Haringey Council

Data protection audit report

May 2024

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Haringey Council (the Council) agreed to a consensual audit of its data protection practices.

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

The scope areas covered by this audit are determined following a risk-based analysis of the Council's processing of personal data. The scope may take into account any data protection issues or risks which are specific to the Council, identified from ICO intelligence or the Council's own concerns, or any data protection issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of the Council, the nature and extent of the Council's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to the Council.

Following a meeting with the Council on 28 February 2024, it was agreed that the audit would focus on the following areas:

Scope area	Description
Governance and 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 UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Training and Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.
Personal Data Breach Management and Reporting	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate

Audits are 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, remote interviews with selected staff, and a virtual review of evidential documentation.

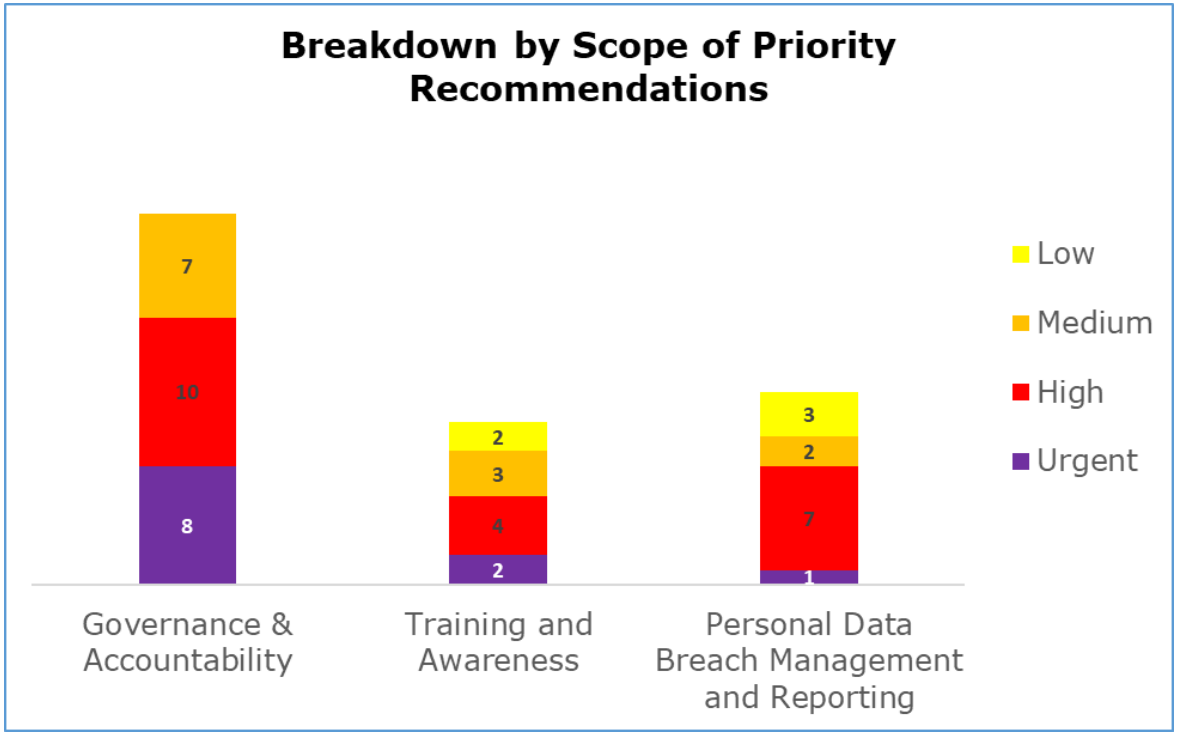
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Council in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. The 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 and 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.
Training and Awareness	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.
Personal Data Breach Management and Reporting	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations



The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has eight urgent, 10 high and seven medium recommendations.
- Training and Awareness has two urgent, four high, three medium and two low priority recommendations.
- Personal Data Breach Management and Reporting has one urgent, seven high, two medium and three low priority recommendations.

Areas for Improvement

Governance and Accountability

- The Council must ensure that there are consistent processes across services that allow them to have oversight and accountability. For example, risk management, DPIA and data minimisation processes.
- The Council must ensure that all third-party processors have an appropriate level of due diligence completed and that all necessary clauses are consistently included in contracts.
- The Council should review the ROPA regularly to ensure it remains accurate and review the use of Public Task as a lawful basis to ensure it is being applied appropriately.

Training and Awareness

- The Council should continue with their plans to implement new mandatory Information Governance (IG) training that is suited specifically to the context of the Council.
- The Council should complete a training needs analysis (TNA). This will ensure that all employees receive necessary IG training and will help with identifying the roles which require specialist DP knowledge.
- Once a TNA is completed, the Council should implement appropriate additional DP training for all staff in specialised roles, that is completed on an appropriate periodic basis.
- The Council must continue with their plans to improve IG training completion rates across the council.

Personal Data Breach Management and Reporting

- The Council must ensure that there are organisational measures, supporting the technical measures already in place, to support the prevention and detection of Personal Data Breaches (PDBs), and monitor compliance with these measures using methods such as dip sampling or audit programmes.

- The Council should reduce the reliance on the IG team to identify and mitigate risks of PDBs as part of the DPIA process. Staff should be confident in their ability to understand risks to personal data as part of their roles.
- The Council must ensure that root cause analysis is completed consistently, and any risks following a breach are being recorded on risk registers as per Council policy. This risk oversight should then feed into monitoring practices and audit programmes to reduce the risk of reoccurrence.

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 Haringey 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 Haringey Council. The scope areas and controls covered by the audit have been tailored to Haringey Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.