Other policy projects

Threats and Opportunities Report

An update to the Threats and Opportunities report was made available internally during Q2 and presented to SMT and circulated to appropriate ICO staff. The report was also discussed within the ET-PAAG (see below) in order to discuss priority areas for further ICO activity.

Contact: Simon Rice

Emerging Technologies PAAG

The Emerging Technologies Priority Area Action Group met and identified key technology areas from the Threats and Opportunities report for further investigation. Strategic Liaison and Policy Delivery are developing a call for evidence format to obtain external input to inform policy thinking on privacy issues with connected and autonomous vehicles.

Next steps: develop call for evidence aspect of the ICO Policy Methodology and develop using connected cars issue. Internal research on vehicle telematics will continue to further inform the ICO.

Contact: Simon Rice/Carl Wiper

Communication

A follow-up blog to the 2014 communication on internet-connected video cameras was published on the ICO blog site in addition to a publication on the Huffington Post. The focus was to highlight the need for organisations and consumers to stop the practice of using default passwords for internet connected devices and to instead secure these services with strong passwords.

Public must act to protect themselves when using Internet of Things devices - https://iconewsblog.wordpress.com/2016/07/15/public-must-act-to-protect-themselves-when-using-internet-of-things-devices/ http://www.huffingtonpost.co.uk/dr-simon-rice/uk-families-still-at-risk_b_10958428.html?

Contact: Simon Rice

Development of a public standard for icons within privacy notices

The ICO is a member of the BSI Steering Group developing a publically accessible standard for the use of icons within privacy notices. We provided our initial comments to the early draft of the standard and attended the first steering group meeting in September.

Next steps: further drafts of the standard will be considered by the steering group in advance of the public consultation phase. The aim is that the standard will be available in March 2017.

Contact: Jo Pedder/Carl Wiper

Embedding information rights in the HE/FE sector

The ICO has launched a project to assess the feasibility of embedding information rights teaching in the HE/FE sector. As phase 1 of this project we have commissioned research to help us understand what teaching of information rights already takes place and on which courses. The research will also seek to identify areas where there might be scope to embed or enhance the coverage of information rights, and the ways in which that could be facilitated. The research is being carried out by Quadrant and Marketwise Strategies. To date in-depth interviews have been carried out with academics.

Next steps: an online survey element to the research is about to be launched. Quadrant will submit a report of the findings to the ICO at which point we will consider phase 2 of the project.

Contact: Jo Pedder/Lisa Atkinson/Vicki Heath

Post referendum - implications of the UK's decision to leave the EU

The ICO provided written evidence to the Joint Committee on Human Rights on the human rights implications of the decision to leave the EU and specifically the impact on information rights.

In collaboration with Strategic Liaison colleagues, written evidence was also submitted to the House of Lords EU Internal Markets sub- committee

inquiry on ‘Brexit: future trade between the UK and the EU’. This evidence focussed on the importance of data protection to consumer confidence and trust in how their personal information is processed as a key component in the development of the digital economy.

Contact: Jo Pedder/Carl Wiper/Garreth Cameron

3. Government and Society Sector

Digital Economy Bill

The Digital Economy Bill continues its progress through Parliament and has now reached committee stage in the House of Commons. The Commissioner and Deputy Commissioner appeared before the Public Bill Committee on 13 October 2016. The oral evidence sessions are now complete and the committee will now consider the Bill on a line by line basis. 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. The Bill includes powers to allow data sharing for a number of purposes including for delivery of public services such as tackling fuel poverty; research and statistics; fraud; debt and the General Register Office data (births, deaths).

Outcome:

The Commissioner in her oral and written evidence to the Committee welcomed the efforts to put defined areas of data sharing on a clear footing and made clear her aim to improve public trust in the use of personal data and to make transparency for citizens a priority for all organisations that collect and use personal data. She recognised the potential benefits of justified and proportionate data sharing, acknowledging that citizens want improved, seamless online services from the public sector and this may require more effective sharing of data between public authorities. She encouraged the government to consider further work to develop consistency between the codes and align them more closely with the ICO's Data Sharing Code of Practice and suggested the addition of a clause in the Bill that makes clear that the codes of practice established under Part 5 of the Bill will be subordinate to the ICO's statutory Data Sharing Code of Practice. She also advised that risks posed by complexity in the Bill needed to be addressed and recommended that a reference to the ICO code of practice on privacy notices and transparency for individuals should be made on the face of the Bill.

Future work:

We shall continue to monitor the Bill's progress through Parliament and engage with the Cabinet Office and DCMS as they develop proposals arising from the Bill. We stand ready to respond formally when consultations on the codes are launched. We will remain alert to civil society concerns over the data sharing proposals and will continue to advise the government to develop consistency between the codes.

Contact: Judith Jones, Jonathan Bamford

EU referendum

We responded to the Public Administration and Constitutional Affairs Committee's inquiry into 'Lessons learned from the EU Referendum'. We explained that, notwithstanding the Electoral Commission's primary role in this area, the Information Commissioner has a role where issues of data protection and privacy arise with regard to electoral arrangements. We outlined our work on the introduction of Individual Electoral Registration and our concerns regarding the operation of the open register. We made a number of points reflecting the concerns the ICO received from members of the public during the pre–referendum period and highlighted the fact that the Information Commissioner issued a civil monetary penalty against a campaigning organisation relating to a serious breach of the Privacy and Electronic Communications Regulations. Many voters were unaware that referendum campaigning organisations and individuals were entitled, on registration, to have access to the full electoral register. We remain concerned about the transparency of electoral arrangements including the full and open registers. Complaints we received showed that the public were often unclear about the purposes of the registers, whether they had opted out of the open register and what the registered permitted participants and also the two designated campaigning groups were allowed to do with the full register during the referendum. We also highlighted our concerns that registered permitted participants should dispose securely of all copies of the full register, explaining we were liaising with the Electoral Commission to ensure this.

Outcome:

We have worked with the Electoral Commission who agreed to contact all permitted participants to remind them that in accordance with the requirements of the data protection legislation they should securely dispose of their copies of the electoral register.

Further action:

We continue to liaise with the Electoral Commission and propose to meet with them to discuss issues of common interest including those relating to the referendum. We also continue to monitor the Committee's work in relation to their inquiry and will review any recommendations that fall within the ICO's remit.

Contact: Judith Jones, Sue Markey

HMRC employment history subject access requests

HMRC is continuing to struggle to respond to tens of thousands of subject access requests (SARs) for employment histories within the statutory 40 days. The information being requested is for individuals' old employment histories to support compensation claims for health conditions caused at work (particularly noise induced hearing loss). Over 5bn records dating between 1961 and 2013 are held on 352,000 microfilm tapes and HMRC has 38 ageing and obsolete microfilm reading machines working at maximum capacity.

In their September 2016 update, HMRC reported they had 58,000 SARs over the 40 day deadline. This is slightly higher than the figure of 56,500 at the time of the last information rights report in July. However, HMRC have been using the summer months to trial new machines and conduct an audit of processing and this has slightly reduced the number of staff and microfilm machines available. HMRC continue to prioritise requests relating to the most serious and life-threatening conditions, which they respond to within ten days. The number of requests submitted on a monthly basis continues to run at levels well below 2015 - year-to-date requests are currently running at half the rate at this stage last year.

Outcome:

We wrote to HMRC following the ICO's Strategic Tasking and Coordination Group (STCG) decision that enforcement action was not a suitable option at this time. Other than deleting the data, which would seriously disadvantage people with legitimate claims, the digitisation of the records is the only long-term solution but it will take time. HMRC's response confirmed that their Executive Committee has given a commitment to proceed with a project to digitise the very fragile records but they have to go through a lengthy procurement exercise. HMRC have now received detailed costings from suppliers for scanning and digitisation solutions, and these figures are due to go to an Investment Committee for a decision in November.

As an interim measure HMRC have started the process of replacing the microfilm readers with new, more reliable machines. HMRC have addressed some of the demand for employment histories by asking members of the Association of Personal Injury Lawyers to remove any requests for histories that are related to noise-induced hearing loss claims that have now been withdrawn. HMRC have received confirmation from a number of law firms that they will be submitting lists of employment history requests that will now be withdrawn and no longer require processing. HMRC's internal audit of the employment history request process has identified 20,000 backlog cases that have been recovered from microfilm but are still awaiting re-purposing into intelligible reports

that can be sent to requestors. The employment histories unit have had approval for additional staff to immediately begin the process of compiling the information for these 20,000 cases into reports that can be sent within the next two months. This will reduce the 58,000 figure of overdue SARs by over a third by December 2016.

We will continue to investigate subject access complaints against HMRC on an individual level as part of our normal course of business.

Future work:

HMRC continue to work constructively with us on possible solutions and to provide us with monthly updates on progress to tackle the backlog. We shall continue to have regular meetings with HMRC to discuss this progress, and they have agreed to the ICO making a second visit to their site in northeast England where the requests are processed. The TCG will be re-convened with a view to providing an outcome and update report to the STCG.

Contact: Judith Jones

Charity fundraising

[Redacted]

4. Police, Justice and Borders Sector

Good Practice

The Business Crime Reduction Partnerships project is progressing well; six individual reports have been produced so far and more visits are scheduled. Good Practice has a representative at the London BCRP conference and we have been asked to speak at the National Association of Business Crime Partnerships conference in April next year.

Police use of surveillance technologies

We continue to work with and provide advice to key stakeholders across the law enforcement sector on surveillance technologies. One area which is proving challenging for stakeholders is the redaction of third parties from moving footage (either CCTV or Body Worn Video (BWV)) in order to respond to subject access requests and we met with the Home Office CAST (Centre for Applied Science and Technology) to discuss video analytics and the options for redacting personal data from video footage. Their advice was that specialist software and expertise is required in order to do this effectively and we will need to continue engaging with them on this. We also met with SeeQuestor, a third party provider of video analytic software for law enforcement, to discuss the capabilities of the software and how the service complies with the requirements of the DPA.

The Surveillance Camera Commissioner has launched his National Surveillance Camera Strategy (NSCS) and we are part of the regulatory work stream led by the Office of the Surveillance Commissioners which will consider how the twelve principles in the Secretary of State's Surveillance Camera code of practice fit within the broader regulatory landscape. At present the Strategy is portrayed as a national one with wide effect when its provisions are actually focussed on promoting compliance with and extending the reach of the Surveillance Camera Code.

We continue to work closely with the ANPR community across the police to improve transparency and now sit on the ANPR Privacy and Transparency Panel which is considering governance models for ANPR. We continue to provide advice on PIAs and are in the process of advising on retention as the NPCC explore the possibility of putting ANPR on a statutory footing. We are waiting on confirmation of deletion of older ANPR data being held within the Met Police Service which will result in the deletion of 12 billion reads.

We have undertaken a number of PIA workshops for the biometric community across the Home Office. It is likely to become mandatory for PIAs to be undertaken on any new initiative involving biometrics and it is

important that they are done appropriately, identifying and mitigating the relevant risks to privacy. As more and more biometric data is collected in the immigration/borders sphere and as technology develops this is becoming a detailed source of information about individuals and added to that framework is the use of facial recognition technology.

Outcome:

We continue to influence and provide detailed advice to key stakeholders on surveillance issues. We have been invited to sit on a number of groups and panels and we are involved with the ongoing work on the National Surveillance Camera Strategy.

Future Work:

We will continue to provide advice to Forces on the information rights issues associated with BWV. It is becoming apparent that the management of a substantial amount of data being collected from the devices is proving challenging for forces particularly in the context of responding to disclosure requests and obligations but also in terms of locating information. We will also be making contact with the National Offender Management Service as BWV is being rolled out in prisons.

We will be presenting at the national ANPR conference, the theme for this year being transparency. We will also be undertaking two ANPR workshops. We have future meetings with the Met Police Service and are awaiting confirmation that the 'Olympic feed' ANPR data (12 billion reads) has been deleted.

We will be participating in the Surveillance Camera Commissioner's stakeholder engagement event on the proposed national strategy.

Contacts: Anne Russell, Meagan Mirza, Jonathan Bamford

Police National Computer

The Police National Computer (PNC) is the national police-run database which contains records of any individual's interaction with the police in the context of a criminal offence. The PNC contains details of individuals arrested, charged and convicted and the current retention policy is that all records are retained until an individual reaches 100 years of age unless an individual makes a successful application under the Record Deletion Process (RDP). The RDP provides very narrow criteria under which individuals can make an application to the originating police force to have their records removed which covers, for example, incidents where there was 'no crime' or an arrest was unlawful. Our office has a role in the RDP

in that individuals can complain to us if a force refuses to delete their record.

Police National Database

[Redacted]

Investigatory powers legislation

[Redacted]

5. Public Services Sector

Good Practice

We continue to work closely with umbrella organisations to promote the outcomes of our work and have engaged with the NHS Digital IT Toolkit Team to share intelligence and experiences in order to improve DP compliance.

We continue to work with the General Pharmaceutical Council on a programme of work within the pharmacy sector.

We have begun a number of advisory visits to nurseries and aim to summarise our findings in an outcomes report for the early years learning sector as a whole.

We have also launched an online survey about the governance of data protection and freedom of information within local authorities. We have received nearly 100 responses so far and intend to use these to identify common areas of good practice and weakness with a view to producing targeted advice and assistance for the sector on this issue.

National Pupil Database

The Department for Education (DfE) collects a variety of information on pupils from schools in order to maintain the National Pupil Database (the NPD). A concern had been raised with the ICO around the purpose for retention and the length of time the personal data was being retained for.

We have written to the DfE relating to these matters and established that the purpose for collecting this personal data was for research purposes and they contested that they were relying on the exemption at s.33 of the Data Protection Act 1998. We were satisfied that the s.33 exemption did apply. Further concerns were then raised with us around the legal basis for collecting the personal data and the fair processing information that is being provided to pupils and parents.

We have also received some media enquiries regarding this after some schools were misunderstanding the requirements and collecting information they didn't otherwise hold in order to provide it to the DfE.

Outcome:

We have written to the DfE again in relation to the principle 1 concerns that were raised with us. They have clearly set out that they have powers set out in Regulations to collect specified information for the purposes they have already set out to us. We also sought some further clarification

that those purposes were **only** for research purposes. The DfE have explained to us clearly what happens to that data and we are satisfied that it is being processed only for research purposes.

Future Work:

There remain some concerns around schools' understanding of what information they are required to provide and what they do not need to provide as well as the quality of the fair processing information that is being provided. We will be contacting the DfE again to remind them of their obligations to advise and support schools to ensure that they are able to comply with their obligations under the DPA.

Contact: Victoria Cetinkaya

National Data Guardian Review of Health and Care Data Security and Consent - Consultation Response

The Secretary of State for Health commissioned the NDG to review and produce a report on security and also detailing whether the NHS should offer an opt out of data being used for purposes other than direct care. We took part in the NDG review panel. The Care Quality Commission (CQC) was also commissioned to produce a report on data security. Both these reports have been published by the Secretary of State together.

The CQC report recognises that whilst there is widespread commitment to the security of patient data there are challenges in delivering it in practice. It makes six general recommendations to improve matters.

The NDG review makes ten recommendations around security and further recommendations about establishing a new patient consent/opt out model. The Government will consult on these though has already stated it is supportive of the introduction of stronger criminal sanctions against those who use anonymised data to re-identify individuals.

The Government also published its response to an earlier consultation on the role of the NDG. The response includes numerous references to ICO evidence and aligns with our comments on the need for the ICO and NDG to work closely to provide effective regulation.

Outcome:

Following our extensive involvement in the conduct of the review, we drafted and submitted our response to the follow up consultation on the 7 September 2016. In it, we reiterated our views that whatever consent model was decided on, it was essential that individuals were told as

clearly as possible exactly what choices they had in terms of how their data was used and equally important where they did not have a choice.

We were also represented on a panel discussion at the Health Expo in Manchester alongside other members of the review panel. This was shortly after the consultation response was submitted so was a great opportunity for us to go out and let people know what our views were on the findings of the review.

Future Work:

Off the back of the review, we have been contacted by NHS England and NHS Digital regarding pieces of work they are doing around anonymising data. We have been, and will continue to be, working closely with NHS England and NHS Digital and other bodies in the health and social care sector to ensure that, in so far as they impact upon data protection, the recommendations of the review are implemented properly.

Contact: Stacey Egerton, Victoria Cetinkaya, Ian Inman

National Data Controller Model

In response to concerns raised by General Practitioners, NHS England has been working to develop a standard set of business requirements that supplier systems need to provide to enable data controllers to meet their obligations under the DPA when sharing data. We have attended three national workshops and numerous meetings with NHS England, data controllers and suppliers to provide advice. One supplier, whose system we have concerns about, has so far been resistant to the proposed changes, arguing that they are unnecessary.

Outcome:

We have been heavily involved in the various discussions that have been taking place on this topic, including dealing with a complaint about one of the system providers.

NHS England is in the process of finalizing the requirements agreed with data controllers and will be providing these to suppliers so they can provide costs and indicative timescales for implementing the proposed changes. We have advised that the proposed changes would go a long way to satisfying our concerns about the ability of data controllers to comply with their responsibilities.

Future Work:

We will continue to advise and support NHS England in finalising the requirements and to engage with key stakeholders to ensure that our concerns are addressed.

In addition, one of the system suppliers disputed our views on the nature of the system they provide. We will be going through their letter and advising NHS England of our views on it accordingly.

Contact: Andrew Rose, Victoria Cetinkaya

Connected Health Cities

We initially met with representatives from Manchester University who were working on the Connected Health Cities project. The project is looking at taking the premise of Care.data, using people's health data to improve health care in various ways but is looking to apply it on a local level. The project aims to make use of citizens juries to generate better 'buy in' from individuals about the benefits of the use of their health data, something they claim was one of the major issues with care.data.

The project has various initiatives going on across the North West and is still in the very early stages. However, we have already identified some issues around their understanding of anonymised data, as we feel that in some cases the data would not be anonymised.

Outcome:

We have agreed to meet with them again once they have completed their privacy impact assessment and we have had a chance to review it. They have also offered us the opportunity to be represented on both the Information Governance Steering Group and the overarching project board for the connected health cities project. This will enable us to influence the project and identify and address any further data protection or information governance issues early on.

Future Work:

The first meeting of the project board will be on the 1 November and we will be represented on that. In addition we are waiting on them to provide us with a copy of their privacy impact assessment for us to review. We will have a further meeting with them once this is done. This piece of work also ties in with the citizens' juries' work that we are engaged in. A second meeting of the jury review panel is pencilled in for late October.

Contact: Ian Inman, Andrew Rose

6. Business & Industry Sector

Good Practice

Work continues on further development of a second version of the SME toolkit. We are also working with a third party, the Outcomes Partnership, who wish to use the Toolkit content in a SharePoint application which they hope to make available via the Office 365 Security & Compliance Centre.

We have undertaken a number of visits to solicitors and aim to collate a summary of our findings to disseminate and assist compliance within the sector as a whole.

WhatsApp terms of service and privacy policy

[Redacted]

CMA Energy markets investigation: Energy database remedy

[Redacted]

Delivery of common API standards

To achieve the delivery of common API standards the CMA require nine UK banks to adopt and maintain common API standards through which data can be shared with other providers and third parties. The open API standard should be developed to be compatible with other regulatory requirements, such as the Payment Services Directive (PSD2).

To deliver this remedy, the CMA is requiring the nine institutions to create and fund an Implementation Entity with an Implementation Trustee, accountable to the CMA. Andrew Pinder has been appointed as the trustee by the Implementation Entity Steering Group.

The introduction of an Open API standard raises data protection and information security concerns in relation to third parties gaining access to sensitive banking and financial transaction data. The ICO recognises consumer trust over the use of data is vital in the delivery of common API standards. Strategic Liaison has taken part in FCA consumer panel sessions to address data protection issues over data handling and consumer trust. We consider open API third party service providers to be a potential market for the data protection seals scheme to focus on.

Further Action:

The banks are working towards meeting their requirements to make data available to third parties and open API standards a reality. As this work

progresses, the ICO will continue to engage with the British Banking Association, Payments UK, CMA and the relevant regulatory and consumer groups to ensure information rights and data protection remain key elements of the project.

Contact: Garreth Cameron

7. National Regions

ICO Regions

This quarter saw a change of reporting structure in the three Regional Offices following the retirement
of the former Assistant Commissioner for Wales, Anne Jones. The offices now constitute a single department under the leadership of the Head of ICO Regions who is supported by a Regional Manager in each location. In addition, the Senior Case Officers based in Northern Ireland and Wales have reverted to local line management. Whilst each office will continue to focus on local priorities determined in part by the priorities of the three devolved administrations, it is expected that the new structure will enhance the degree of complementarity shown in the actions of the offices.

Improving information rights compliance within the community and voluntary sectors

Work Includes: The NI Office continued its successful engagement with the sector through effective sector partnership with NI Council for Voluntary Action (NICVA) in the delivery of the #Data Friday programme. Sessions on 'Information Governance and Privacy by Design' and 'Data Protection in the Digital Age' took place as well as involvement in a separate but linked event on Cyber Security where key issues for the sector to consider in preparing for GDPR were considered. Partly as a consequence of this work, the Scotland Office has now developed similar links with the Scottish Council for Voluntary Organisations (SCVO).

Future action: Activity targeting the voluntary sector as a whole will continue in both offices. In Northern Ireland, a review aiming to further develop the programme through this partnership approach will take place whilst, in Scotland, the first outputs of the new relationship will be seen in the form of a series of blogs by the Regional Manager to be published on the SCVO website.

Outcomes: Improved information rights compliance across the voluntary and community sector in both Scotland and NI. Improved relationships brokered with the sector. Increased awareness of the two regional offices and of the ICO as a whole.

Contact: Shauna Dunlop, Rachael Gallagher (Northern Ireland)
Maureen Falconer (Scotland)

Embedding a Privacy by Design approach into the use of technology by Police Service of Northern Ireland (PSNI)

Work Includes: Following contact with the ICO regarding the rollout of Body Worn Cameras in the PSNI, staff from the NI office and Strategic Liaison worked together to provide bespoke advice to the PSNI. This included a recommendation that a Privacy Impact Assessment should be carried out to identify privacy risks to citizens.

Future action: No future work planned at present.

Outcomes: Following completion of the PIA and having undertaken our recommendations, BWV has now been rolled out across the Service in a privacy-friendly manner.

Contact: Rachael Gallagher (Northern Ireland)

Effective and informed application of information rights requirements in GP Practices across Northern Ireland

Work Includes: The development and delivery of a bespoke workshop for over 40 GP Practice Managers in Northern Ireland, incorporating key lessons from recent enforcement action. In addition, an information resource pack which included links to case studies, ICO guidance and details of other good practice compliance tools such as security toolkits, was provided.

Future action: We have been asked to consider developing an interactive and practical session for GPs.

Outcomes: Improved understanding across GP Practices of the technical and organisational management requirements to help ensure patients' data are properly protected, in part through the use of free ICO tools such as the self-assessment toolkit.

Contact: Shauna Dunlop (Northern Ireland)

Participation in the appeals system

Work Includes: Local staff attending an Information Rights Tribunal held in Belfast on 29 September were requested to provide clarification on exemptions and give advice on some of the information presented despite not formally representing the ICO at the Hearing.

Future action: Build on existing partnerships between local senior case officers and legal representatives within the ICO. Provide regional support internally and participate in court proceedings where necessary.

Outcomes: Enhanced profile and reputation of the ICO. Strengthened understanding and increased knowledge of legal proceedings in the ROs.

Contact: Deirdre Collins, Sarah O'Cathain, Rachael Gallagher (Northern Ireland)

Children & Young People (Scotland) Act 2014

Work Includes: This Act, amongst other things, provides for the establishment of a Named Person service providing a source of advice for parents and children as well as coordinating the exchange of information between professionals where a well-being concern existed. During the passage of the Bill, we had raised concerns over the relevancy of information shared and the need to provide practitioners with clear guidance on when and how information should be shared but we were not invited to give oral evidence. After two unsuccessful Petitions to the Court of Session, the Petitioners took their case to the Supreme Court which, in July, determined that the information sharing provisions of the Act had the potential to breach Article 8 of the ECHR. The Scottish Government is now embarking on a public engagement exercise to take advice on how the information sharing provisions of the Act should be enhanced to address the concerns of the Supreme Court and a short preliminary meeting has been held between the Deputy First Minister and ICO in this regard.

Future Action: Further meetings with the Deputy First Minister. Participation as observers on relevant working groups. Involvement in awareness raising sessions with practitioners.

Outcomes: ECHR Compliance of this key initiative of the Scottish Government. Enhanced understanding by professionals when non-consensual data-sharing is appropriate.

Contact: Ken Macdonald (Head of ICO Regions), Maureen Falconer (Scotland)

Child Death Reviews

Work Includes: The Scottish Government is seeking to establish a formal non-statutory process to review all child deaths in Scotland (in England, reviews are undertaken under relevant legislation). The ICO met with relevant officials to discuss the possible DP implications for family and professionals involved and how these might be addressed.

Future Action: To ensure DP considerations remain at the forefront of this initiative, the ICO will be represented on the project board as an Observer to provide advice and guidance.

Outcomes: Privacy issues are properly considered during the review and in the publication of any subsequent reports.

Contact: Maureen Falconer (Scotland)

Legislative Bodies

Work Includes: The ICO has been engaging with the staff of both the Scottish Parliament and the National Assembly of Wales. In Scotland, a series of DP awareness sessions have been delivered to the constituency and parliamentary staff of MSPs, explaining the basics of the DPA and how it affects their work both in acting on behalf of constituents, and developing or scrutinising legislation (this follows a similar strand of work undertaken with MSPs after the May elections). In addition, the information governance specialists from the offices of Ombudsman and Commissioners reporting to the Parliament attended a separate briefing at Holyrood focusing on the GDPR. In Wales, initial contact has been made with officials with the intention of delivering awareness raising workshops to the AMs; these will be similar to the sessions delivered to MSPs in Scotland.

Future Action: Further workshops in both the Scottish Parliament and the National Assembly of Wales.

Outcomes: Increased understanding of information rights by legislators and their staff. Improved scrutiny of legislation affecting individual privacy.

Contact: Ken Macdonald (Head of ICO Regions) David Freeland (Scotland), Dave Teague, Helen Thomas (Wales)

Welsh Government

Work Includes: A meeting was held with the Welsh Government IG lead to investigate how a closer working relationship between the ICO and the Welsh Government policy teams could be developed. An approach was agreed, focusing initially on workshops with staff and senior managers which would also incorporate examples of the contributions made by the ICO in the work of the other devolved administrations.

Future Action: Delivery of workshops to the Divisional Knowledge and Information Managers in October; Meeting with the Government's influential Operations Committee.

Outcomes: Enhanced understanding of data protection by Government policy teams. Incorporation of privacy considerations in policy development.

Contact: Ken Macdonald (Head of ICO Regions), Dave Teague, Helen Thomas (Wales)

NHS Wales

Work Includes: Recent activity within the Welsh health sector has focused on work with overarching groups. For example, we supported the Royal College of Speech and Language Therapists with their Therapy Outcomes Measures project and established a good working relationship with Community Pharmacy Wales. We also attended the NHS IG Managers Action Group where, following a complaint raised, we highlighted issues of lost health records and handling of transgender patients' records.

Future Action: Community Pharmacy Wales is to help coordinate auditing work being undertaken by the ICO in October. Follow-up review of Training and Awareness in NHS Wales to be undertaken in 2017.

Outcomes: Improved working relationship with Community Pharmacies Wales. NHS Wales is to update its policies and procedures relating to both load records and the handling of transgender patients' records.

Contact: Dave Teague, Helen Thomas, Bethan Bonsall (Wales)

Local Government

Work Includes: An anticipated reorganisation of local government in Wales has been postponed but we are continuing with a programme of local authority liaison which was initiated in advance of it. In this quarter, we met with both Gwynnedd County Council and the Isle of Anglesey Council where we focused on matters relating to governance and the requirements of the GDPR.

Future Action: Continued work with local authorities throughout Wales. Monitoring Welsh Government plans for this sector.

Outcomes: Raised awareness of GDPR and obligations arising from it.

Contact: Dave Teague, Helen Thomas (Wales)

8. International

Article 29 working party – EU data protection reform preparations

Stakeholder consultation on preparing for work under the GDPR

Following the ICO suggestion that the European Data Protection Board needs to be outward looking, in line with our own engagement policy, Article 29 Working Party members collectively hosted a workshop in late July. Stakeholders from public/private/third sector and academia were able to input at an early stage of preparations for the new EU legal framework. The event focussed on the Working Party developing a consistent approach in the four areas of the General Data Protection Regulation (GDPR) identified in the 2016 Work plan: Data Protection Impact Assessments, Data Protection Officers, Certification/Codes of Conduct and the new right of Data Portability. The ICO co-led the data portability session with civil society organisation eDRI.

Outcome: the results from the workshops have been published on the Article 29 Working Party website demonstrating a commitment to transparency. Working Party members working on Opinions and Guidance on these themes in preparation for the EDPB will use the results to inform the content. The outputs have also been shared across the ICO to aid our own implementation. The stakeholders provided positive feedback on the workshop and written input was also supplied by people unable to attend the event.

Next steps: a similar event on 2017 Work plan priorities for the Working Party will be held in the first half of 2017. The ICO will be working with the EDPS, the French data protection authority and others on guidance relating to certification of data controllers' activities under the GDPR.

Contact: Steve Wood/Hannah McCausland/Gemma Farmer

Article 29 Working Party members finding new ways for cooperation and consistency

The Working Party is required to make an effective transition to the European Data Protection Board (EDPB) by May 2018 when the General Data Protection Regulation starts to apply. This means that the Working Party must produce effective processes to ensure good cooperation and a consistent outcome across the EDPB's work. This involves the effective interpretation of article 60 GDPR on cooperation between the authorities, ensuring that members are clear about how to determine the lead supervisory authority, how to provide each other with mutual assistance (article 61), how to develop a successful joint operation (article 62) and

how to ensure the effective management of draft decisions before and during their passage to the EDPB (several articles).

The EDPB's Rules of Procedure will also develop detail around member voting, sub-group and reporting structure and the management of items admitted to the EDPB agenda. The EDPB's work also requires an effective IT system to enable rapid and straightforward communication between the EDPB members, as well as supporting the EDPS Secretariat in running the Board. The ICO forms part of the EDPB IT Taskforce and has contributed to the conduct of a survey of all data protection authorities in the EU on what should feature in the new EDPB IT system.

Several workshops were held at the end of the summer to elaborate these processes. The ICO is co-leading work on the determination of the lead supervisory authority, on the provision of mutual assistance to another supervisory authority as well as on the consistent application of administrative fines and other corrective measures. Members of the ICO International, Enforcement and Policy Legal teams participated. The ICO is reflecting on how to achieve a consistent approach to administrative fines and other corrective measures among supervisory authorities when cultural, economic and other factors come into play. A system requiring such a level of consistency relating to data protection is unprecedented but the Working Party has been looking for inspiration from existing systems in other sectors such as cooperation between national regulatory authorities in the competition or consumer protection domains.

Outcome: the ICO took the views expressed at the workshops and identified the main issues to take forward in the mutual assistance and administrative fines papers. The diverse views in the administrative fines debate will require more work than the work plan originally foresaw into 2017. Other pieces of guidance will likely meet the deadline of December 2016.

The ICO is remaining fully engaged in Article 29 Working Party activities in preparation for the GDPR notwithstanding the outcome of the June 2016 EU referendum in the UK. The future framework for data protection applicable to the UK has not yet been announced by the UK Government.

Contact: Hannah McCausland/Iain Bourne/Sally Anne Poole/Geraldine Dersley/Steve Wood/Jo Pedder

<u>International Conference of Data Protection and Privacy Commissioners (ICDPPC)</u>

The ICO has proposed a draft Resolution on International Enforcement Cooperation to the ICDPPC to improve the privacy enforcement authorities' collective response to cross-border cases. This continues ICO

work in this area ongoing for several years, examples of which include the Annual International Enforcement Cooperation event, the acceptance by the Conference of a Global Cross-border Enforcement Cooperation Arrangement and the Handbook on International Enforcement Cooperation.

Outcome: this resolution gathered the support from a variety of other authorities from a cross-section of continents around the globe.

Next steps: the Resolution will be tabled for adoption at the ICDPPC in Marrakech in October. If adopted, the ICO will produce an action plan for the rollout of the proposals in the Resolution. Any follow-up will need to be achieved by October 2017. The ICO and Canada's Office of the Privacy Commissioner (OPC) will also present the updated Handbook on International Enforcement Cooperation to the ICDPPC.

Contact: Hannah McCausland

Establishment of a new Article 29 Working Party sub-group on Enforcement initiatives

The activities of large or global business increasingly impact on many individuals within the jurisdiction of a large number or occasionally all Article 29 Working Party members. The effective management of these cases requires a greater level of information sharing among the Working Party.

Up to present, information has been shared in small task forces or contact groups and a less ad-hoc approach is required to ensure a more timely response from the Working Party.

Outcome: in light of a series of announcements recently about changes some global companies have made to their privacy policies and a number of major cross-border data breaches, the Working Party has decided to reactivate the dormant enforcement subgroup in order to increase its information sharing capacity. The new sub group's main objective is to help members to be as consistent as possible in their enforcement activity involving key actors operating in several Member States. It may also be able to test the cooperation mechanisms within the GDPR, though it is clear that the 1995 Directive still fully applies until May 2018. The subgroup will allow national enforcement officers to work together on the enforcement case in question as far as current legislation allows.

Next steps:
The first meeting will be held in November with the mandate expected to continue until May 2018. Members will need to choose a Chair.

Contact: Steve Wood/ Hannah McCausland

Article 29 Working Party: other matters arising

The Article 29 Working Party has worked on an Opinion on the revisions required to the ePrivacy Directive to bring it into line with the new GDPR.

Next steps: the Article 29 Working Party will be embarking on work in the following areas with the ICO's involvement:

- An opinion on access by public authorities to data held by private entities.
- A co-rapporteur role on a new piece of work analysing mobile health apps.
- A reflection document on profiling in relation to financial sector data processing, notably creditworthiness which will feed into a wider piece of work on risk and profiling of individuals in 2017.
- Further work following the European Commission's consultation on the upcoming presentation of a revised ePrivacy Directive, ensuring compatibility with the GDPR.

Contact: Hannah McCausland/Jo Pedder

International transfers to the US

On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield adequacy decision. The Article 29 Working Party welcomed the improvements brought by the Privacy Shield mechanism compared to the Safe Harbor decision. The finalised adequacy agreement contained a number of improvements the Working Party had called for. However, a number of concerns remain regarding both the commercial aspects and the access by U.S. public authorities to data transferred from the EU.

Outcome: the finalised Privacy Shield contains a number of enhanced privacy and redress rights for individuals which will make it easier for supervisory authorities to investigate any complaint about the way their personal data has been handled. The Privacy Shield also contains strengthened obligations for companies to protect personal data in line with the Privacy Principles:

- A right to be informed about the processing
- Limitations on the use of data for different purposes
- Data minimisation and retention periods
- Information about when data may be transferred to another company
- Right of access and correction
- Right to lodge a complaint and obtain a remedy
- Redress in case of access by US public authorities

The European Commission's Citizens' Guide to the Privacy Shield has been published which contains more information about the requirements of this instrument and will be regularly reviewed.

Next steps: the ICO will continue to work with our European colleagues to implement the requirements of the Privacy Shield including the EU centralised body and the process for transmitting complaints to the US. The ICO will provide further guidance to individuals and data controllers as these processes develop. The first joint annual review in summer 2017 will also be a key moment for the robustness and efficiency of the Privacy Shield mechanism to be further assessed. The possibility remains that a new case against the Privacy Shield could be taken to the Court of Justice of the European Union (CJEU). We continue to wait for the declaratory relief hearing in the Irish High Court and a referral to the CJEU to determine the legal status of data transfers under Standard Contractual Clauses.

Contact: Steve Wood/Geraldine Dersley/Naomi Osborne-Wood

International visitors

The ICO received three visits this period; the Dutch and Irish DPA Commissioners had introductory meetings with Elizabeth Denham. Commissioner Denham also visited the French DPA Commissioner. A representative of the Office of the Complaints Commissioner in the Cayman Islands also came to Wilmslow. The visit included discussions on designing training on data protection, technical and information security expertise and assessing security risks.

Contact: Alain Kapper/Naomi Osborne-Wood

Common Thread Network – relations with Commonwealth counterparts

The collection of data protection authorities in Commonwealth countries, known as the Common Thread Network, is continuing to grow and cooperation is flourishing.

Outcome: the Network has created a dedicated online portal to showcase its activities to any Commonwealth governments and other interested entities from civil society and the public at large which helps to promote the messages of good data protection practice across the Commonwealth. The portal has been soft-launched on 21 September and will be officially launched during the Annual General Meeting.

Next steps: the Network will meet for its Annual General Meeting at the International Conference of Data Protection and Privacy Commissioners in October to agree on its Terms of Reference as well as its work plan for 2017.

Contact: Hannah McCausland/Alain Kapper

Case Handling Workshop

The Annual European case handling workshop, which is organised under the aegis of the European Spring Conference of Data Protection Authorities is took place in Podgorica, Montenegro, on 13 and 14 October.

Outcome: the ICO has made a commitment to continue developing this valuable forum for data protection practitioners and ICO delegates will attend and present at the October event.

Next steps: the ICO intends to bid to host the 2017 case-handling workshop as part of our International Strategy to share know-how with our international colleagues and present ICO best practices in case-handling techniques. We will also produce a GPEN Enforcement Practitioners' Event to widen the knowledge-sharing to the global level.

Schengen Information System II (SIS II)

The ICO participates in the SIS II Supervision Coordination Group with other Schengen system participating countries in Europe. Supervision of the data processing in the SIS II units at national level is allocated to the data protection authorities in each Member State.

Between 5 and 9 September, the ICO Good Practice Team participated in its first expert on-site visit mission to evaluate the application of the Schengen Acquis in Malta in the field of data protection.

The first triennial SIS II Report, covering the activities of the Supervision Coordination Group and of its members between 2013 and 2015, was published in July 2016. This featured work that the ICO has contributed to including a SchEval evaluation visit (October 2013) as part of the assessment of the UK for its admission into part of the SIS II System, and took on board the comments made by the evaluation group.

Outcome/Next steps: the draft report of the evaluation mission is expected to be circulated by mid-October, once other aspects of the evaluation (police cooperation, visa issuance and borders) have been concluded. The ICO will provide comments where applicable.

Contact: Alain Kapper

BIIDPA – British, Islands and Irish Data Protection Authorities

The Data Protection authorities of the British Islands and Ireland (BIIDPA) continued their dialogue on the changing nature of adequacy in third countries' data protection law as a result of recent European case-law and what is required in order to fulfil their responsibilities set out in the new European data protection framework applying from 2018. Given the result of the UK European Union membership referendum on 23 June, the UK may start to experience some similar issues to its non-EU counterparts which were raised in these discussions. Therefore the continuation of contacts in this forum is even more valuable than prior to the referendum.

Next steps: the ICO has invited BIIDPA members to attend a workshop on 5 October with representatives of DCMS to discuss what the referendum vote means for the GDPR in the UK and the Crown Dependencies.
Contact: Alain Kapper

DfID Global Governance Fund: institution-to-institution Support Facility (GGF i2i Facility)

Two members of the ICO's Good Practice department went to Georgia in the last week of September 2016 to support the Georgia Office of the Personal Data Protection Inspector in implementing audit methodology in their everyday practice. This visit was made through the UK Department for International Development GGF i2i facility and was particularly relevant in helping the Georgian DPA to establish new risk assessment methods and review their audit methodology, allocate human resources and develop the overall management of audits and the way in which the outcomes are communicated to the wider public.

Outcome: the ICO received very positive feedback as a result of the visit and our staff found the work helped to inform our own future strategy.

Next steps: this was a first trial with this project and the ICO will consider future project invitations as they arise. The event report will be finalised and made available to SMT.

Contact: Alain Kapper

EURODAC Regulation 603/2013 (Recast)

Eurodac is the large scale database meant to store fingerprints from all people who cross the border into a European country without permission – asylum seekers as well as irregular migrants. The original Eurodac Regulation (EC) No 2725/2000 of 11 December 2000 intended to prevent multiple asylum applications and unauthorised entry. Its access was restricted to immigration authorities only. The recast Eurodac Regulation 603/2013 (1), which started to apply on 20 July 2015, has opened up access to police and public prosecutors, such as Europol, for enforcement purposes. Work has been undertaken to define the ICO's role.

Under Article 30 of the recast Eurodac Regulation (Article 19 of the original Eurodac Regulation 2725/2000), national supervisory authorities including the ICO are required to monitor the lawfulness of the processing of personal data by their member states. To assist with that monitoring, the Eurodac Supervision Coordination Group (SCG) had drafted a Standardised Inspection Plan in 2012, which required drastic adjustments in light of the recast Regulation.

The ICO has volunteered as co-rapporteur to review what changes are necessary to comply with the recast Regulation and assist DPAs in their task of evaluating the application of the Regulation in the field of data protection.

Next steps: a draft revised Standardised Inspection Plan has been submitted to the Chair of the EURODAC SCG and will be discussed at the next SCG meeting on 23 November 2016.

Contact: Alain Kapper

9. Enforcement

Direct marketing and nuisance calls

This quarter we issued four civil monetary penalties totaling £260,000 for contraventions of the Privacy and Electronic Communication Regulations (PECR), by organisations making or sending unsolicited marketing calls and messages.

The largest fine in this quarter was £130,000 against Intelligent Lending t/a Ocean Finance. Other fines included £60,000 against Omega Marketing Limited, £40,000 against Vincent Bond and £30,000 against Carfinance 247 Ltd. In the year to date we have issued nine monetary penalties for marketing contraventions for £870,000 in total. Nearly half a million pounds has been issued through Notices of Intent for which we await representations, with a further £1.5 million currently going through our internal decision making processes.

This quarter we also served two Enforcement Notices; one to Intelligent Lending t/a Ocean Finance, to accompany the monetary penalty above, and one against Change and Save Ltd to compel their future compliance with the law. Four further Preliminary Enforcement Notices were issued against companies in this period. Representations are due in the next quarter in respect of those notices.

We issued one fixed penalty notice under the Privacy and Electronic Communication Regulations against a communications service provider for failing to report an unauthorised disclosure of personal data as a result of a security breach. Telefonica 02 received a fixed penalty of £1,000.

We monitored five organisations this quarter which we believe represent risks in relation to compliance with PECR. We held five meetings with organisations to tell them to improve their direct marketing practices. In the year to date, we have monitored nine organisations and held 11 compliance meetings.

The ICO's investigation into a number of charities and their fundraising activities is drawing to a close. We expect to conclude our investigations soon, with decisions about formal enforcement action being made in the next quarter. Any decisions will be publicised in the usual way, and according to our policy on Communicating Regulatory Activity. We also met with the Charity Commission on 2 September to discuss our developing working relationship.

We are developing our understanding of the lead generation and list brokerage industry through Operation HIDA, which has involved mapping the organisations involved in trading and sharing personal data. Internal

briefings on the project's findings have been completed and next steps are to be agreed and progressed during the next quarter, when we also aim to publish an external report on our findings.

Data loss incidents and Cyber-security

Case receipts have remained steady – with approximately 500 new cases being received into and risk assessed by the civil team. We are reviewing our approach to the triage process following a successful pilot in September, which identified some efficiencies in the progression of cases.

As reported at the end of the first quarter, the team introduced new categories into the risk assessment in relation to cyber incidents, to enable more detailed statistical information to be provided in relation to these incidents. The team has received reports of 73 cyber incidents in the second quarter, compared with 50 incidents in the first quarter.

We are currently running recruitment exercises to recruit a specialist sub-team, to sit within the civil team, to investigate breaches of the DPA relating to technology. However, both exercises have failed to attract applicants with the relevant experience. We will be meeting with HR to discuss how to approach this problem, which may include seeking temporary staff through recruitment agencies or looking at secondment opportunities from outside the business.

To help better manage our response to cyber incidents, we are looking to convene an ongoing group of regulators with an interest in cyber-security to share good practice, exchange information and ensure consistent messages to businesses. We are currently looking to link in with the likes of the National Cyber Security Centre at GCHQ and the NCA Cyber Security Hubs. Work on this project will continue into the third quarter.

The investigation into the widely publicised TalkTalk data security breach of October 2015 concluded in the second quarter, with the serving of a civil monetary penalty. TalkTalk Telecom Group PLC was fined £400,000 – a record amount for the ICO.

We have served a further three CMPs in relation to data loss incidents:

- To Hampshire County Council – a CMP for £100,000 in relation to the council's failure to decommission a building properly.
- To Whitehead Nursing Home Ltd – a CMP for £15,000. The data controller reported the theft of an unencrypted laptop from a staff member's home. The investigation revealed a lack of policies, procedures and training in relation to data protection. This was the ICO's first CMP to a care home.
- To Regal Chambers Surgery – a CMP for £40,000 following the disclosure of confidential details about a woman and her family, to

her former partner in error. This was the ICO's first CMP to a GPs surgery.

The team has served two undertakings in the second quarter. The undertakings were served on Northern Health and Social Care Trust, following a breach that led to emails being sent to a member of the public in error, and Kent Police, to commit the data controller to taking steps to address a compliance issue that was the subject of a CMP in the first quarter of this year.

So far this year the team has served eight monetary penalty notices (MPNs) and four notices of intent (NOIs). This is a significant increase on last year's activity, when two MPNs and two NOIs were served by 30 September 2016.

The department is continuing to prepare for the implementation of the GDPR. In August, we held a workshop for delegates across the ICO, to discuss case studies and consider how we may exercise our investigative and corrective powers from 25 May 2018. Two members of staff attended a workshop in Brussels on 1 September 2016, to further the collaborative work being undertaken with Norway on guidance for the issue of fines and penalties as part of the Article 29 subgroup.

Subject Access

Three Enforcement Notices were served in relation to non-compliance with subject access requests.

Operation Spruce

[Redacted]

Criminal investigation and prosecutions

[Redacted]

International enforcement

The result of the GPEN Sweep, this year focusing on 'Internet of Things' devices, was announced on 22 September 2016. The Intelligence Hub led the exercise on behalf of the ICO, with 25 authorities participating globally. From a UK perspective we looked at health and fitness devices, purchasing wearable devices, reviewing privacy policies and contacting NHS Trusts. A working group has been set up to coordinate follow-up activity. We have also started work to decide upon a topic for the 2017 Sweep.

We are pursuing a number of projects with members of the London Action Plan, as well as coordinating the recent name change to the Unsolicited Communications Enforcement Network (UCENet). Ongoing projects include identifying intelligence contacts, combining expertise and training materials and continuing to develop the first UCENet Sweep, where members will cooperate on the theme of affiliate marketing. This will develop a global understanding of the practice and identify opportunities to coordinate activity. The ICO will be presenting a number of sessions at the upcoming UCENet 38th annual event in Paris in October.

Work is underway to prepare for the International Conference in October – including changes being made to the International Enforcement Cooperation Handbook, and work on a new resolution about international enforcement cooperation. We are working with international colleagues in relation to high profile issues such as the Vtech breach and the changes to the WhatsApp privacy policy.

A member of staff is on secondment to the Office of the Privacy Commissioner in Canada, thus strengthening ties with that organisation.

A workshop to consider the international co-operation aspects of GDPR is taking place in November.

Engagement activities and service improvements

We publish a quarterly data security incident trends report as well as the monthly nuisance calls and messages threat assessments on our website. The nuisance calls report was recently revised to make it easier to read and to help people understand the key information. We shared intelligence with other regulatory and law enforcement organisations to support our enforcement activity and their priorities.

We chaired a meeting of the Operation LINDEN group on 22 July 2016, providing an opportunity to coordinate activity amongst regulators and consumer and industry groups on the topic of unsolicited calls and text messages. We attended the Insurance Fraud Disruption Committee on 13 July, chaired by the Insurance Fraud Bureau, which facilitates the sharing of intelligence in relation to our criminal investigations and PECR enforcement.

We reviewed our current approach to the enforcement of Cookies, taking a paper to SMT to ensure that we are continuing to target the appropriate organisations and taking into account new technologies. A new process is in production.

Recruitment to new vacant posts in the Intelligence Hub has been completed.

Following the successful Local Government workshops held across the country last year to improve Data Protection compliance in Children's Services, we will be revisiting a Data Controller in November who attended the Manchester workshop to see how they used the learnings from the event to improve compliance in their organisation. The visit will be filmed by the Communications Team and incorporated into the filming already held of the actual workshop in Manchester.

Enforcement Forward Activity

[Redacted]

10. Performance Improvement

The second quarter of 2016/17 has continued to challenge because of significant increases in intake. It is a risk to the organisation that we won't be able to deal with all of the complaints made to us this year, and our outstanding caseloads will continue to rise.

DP complaints/concerns cases are up by 22% when compared to the same quarter last year and FOI cases are also up a further 10% on those received last year. As highlighted at the end of the first quarter we have the highest intakes across DP and FOI since 2009. As a result we have not been able to exceed intake with closures. This is despite some good overall productivity returns – output for DP is up 18% and FOI by 7%. Inevitably overall caseloads have increased. We are still able to close with over 70% of cases coming to us within 3 months of receipt, but there is a risk that this performance will suffer as the age of unresolved cases increases.

In an attempt to increase capacity we intend to introduce a 7th Improving Practice Group that will have responsibility for a significant number of data controllers and predominantly across those in the private sector. Although case increases are seen across the board, the general business sector is the one that requires most assistance. We have completed lengthy recruitment exercises for new staff at the case officer grade, and have 12 new entrants due to join the ICO this quarter. We still provide experienced staff to various other areas in the business to support preparations for the future and implementation of GDPR, as well as other ICO initiatives. With our new joiners the Performance Improvement Department should be in line with agreed headcount for this year. 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 65 new cases this quarter and we were able to conclude 59. This is a slight decrease in numbers from the previous quarter. Lower level self-reported incidents are also being handled within the department and we have dealt with an additional 480 cases at the time of writing.

Formal Freedom of Information monitoring activity continues. Following the latest monitoring report, and a co-ordination meeting, London Borough of Newham was put on formal monitoring, this will cover the period up to and including November 2016. Two other Councils were also identified as potential formal monitoring candidates but further investigation and consultation determined that this would not be

appropriate or proportionate to pursue formal activity at this time. This quarter, following sustained improvement, Trafford Council were taken off formal monitoring. However, we are following up with them on one long overdue request which could potentially become an enforcement notice issue.

The Metropolitan Police Service has shown improvement in its information rights delivery over the last 3 months. This is mainly due to further recruitment and making some operational changes, to address their performance issues. We continue to work closely with them and although their 'in time' performance is still not to a satisfactory level (latest figure 80%), the age profile of their cases is improving. We will be meeting them again to discuss performance in October. The Cabinet Office quarterly FOI statistics for central government were published last week. These figures along with the previous quarter and the 2015 annual figures are being used to tailor letters to all Departments of State regarding their FOI performance. These letters will go out in early October 2016. This follows on from the successful initiative carried out with Northern Ireland Departments during 2015/2016. During the quarter we also concluded the informal monitoring of a government department, a district council and an NHS body following sustained improvements.

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

We received a complaint about a travel company who disclosed a client's debit card details in an email to another client. An action plan was requested and the organisation has since implemented new procedures such as no longer sending card or bank details via email, the introduction of risk register, and providing specific training for all staff in relation to disclosure of personal data via email.

An organisation refused to comply with a request for their personal information because the employee dealing with the request had focused on the threat of a court application being made for pre action disclosure of the requested information. The individual received the requested information five months after the original request. As part of our investigation the organisation provided an action plan to ensure that future subject access requests are dealt with correctly it has introduced a wallpaper for staff computers detailing how to handle access requests, and is introducing compulsory training for all qualified lawyers surrounding handling SARs and data security.

A prisoner's documents were handed to visitors without her knowledge or consent. Procedures were in place but the staff member was new to

reception and it was unclear whether they were aware of them – staff were “encouraged" to familiarise themselves with policies. When the prisoner reported this the DPA concerns did not appear to be addressed. An action plan has been requested to outline how recurrence of this can be minimised and to detail how staff will be trained and apprised of policies and also to ensure breaches responded to swiftly.

As a result of individual complaints we were concerned that an organisation was misapplying section 9(a) of the DPA, suggesting data could not be considered as it fell outside of a relevant filing system/the request was voluminous. The case officer had a telephone conference with the organisation to provide clarification. The organisation subsequently reviewed its handling of the DPA issues raised, accepted s.9 (a) wasn’t applicable and disclosed more information to the individuals in question. The organisation has continued to engage with the ICO which has resulted in a Senior Policy Officer from the Scotland office attending and contributing to a DC training day. The DC has also requested further correspondence to ensure future requests are handled in-line with our guidance.

An organisation was using body worn camera footage to issue littering fines. When an individual made a subject access request for the footage / image it refused to provide this but did not seemingly have a basis for doing so. We asked the organisation to take action and bring themselves in line with the requirements of the DPA. The company has since agreed to provide the individual with the images. It has also updated its standard operating procedure manual as a result of our intervention.

An action plan was requested from a council following concerns about the disclosure of personal data along with accuracy and adequacy concerns of the data being recorded. The council has now created a new data breach action log with reports being sent to senior leadership. It has also changed its procedures regarding mandatory DPA training and will now co-ordinate complaints and data breaches within one office to ensure consistency. In addition the council has created a new case record system to ensure records are updated and new procedures have been put in place to scrutinize the quality of case recordings.

Two of the ICO’s Lead Case Officers are delivering an introductory session to the FOIA/EIR for up to 60 delegates at the 2016 national conference for the Society of Local Council Clerks. Through this session they expect to improve the knowledge held by clerks about managing information requests and also promote the proactive disclosure of official information through Publication Schemes under s.19 of the FOIA.

A council disclosed sensitive personal data about third parties when sending a transport appeal form from their Special Educational Needs

department. The form should have been blank, however it was emailed without appropriate checking and accidently contained sensitive attachments. The council has since introduced compulsory e-learning course for staff across organisation and the DP officer is also giving face to face DP training to the team responsible for disclosure to highlight importance of data handling.

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

Contact : Andy Laing