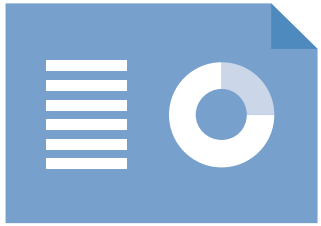
Schengen Information System – UK SIRENE Bureau

Data protection audit report

April 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 119 of the Data Protection Act 2018 (DPA18) contains a provision giving the Information Commissioner power to inspect any personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom.

Article 60 of Council Decision 2007/533/JHA specifies that the ICO shall ensure that an audit of the data processing operations in the UK Schengen Information System (SIS II) is carried out in accordance with international auditing standards at least every four years.

The National Crime Agency (NCA) provides the UK's SIRENE Bureau function, which is responsible for the co-ordination of activities connected to SIS alerts. The NCA agreed to an audit of the UK SIRENE Bureau by the ICO.

The purpose of the audit is to provide the Information Commissioner and the NCA with an independent assurance of the extent to which the UK SIRENE Bureau, within the scope of this agreed audit, is complying with data protection legislation and Council Decision 2007/533/JHA.

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

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

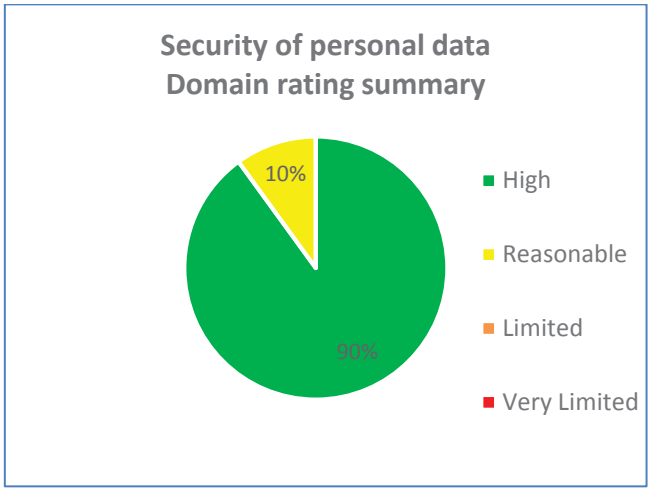
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

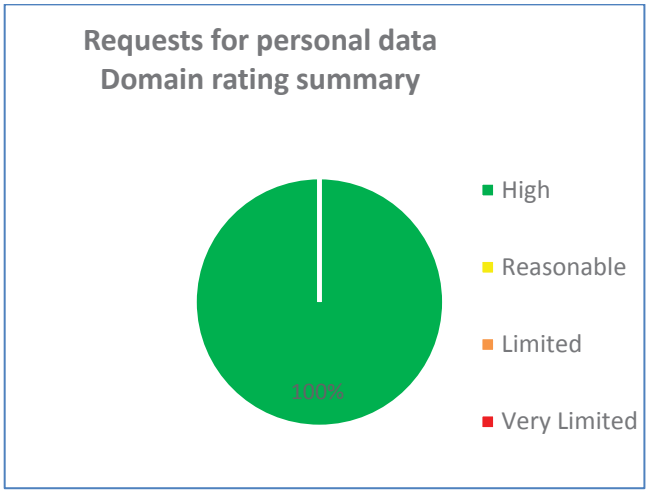
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the NCA and the SIRENE Bureau in implementing the recommendations each has been assigned a priority rating based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

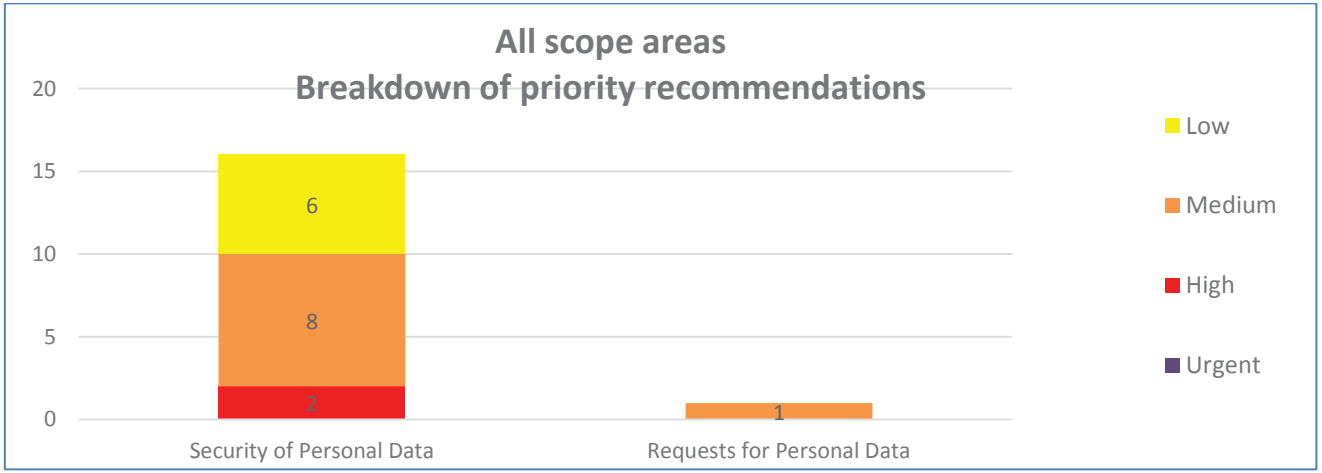
Audit Summary

Audit Scope Area	Assurance Rating	Overall Opinion
Security of personal data	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
Requests for personal data	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.

Graphs and Charts







Areas for Improvement

- Training needs analysis should be undertaken to identify where training is required in relation to data protection and information security. Induction training should be supported by regular refresher training for existing staff. Specialised SAR training for staff involved in handling requests for personal data should also be regularly refreshed.

- Regular physical checks should be undertaken against the hardware inventory to ensure that the inventory is up-to-date and accurate.

- Regular monitoring should be put in place to ensure that security controls, such as the clear desk policy, are operating effectively. Regular physical security risk assessments should be undertaken to allow potential security risks to be identified and addressed appropriately.

- A review of the incident management procedures should be undertaken to identify how local representatives can have greater involvement in the response to incidents and greater oversight of the results of investigations, to allow them greater opportunity to identify localised trends and required improvements to processes and procedures.

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 the NCA.

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