Sussex Police

Data protection audit report

October 2023

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 (UKGDPR), 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.

Sussex Police agreed to a consensual audit of its data protection practices. An introductory telephone meeting was held on 26 July 2023 with a representative of Sussex Police to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and Sussex Police with an independent assurance of the extent to which Sussex Police, 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 Sussex Police's processing of personal data. The scope may take into account any data protection issues or risks which are specific to Sussex Police, identified from ICO intelligence or Sussex Police'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 Sussex Police, the nature and extent of Sussex Police's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to Sussex Police.

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

Scope area	Description
Request for Access	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.

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.

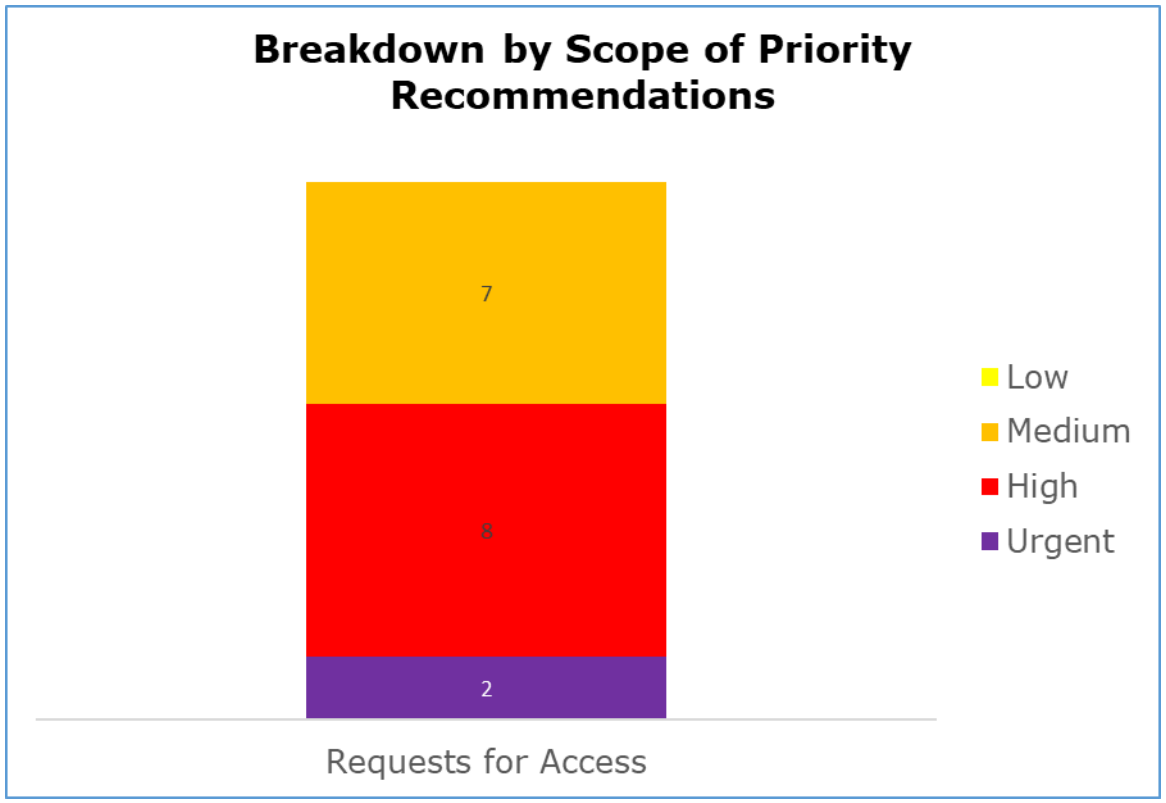
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist Sussex Police in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. Sussex Police'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
Request for Access	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.

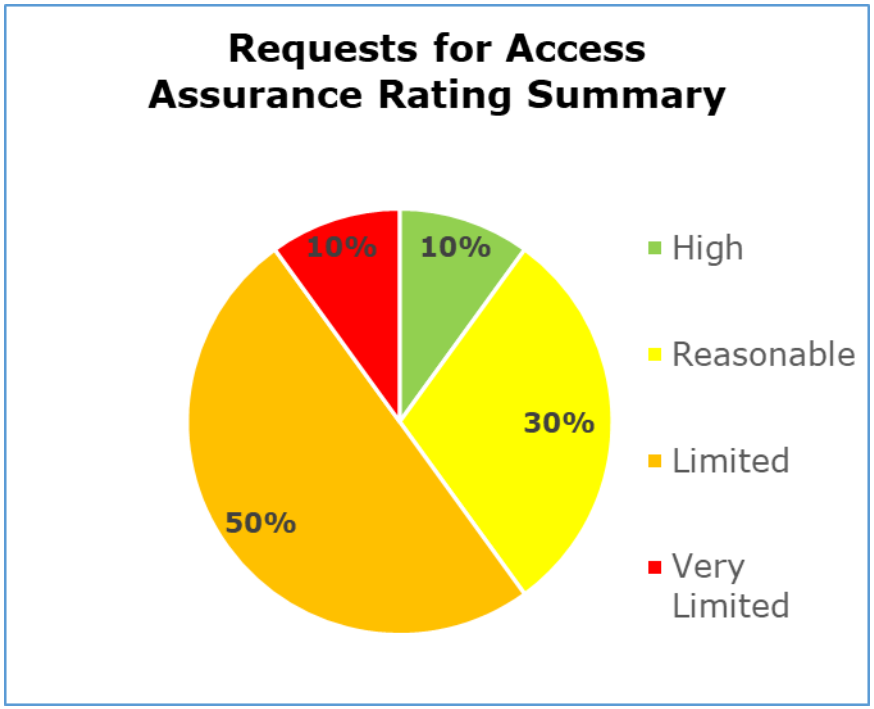
Priority Recommendations



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

- The Request for Access scope has **2** urgent, **8** high and **7** medium priority recommendations.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded. **10%** high assurance, **30%** reasonable assurance, **50%** limited assurance, **10%** very limited assurance.

Areas for Improvement

Sussex Police currently have a backlog of subject access requests which means they are not meeting statutory timescales. Sussex Police should continue to monitor the level of resources it has in place, to ensure it is sufficient to handle incoming requests for access whilst also working through the existing backlog.

Request for access procedures should be improved to sufficiently detail the legislative requirements of Section 53 of the DPA18 and to ensure they reflect requirements of the UKGDPR and of the DPA18 legislation in relation to where extending the timeframe for complex and/or numerous requests would apply.

Sussex Police should formally document the approval process for the removal of personal and third party data that is exempt from disclosure. Furthermore, the documented quality assurance process would ensure a consistent approach to the application of exemptions and the removal of personal and third party data, across the Information Access team.

Sussex Police should carry out cold case reviews on completed requests to ensure that there is a consistent approach being taken across the organisation to exemption and redaction.

There is no dip sampling on completed requests carried out by experienced staff to gain assurances that verification checks are being carried out to safeguard individuals' privacy and to ensure standards in responses remain consistent.

The disclosure information provided to data subjects should explain the searches Sussex Police have undertaken and an overview of what information has been provided as a result of those searches.

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 Sussex Police.

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