Parliamentary and Health Ombudsman

Data protection audit report

Executive summary
March 2018

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.

Parliamentary and Health Service Ombudsman (PHSO) has agreed to a consensual audit by the ICO of its processing of personal data.

An introductory meeting was held on 11 January 2018 with representatives of PHSO to identify and discuss the scope of the audit and after subsequently to agree the schedule of interviews.

The audit field work was undertaken at Manchester and London offices, plus the third party storage facility, between 5 and 8 March 2018

2. Scope of the audit

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

Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

Records management (manual) – The processes in place for managing both manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

Where possible, a review of plans to comply with the requirements of the forthcoming GDPR / data protection legislation will also be included within the scope of the audit, with any relevant recommendations made, although this will not count towards the assurance where requirement is new for GDPR.

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 PHSO with an independent assurance of the extent to which PHSO, within the scope of this agreed audit, is complying with the DPA.

Where weaknesses 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 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 based upon the ICO's assessment of the risks involved. PHSO'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 PHSO with an independent assurance of the extent to which PHSO, within the scope of this agreed audit, is complying 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. We have made one limited (Record management) and one reasonable assurance assessment (Governance) where controls could be enhanced to address the issues which are summarised below

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 **4** urgent priority recommendations across both scope areas: **2** in Governance and **2** in Record Management 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 **15** high priority recommendations across both scope areas: **4** in Governance and **11** in Record Management where controls could be enhanced to address the issues identified. Of these **3** recommendations specifically relate to PHSO's readiness for the GDPR.
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 **20** medium priority recommendations both scope areas: **9** in Governance and **11** in Record Management where controls could be enhanced to address the issues identified. Of these **2** recommendations specifically relate to PHSO's readiness for the GDPR.
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 **6** low priority recommendations both scope areas: **0** in Governance and 6 in Record Management area where controls could be enhanced to address the issues identified.

6. Summary of audit findings

Areas of good practice

There are defined management structures in place within PHSO to support their Data Protection agenda, although most roles are very new to post.

Significant work has been done in preparation for the introduction to General Data Protection Regulations in May 2018, including the drafting of a new suite of policies and appointing a Data Protection Officer.

There is an Information and Record Manager in post and PHSO are aiming to move towards a paperless environment as much as possible.

Areas for improvement

There are limited methodical mechanisms in place to provide effective oversight of data protection compliance within PHSO such as comprehensive compliance checks or key performance indicators.

There are some data processors currently in use with no contracts in place (as the contract end date had expired at the time of the audit) which is contrary to principle 7 of the Data Protection Act 1998 and will be non-compliant to the requirements as laid out in Articles 28-36 of the GDPR.

Although there are some changes being made to contracts and third parties responsibilities ahead of GDPR, there are currently no robust processes in place to seek assurances from third party contractors that they are complying with their data protection responsibilities.

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 PHSO.

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.