Metropolitan Police Service

Data protection audit report

Executive summary
May 2017

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.

The Metropolitan Police Service (MPS) has agreed to a consensual audit by the ICO of its processing of personal data.

An introductory meeting was held on 13 January 2017 with representatives of the MPS to identify and discuss the scope of the audit.

2. Scope of the audit

Following pre-audit discussions with the MPS, 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.

3. Audit opinion

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

The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Limited Assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non- compliance with the DPA.

4. Summary of audit findings

Areas of good practice

The MPS security manual and METSEC code, provides guidance to staff on their personal responsibility for information security. This includes reporting security incidents, access to MPS information, clear desk and security of mobile devices. There is also an Information Management policy for the management, security and control of information assets both electronic and manual.

The Information Assurance Unit (IAU) have responsibility for managing information security incidents, which are escalated to the Deputy Data Protection Officer (DPO) and reported to the ICO where appropriate.

The IAU has an internal audit plan which includes risk based physical security audits of MPS premises and monitoring of emails.

Staff are encouraged to challenge visitors to ensure they have authorised access to police premises. Awareness reminders which include clear desk and clear screen requirements are located in the Empress State Building.

Areas for improvement

The MPS still use Microsoft Windows XP Operating System on some desktop computers and laptops. There is an ongoing project to replace Windows XP as it is no longer supported by Microsoft. Without critical Windows XP security updates there is a residual risk to personal data.

There are currently weaknesses relating to removal of access to MPS applications and buildings once no longer required. The MPS are aware of these risks and are working to replace systems to mitigate the risk of unauthorised access to buildings.

Backup arrangements for file systems are not tested to ensure that they are recoverable in the event of a disaster.

A number of Business Continuity (BC) plans are incomplete or overdue for review. Some had not been tested and do not include how to maintain or recover records in the event of an adverse situation. The database used to store BC information is unsupported and not backed up.

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of the MPS.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.