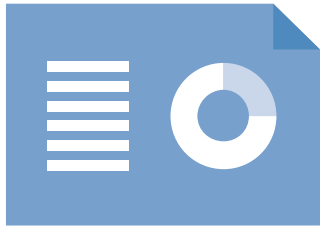
Middlesbrough Council

Data protection audit report

December 2019

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Following a registration of interest made by Middlesbrough Council to the ICO in June 2019 to engage in a consensual audit, the ICO agreed to conduct an audit of its processing of personal data.

The purpose of the audit is to provide the Information Commissioner and Middlesbrough Council with an independent assurance of the extent to which Middlesbrough Council, within the scope of this agreed audit, is complying with data protection legislation.

It was agreed that the audit would focus on the following areas:

Scope Area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.
Security of Personal Data	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Requests for Personal Data & Data Portability	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to or to transfer their personal data.

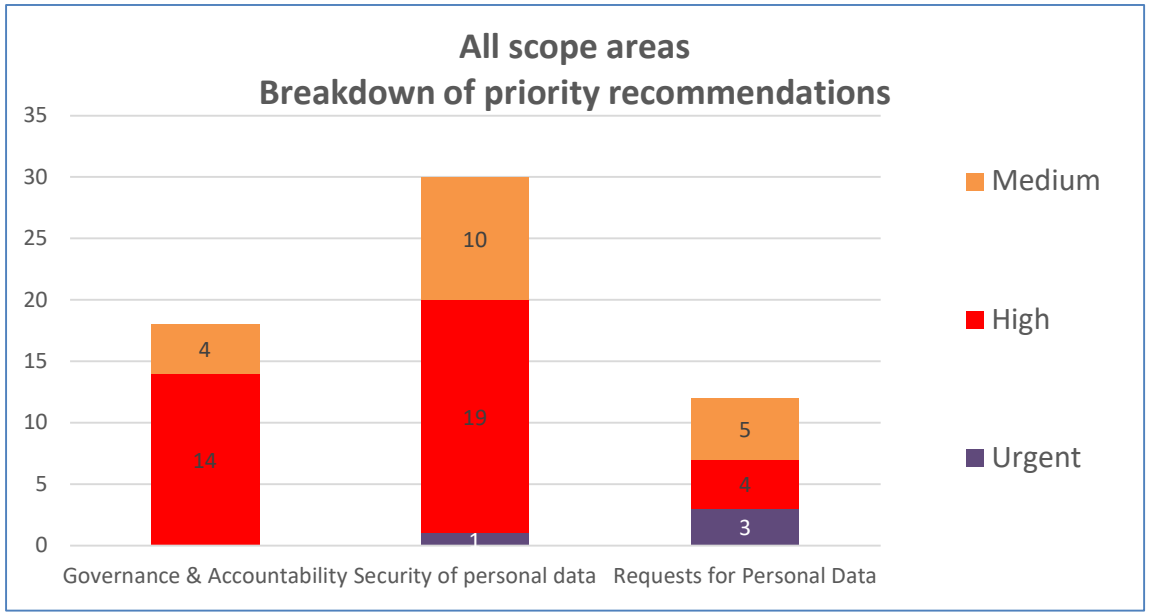
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist Middlesbrough Council in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. Middlesbrough Council's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Security of Personal Data	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Requests for Personal Data & Data Portability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Priority Recommendations



Areas for Improvement

The Council should continue to produce a completed Record of Processing of Activities for each of its service functions.

In public-facing areas where personal data is being provided, the Council should ensure that information about how it processes individuals' personal data (i.e. privacy notices) is made readily available and in an appropriate format. It should also ensure that whenever it is capturing special category personal data, details of individuals' rights in line with data protection legislation are transparent and clear.

The Council should provide specialised data protection training for operational staff teams who encounter higher risks in their practice and/or those with more specialised job functions.

The Council should review the policies and procedures around physical access control.

The Council should extend the practice of periodically reviewing access rights to all case management systems where personal data is being processed.

Periodic checks should be introduced of the access activity to all case management systems where personal data is being processed.

The Council should monitor its compliance with Subject Access Requests (SARs), including introducing Key Performance Indicators (KPIs) in relation to historical SARs, to identify if any additional resources or changes to procedures around SARs need to be considered.

The Council should assess the training requirements of staff responsible for handling SARs and introduce mandatory specialised training for all staff who have a responsibility for processing requests.

Disclaimer

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 Middlesbrough Council.

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.

This report is an exception report and is solely for the use of Middlesbrough Council. The scope areas and controls covered by the audit have been tailored to Middlesbrough Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.