Scottish Police Authority

Data protection audit report

Executive summary

Information Commissioner's Office

1. Background

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

In December 2014 the Scottish Police Authority (SPA) and Police Service of Scotland (PSoS) self-reported an information security breach which occurred in April 2014. The breach involved the loss of an unencrypted data stick containing sensitive personal data relating to 15 criminal investigations. The ICO Enforcement Department conducted an investigation and this resulted in a recommendation that a consensual audit would be the most effective way of improving compliance within SPA. The ICO recommended the following remedial action:

1. This breach highlighted the use of unencrypted devices within the organisation. Please ensure that unencrypted devices are not used for the storage and transportation of personal data, by third parties with whom personal data is shared or by the Scottish Police Authority itself.

2. Please ensure that the organisation has information sharing protocols in place between itself and other third parties where personal data is shared including Police Scotland.

3. Please ensure that staff awareness of DP issues continues to be raised by ensuring good attendance rates at any mandatory DP training the organisation may provide and that this training is regularly reviewed and updated as necessary, with refresher training being provided as appropriate. Please ensure that the organisation is able to track attendance on such training.

SPA agreed to a consensual audit by the ICO of its processing of personal data.

A teleconference was held on 25 May 2017 with representatives of SPA to identify and discuss the scope of the audit.

The audit field work was undertaken at SPA Pacific Quay and Scottish Crime Campus, Gartcosh, Glasgow between 8 and 10 August 2017.

2. Scope of the audit

Following pre-audit discussions with SPA it was agreed that the audit would focus on the following areas:

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.

Training and awareness – The provision and monitoring of staff data protection and information security training and the awareness of data protecting and information security requirements relating to their roles and responsibilities.

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 good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

3. Audit Approach

The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

The purpose of the audit was to provide the Information Commissioner and SPA with an independent opinion of the extent to which SPA within the scope of this agreed audit, is complying with the DPA.

Where areas for improvement were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with the DPA.

In order to assist data controllers in implementing the recommendations each recommendation has been assigned a priority rating based upon the risks that they are intended to address. These ratings are assigned based on the following risk matrix:

Impact	Severe	High	High	Urgent	Urgent
	High	Medium	Medium	High	Urgent
	Medium	Low	Medium	Medium	High
	Low	Low	Low	Medium	High
		Remote	Unlikely	Likely	Very Likely
		Likelihood			

It is important to note that the above ratings are assigned to the recommendations based upon the ICO's assessment of the risks involved. SPA's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

4. Audit opinion

The purpose of the audit is to provide the Information Commissioner and SPA with an independent opinion of the extent to which SPA, within the scope of this agreed audit, is complying with the DPA.

Overall Conclusion	
Very limited assurance	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment. We have made two very limited and one limited assurance assessments where controls could be enhanced to address the issues which have been identified.

5. Summary of Recommendations

Urgent Priority Recommendations – These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of the DPA.	We have made **28** urgent priority recommendations across all three scope areas: **17** in Information Security; **5** in Training and Awareness and **6** in Data Sharing where controls could be enhanced to address the issues identified.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of the DPA.	We have made **72** high priority recommendations across all three scope areas: **39** in Information Security; **18** in Training and Awareness and **15** in Data Sharing where controls could be enhanced to address the issues identified.
Medium Priority Recommendations - These recommendations address risks which can be tackled over a longer timeframe or where mitigating controls are already in place, but which could be enhanced.	We have made **10** medium priority recommendations across all three scope areas: **3** in Information Security; **6** in Training and Awareness; and **1** in Data Sharing where controls could be enhanced to address the issues identified.
Low Priority Recommendations - These recommendations represent enhancements to existing good practice or where we are recommending that the data controller sees existing plans through to completion.	We have made **7** Low priority recommendations across two scope areas: **4** in Information Security; and **3** in Training and Awareness where controls could be enhanced to address the issues identified.

6. Summary of audit findings

Areas of good practice

There is an overall Information Security policy in place supported by some topic-specific related policies and procedures. This includes the Physical and Environmental Security Policy, Electronic Communications SOP and the Remote Working Policy. In addition to information security related policies and SOPs, SPA also has a Data Protection and Records Management Policy.

Desktops and remote devices have Symantec endpoint controls in place to ensure that staff cannot use unauthorised USBs.

Areas for improvement

PSoS provides SPA with ICT services. SPA does not have a written supplier agreement in place with PSoS which includes clear instructions that defines what they can or cannot do with the data accessed as part of the services.

Risk management within SPA does not include information risks. Whilst both a Risk Management Policy and corporate risk register are in place there is no inclusion of information risks.

Privacy impact assessments (PIAs) are not carried out for all new projects and changes to existing systems. PIAs are also not completed to make informed decisions about whether to proceed with information sharing.

There is no effective asset management within SPA. There is no information asset register in place which records both physical and electronic assets held. Information Assets Owners (IAO) have not been established for all assets.

SPA does not have an Access Control Policy in place which defines procedures for Line Management and HR to follow in the event of a new starter/leaver or mover. Due to the lack of communication between departments, access to systems is not effectively managed.

Physical security risk assessments are not carried out by the Information Management Team (IMT) across SPA.

There is no Incident Management Policy in place which clearly defines staff responsibilities and the requirement to report information security incidents to IMT.

There is no formal data protection or information security training programme in place for SPA.

Delivery of training is not consistent within corporate departments and Forensic Services. Whilst the Head of Information Management (HoIM) is responsible for conducting training for corporate SPA, this does not extend to Forensic Services.

SPA does not mandate any data protection or information security refresher training.

SPA regularly shares information with third parties including PSoS, the Crown

Office and Procurator Fiscal Service (COPFS) and the Police Investigations and Review Commissioner (PIRC). SPA do not have formal Data Sharing Agreements (DSAs) in place with any of these separate agencies.

SPA do not provide data subjects with fair processing information or seek consent to share information with third parties where necessary.

SPA does not have processes in place to ensure that shared data is kept accurate and up to date.

SPA does not seek assurance that shared data is deleted or securely destroyed in line with the agreed retention period.
