Police Service of Northern Ireland

Data protection audit report

August 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 (UK 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 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.

Police Service of Northern Ireland (PSNI) agreed to a consensual audit of its processing of personal data. An introductory telephone meeting was held on 03 March 2023 with representatives of PSNI to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and PSNI with an independent assurance of the extent to which PSNI, 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 PSNI processing of personal data. The scope may take into account any data protection issues or risks which are specific to PSNI, identified from ICO intelligence or PSNI's own concerns, and/or any data protection issues or risks which affect their 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 PSNI, the nature and extent of PSNI's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to PSNI. It was agreed that the audit would focus on the following area(s)

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 with Part 3 of the DPA 2018 are in place and in operation throughout the organisation.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

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, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential documentation.

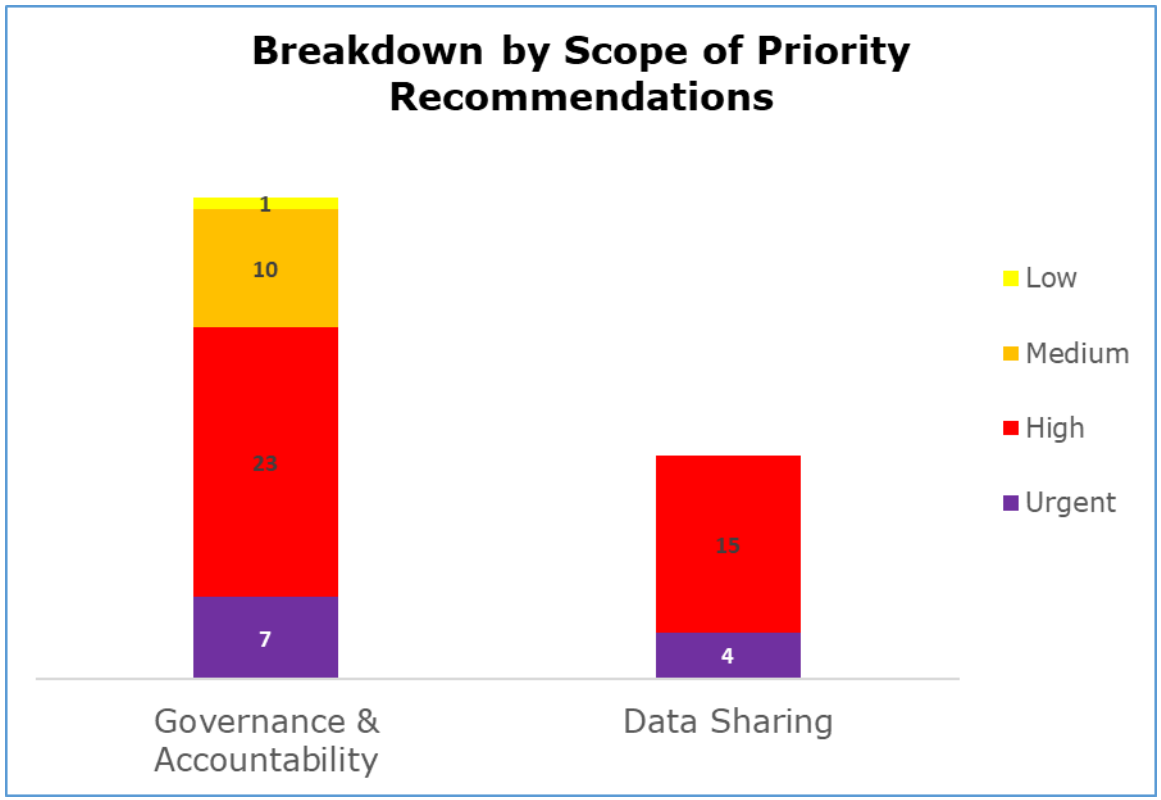
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist PSNI in implementing the recommendations each has been assigned a priority rating based upon the risks that they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

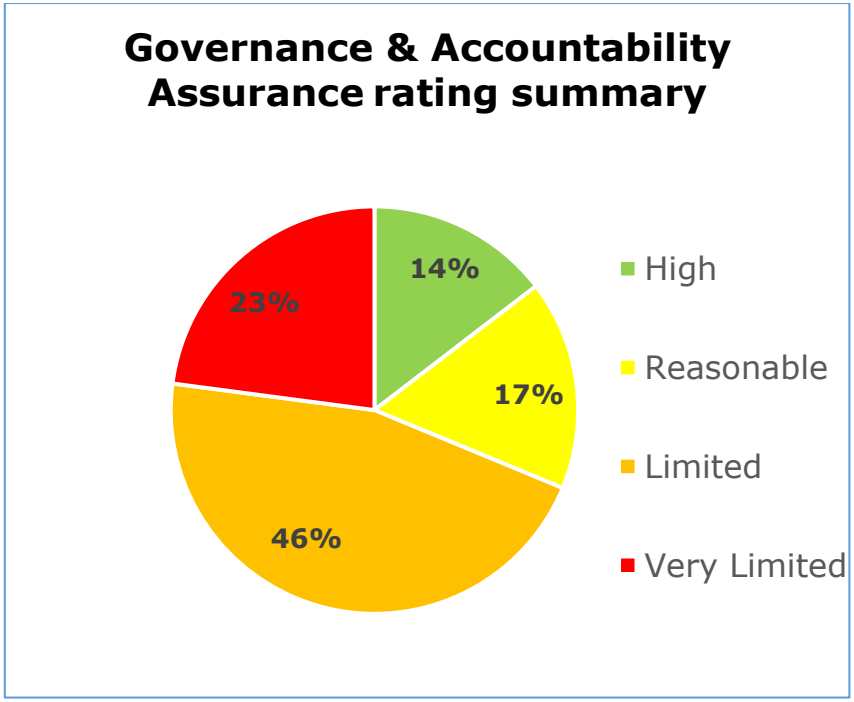
Priority Recommendations



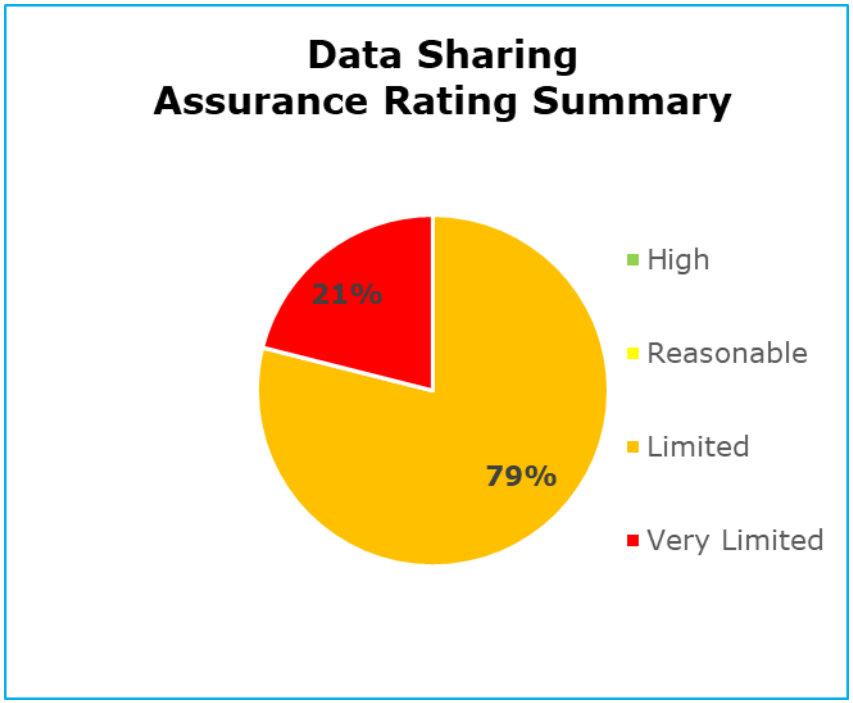
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- The Governance and Accountability scope has **7** urgent, **23** high, **10** medium and **1** low priority recommendations.
- The Data Sharing scope has **4** urgent and **15** high priority recommendations.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. **14%** high assurance, **17%** reasonable assurance, **46%** limited assurance, **23%** very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. **79%** limited assurance, **21%** very limited assurance.

Areas for Improvement

PSNI staff should be made aware of the Information Asset Owner (IAO) handover process to ensure that IAOs are aware of their responsibilities before they take on the role and are fully capable of adhering to the responsibilities including any training necessary.

PSNI's Appropriate Policy Documents (APDs) are not published as required by sections 35 and 42 of the DPA18. The APDs should be made available to members of the public and staff for transparency purposes.

A comprehensive and detailed data mapping exercise should be completed for all information assets and processing activities, to create an overarching record of processing activities (ROPA). The processing activities should be formally reviewed periodically throughout PSNI.

Data Protection Impact Assessment (DPIA) guidance and templates should include details of who has the authority to sign off on risks. This will demonstrate accountability, so staff are able to consult on key decisions made should any issues relating to risks arise in the future and will help to ensure staff are following the correct procedure for sign off.

The roles involved in the data sharing process have not been identified, and a training needs analysis (TNA) exercise to determine necessary training for staff to sufficiently perform their responsibilities has not been completed.

Additionally, an overarching IG training programme should be in place to meet staff training needs. The IG training programme should be approved by senior management and reviewed on a regular basis.

PSNI have not completed their data sharing review to ensure that all routine sharing of personal data, including any existing activities, is identified and a suitable Information Sharing Agreement (ISA) put in place. The ISAs will ensure that routine sharing is as strictly and formally controlled as possible.

The lawful basis for processing personal data and that for sensitive processing, including any condition from Schedule 8 of the DPA18, should be determined and documented for each processing activity in the Information Asset Register (IAR). This includes all processing activities which currently use consent as a lawful basis for law enforcement processing.

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 Police Service of Northern Ireland.

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