Findings from ICO audits and follow up reviews of police forces

Version 1.0, 30 May 2015

Executive summary

This report highlights our experience of personal data handling from 40 ICO audits and 30 follow-up audits of police forces. It is intended to help them, other forces, and others in the criminal justice sector see where they can make improvements in how they handle personal data.

Overall we were encouraged that 54% of all recommendations we had made as part of our initial data protection audits with forces had been completed by the time of our follow up reviews. A further 30% were partially completed or in progress.

Where the 'Requests for personal data' scope was covered as part of our audit we saw the highest assurance ratings in this area. This was also where the most recommendations from follow ups had been successfully completed.

Records management was the area that received the most limited assurance ratings, and was where the fewest recommendations from follow ups had been completed.

We believe that there is still work to be done to mitigate information rights risks, and in particular police forces need to implement changes in some common areas of concern.

Summary of findings

✓ Requests for personal data

Tracking of subject access requests was generally being effectively managed through the use of logging and monitoring processes.

Case study: Effective tracking of subject access requests

A comprehensive log of subject access requests can be maintained by utilising a bespoke application. The application is used to log all requests for data (whether subject access or disclosures) and to manage the process of compiling, redacting and disclosing data in response to those requests.

The application has a built in 'traffic light system' to track the progress of requests and to help ensure they are processed in line with statutory timeframes.

It records all correspondence that is sent and received in relation to each request. For example, copies of letters and emails, records of phone calls, records of cheques received etc. Hard-copy correspondence is scanned onto the application to ensure that the record is complete.

The application of any exemptions and redactions is recorded, as well as any rationale for those actions and any quality assurance process that was undertaken in relation to those decisions.

There is the capability to generate figures and statistics in relation to requests that are received and handled. This allows monitoring and reporting of statistical information.

! Records management

This was the area that received the most limited assurance ratings. It was also the area where the fewest recommendations from follow ups had been completed. Typical areas where we observed that controls could be enhanced and improvement made included:

- Lack of refresher training plans for records management.
- Lack of controls or processes for the secure disposal of electronic and manual records.
- No information asset register or information asset owners.

The risks involved in this area are highlighted in the following case study, which resulted in the ICO issuing a Civil Monetary Penalty.

Case study: Sensitive personal data left in former police station

A box of videotapes belonging to a police force were found in the basement of a former police station. The building which had previously been unoccupied for almost three years was now owned by a private owner. The owner had discovered the tapes and was intending to view the contents as a possible source of entertainment. The items left included documents and video/audio tapes containing confidential and highly sensitive personal data about a significant number of individuals. These included files relating to threats to kill, rape, grievous bodily harm and child abuse cases; interviews with victims, witnesses and informants and suspects; sickness and absence records; and details of loans and pay relating to police staff. Some of the information dated back to the late 1980's but most of it was fairly recent.

This case represents a serious contravention of the seventh data protection principle. In particular, the force failed to take appropriate organisational measures against unauthorised processing and accidental loss of confidential and sensitive personal data.

In the absence of any specific policies or procedures, it wasn’t clear who was ultimately responsible for ensuring that the former police station was vacant at the point of sale. This lack of documented procedures was exacerbated by a breakdown in communication between the different departments involved in the long process of decommissioning the building.

There were inadequate procedures to ensure an accurate inventory of all information assets held at the station, which would have supported specific procedures to ensure that the basement of the former police station was cleared of all items before it was vacated.

Indeed, it was purely by chance that a police officer visited the buyer’s business premises on an unconnected matter and happened to notice the box of videotapes belonging to the force.

The fifth data protection principle was also contravened by the force in that data was kept for longer than was necessary for its purposes.

Recommendations

Based on our overall findings at audit and follow up, we are making the following recommendations to police forces to improve how they are handling data:

Training and awareness

- Introduce specialist training for key roles.
- Conduct refresher training in data protection, records management and information security.
- Implement staff awareness campaigns or strategies to support key information governance policies.

Case study: Effective delivery of data protection induction training

Staff are required to complete data protection and information security as part of their induction, and before they are allowed to access certain systems. All officers and staff, irrespective of their role or employment status, are mandated to complete the induction course; this includes temporary contract staff, agency staff and volunteers. There are plans in place to introduce a procedure which will require new members of staff to complete mandatory e-learning prior to an appointment date being confirmed.

There are also established on-going training plans for existing staff to determine their development needs, including training for data protection, records management and information security.

Bespoke, role based e-learning training and presentations have been created and delivered, such as data sharing training for high risk departments. The e-learning course is made mandatory and includes a knowledge check, with a compulsory pass mark being set.

Audit and compliance checks

- Conduct periodic information security audits which include manual records audits.
- Regularly check compliance to retention and disposal schedules and audit the disposal of electronic and manual records to ensure this is being conducted in line with agreed schedules and has appropriate security controls in place.

- Review the processing by third party suppliers of force 'owned' data, which includes a review of third party contracts, and information security controls.

Policy and procedure

- Establish a clear policy framework for information governance.
- Introduce new policies or procedures, especially in records management, to fill any gaps.
- Ensure there is appropriate version control, document change history and review dates for all key policies.

Information asset registers, owners and risk assessment

- Identify and train information asset owners.
- Create or update an Information asset register, supported by hardware and software registers.
- Conduct risk assessments for all information assets and maintain up to date risk management accreditation document sets (RMADs).
- Create and maintain an Information risk register.

Network access controls

- Implement appropriate endpoint policies and controls to prevent unauthorised uploading or downloading of information to mobile media devices.
- Review the allocation of, access to and usage of hardware assets (printers, faxes, laptops, USBs and body worn cameras).
- Ensure that information systems accesses are reviewed regularly and any changes in employment (eg new starters, leavers, maternity leave or long term sickness) are reflected in current access permissions.

Case study: Effective management of information security incidents

Guidance is made available for staff on the different types of security incidents which may occur. Staff are required to report all incidents to their line managers, who then pass the details on to the Information Security Officer via an online form.

There is an incident log maintained which records all reported incidents and 'near misses'. As part of the maintenance of the incident log, any further actions necessary if incidents are recurring or raise other concerns are recorded and tracked.

Investigations of security breaches are conducted and discussed at the relevant board. All incidents are also flagged to the SIRO. Any new risks are added to the appropriate risk register.

Learning outcomes from security incidents are circulated either via the the force intranet, or by email to all staff. Posters have been created and placed around force buildings to enhance awareness of security procedures in general.

Record storage, retention and disposal

- Implement processes to log and track the movement or security of manual records.
- Review existing records retention and disposal schedules to ensure they remain accurate and up to date.

Governance structures

- Establish clear roles and responsibilities for records management.
- Introduce data protection 'champions' to support the information governance teams in operational departments.

Privacy impact assessments

- Conduct privacy impact assessments for all projects that have data protection implications and ensure the assessments have had input from a data protection or information security representative.

Data sharing

- Regularly review existing information sharing agreements.
- Establish data quality assurance processes and checks before and after the disclosure of personal data.
- Introduce quality controls to ensure data that has been shared with a third party is only kept for as long as necessary.

Further action

The ongoing programme of ICO audits has allowed forces and the Commissioner to gain assurance regarding the way personal data is being processed as well as identifying underlying risk; however, analysis of our follow-up activity shows that some of the key areas highlighted by these audits are yet to be fully addressed. Failure to do so leaves the potential for data breaches and should such a breach result from the failure to accept or fully implement one of the ICO’s recommendations then this may be reflected in the level of regulatory action taken.

We feel there is an opportunity for the risks highlighted during our audits to be explored further through round table discussions amongst data practitioners across various forces, with the aim of sharing of best practice, ideas and methods for overcoming key challenges in order to meet data protection obligations. The ICO is keen to facilitate this and other national organisations such as The National Archives are available to provide support, advice and guidance.

Appendix 1 – audit findings in detail

Overall audit assurance ratings

In total, we have audited 40 police forces and given the following assurance ratings:

Audits completed	High assurance	Reasonable assurance	Limited assurance	Very limited assurance
40	2	24	14	0

During the last 12 months (April 2014 – April 2015) audits have resulted in the following assurance ratings awarded:

Year	Audits completed	High assurance	Reasonable assurance	Limited assurance	Very limited assurance
Apr 2013 – Apr 2014	17	1	10	6	0
Apr 2014 – Apr 2015	10	1	2	7	0

This year has seen an increase in the percentage of limited assurance ratings, with 70% of audits awarded this rating. Prior to this year this rating had only been awarded in 23% of audits.

The year saw another force achieving an overall high assurance rating. In addition, high assurance ratings have been awarded within individual scope areas covered, with most in the requests for personal data scope area.

There has been no overall very limited assurance rating awarded to date, however this rating has been awarded in individual scope areas. The main scope areas of concern were data sharing, and records management. As the figures below show, although data sharing is a relatively new area to be included in our audits, where this scope was covered two-thirds of forces received a limited or very limited assurance rating. This may be indicative of an emerging trend in poor compliance with this area of data protection compliance.

Assurance ratings in individual scope areas

Scope area	Rating	Total
DP governance The arrangements and controls in place to ensure compliance with the DPA.	High	0
	Reasonable	1
	Limited	1
	Very limited	0
Records management The processes in place for managing both electronic and manual records containing personal data.	High	0
	Reasonable	2
	Limited	8
	Very limited	0
Requests for personal data The procedures in place to deal with any requests for personal data.	High	1
	Reasonable	2
	Limited	1
	Very limited	0
Security of personal data The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.	High	0
	Reasonable	2
	Limited	0
	Very limited	0
Training and awareness The provision and monitoring of staff DPA training and the awareness of DPA requirements relating to their roles and responsibilities.	High	0
	Reasonable	0
	Limited	1
	Very limited	0
Data sharing The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the Information Commissioner’s Data Sharing Code of Practice.	High	1
	Reasonable	1
	Limited	2
	Very Limited	2

Appendix 2 – follow up findings in detail

Background

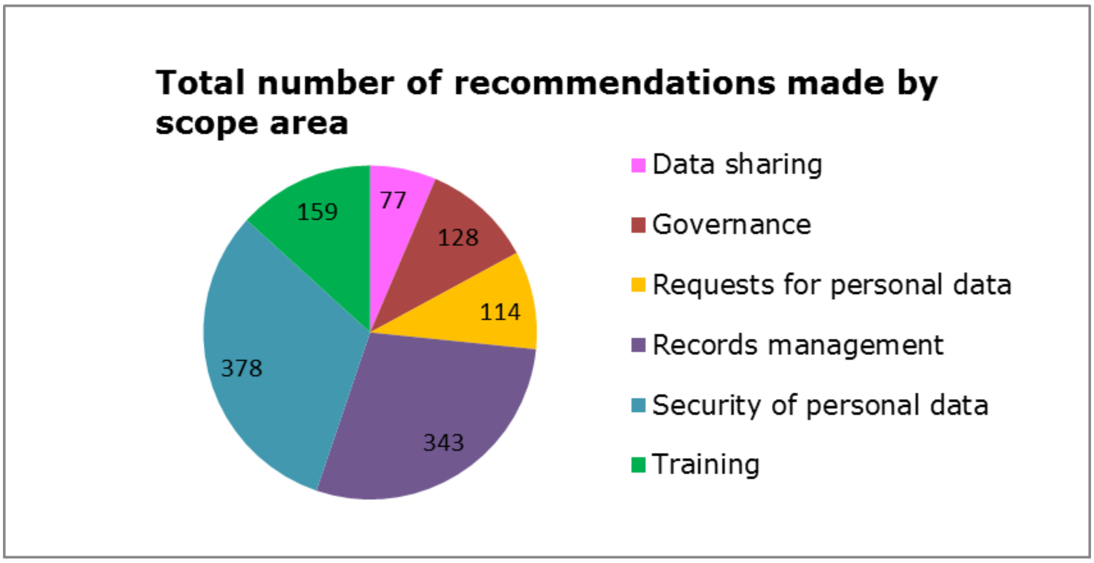
Following our audits, the ICO conducted follow up reviews with each force. The level of this review is dependent on the original assurance rating awarded for the audit. The reviews evaluated the progress forces had made towards addressing priority recommendations through completion of individual audit action plans. They also help the ICO to understand how our audit engagements with data controllers can best add value and maintain focus on the areas of greatest risk.

Overall findings of follow ups

We analysed the 30 follow up reviews to identify the number of recommendations made per scope area that were fully completed, partially completed and not completed or rejected.

Overall we were encouraged that 54% of all recommendations made had been completed by forces by the time of our follow up review. A further 30% were partially completed or in progress.

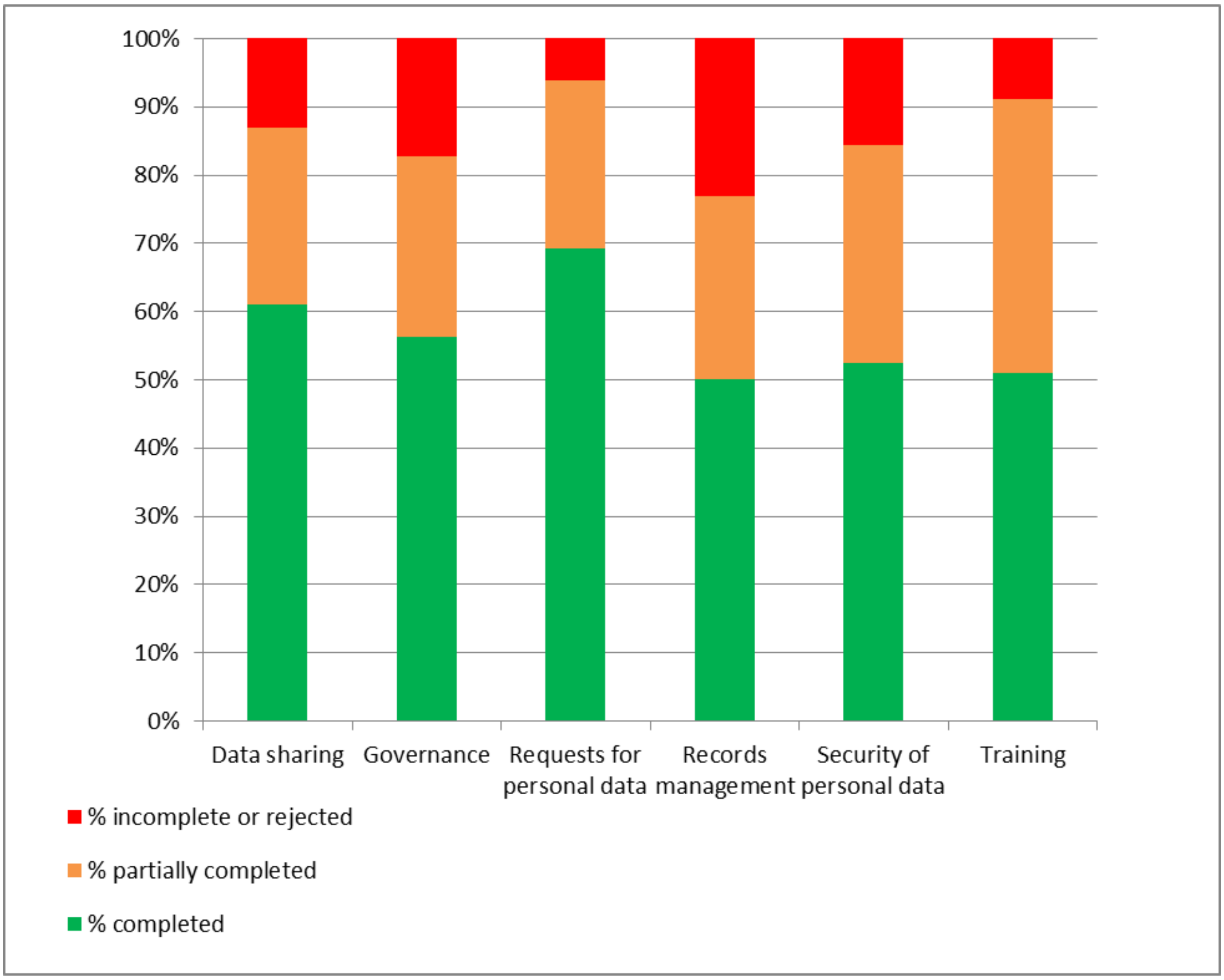
Analysis of the data identified a varying number of recommendations made depending on scope area.



Scope area	Total number of times scope audited	Total number of recommendations made	Average number of recommendations made per audit
Data sharing	8	77	10
Governance	12	128	11
Requests for personal data	14	114	8
Records management	21	343	16
Security of personal data	21	378	18
Training	16	159	10

Although both the records management and security of personal data scope areas had the highest number of recommendations made in total across the period, they were also the scope areas most covered during the audits completed. The average number of recommendations made per audit in these two areas is significantly higher than in other scope areas.

We identified trends in the completion of recommendations based on scope area, with the following results:



The above chart shows that the lowest completion / implementation rate for recommendations made fell within the records management scope area. The highest number of recommendations completed was identified within the requests for personal data scope area.

Conclusions

The analysis of follow up activity conducted to date highlights some key compliance areas where forces have not yet been able to mitigate risks identified during our original audit activity.

Our initial work indicated that forces typically face challenges when undertaking and completing our recommendations in certain scope areas. In particular, recommendations made in relation to processes for managing both electronic and manual records (50% only partially complete or incomplete) and the technical and organisational measures in place to ensure that there is adequate security (48% only partially complete or incomplete) were not always addressed.

Common themes include lack of progress towards creating and maintaining an information asset register (IAR) and assigning and embedding the role of Information Asset Owner, with over a quarter of the incomplete recommendations within the records management scope area directly related to this.

Further trends are highlighted in relation to training and awareness for both general staff and those with specialised roles within information governance, with almost 50% of all recommendations made only being partially completed or incomplete. Forces have national standard e-learning courses available as part of the Management of Police Information NCALT training however there was typically a lack of more bespoke localised training or refresher training, particularly within records management.

Within the security of personal data scope area 28% of recommendations partially complete or incomplete related to audit or compliance checks, particularly around retention and disposal of records and information security checks of both internal force premises and third party suppliers. Recommendations such as the introduction of ‘clear desk’ and workplace security checks and periodic information security audits of third party contractors appeared to pose a challenge for many forces.

It is unclear at this stage the reasons for no action being taken in some areas or why actions have been agreed, but have not progressed to completion as expected. There were inconsistencies identified in individual forces approaches to achieving data protection compliance and the application of police guidance nationally. Also there was an uncertainty within forces as to how to practically tackle some of the issues raised due to funding, resourcing and conflicting policing priorities and what the minimum standards should be.