The Home Office

Data protection audit report

March 2022

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 (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.

In December 2020 the Commissioner decided, in line with her Regulatory Action Policy, to undertake a compulsory audit of the Home Office, using her powers under section 146 of the DPA18. This was due to the high volume of personal data breaches reported to the ICO by the Home Office, and the high volume of complaints received regarding Home Office data processing activities. Due to the diversity of processing activities covered by the breaches and complaints, it was identified that an audit would be the most effective way for the Commissioner to gain assurance regarding the Home Office's compliance with data protection legislation.

An Assessment Notice was issued to the Home Office on 18 December 2020. The audit was carried out remotely due to Covid-19 restrictions, using a desk based document review and video conference software to carry out interviews with relevant staff. The audit programme covered the general processing activities of the Home Office, but also specifically looked at processing of personal data carried out by several specifical directorates – Border Force (BF), UK Visas and Immigration (UKVI), Immigration Enforcement (IE), and HM Passport Office (HMPO).

The purpose of the audit was to provide the Information Commissioner with an assurance of the extent to which the Home Office, within the scope of the audit, is complying with data protection legislation.

The audit controls against which the Home Office has been assessed have been determined based on the requirements of data protection legislation and ICO guidance regarding the implementation of the legislation. Where auditors were unable to confirm that a control was in place, a non-conformance has been written outlining the nature of the issue, and a recommendation has been included on what steps the Home Office should take to bring themselves into compliance. Auditors have also offered observations throughout this report, on issues where the Home Office is in compliance with the audit controls but where there is an opportunity for improvement.

Audit Scope

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

Scope area	Description
Governance	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UKGDPR and national data protection legislation are in place and in operation throughout the organisation.
Information Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Personal Data Breach Management	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
Records Management	The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.
Information Risk Management	The organisation has applied a "privacy by design" approach. Information risks are managed throughout the organisation in a structured way so that management understands the business impact of personal data related risks and manages them effectively to assure the business of the organisation.
Project Management and DPIAs	
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.

Audit Summary

The Home Office is responsible, across all its business areas and directorates, for processing a huge quantity of data. The types of data processing that the audit team either witnessed, read about, or were informed of during the course of the audit are so varied, and in some cases so complex, that it is impossible to provide here a brief summary of how the Home Office process personal data. In the context of this varied and complex data processing, auditors were encouraged to see that the Home Office have taken a proactive approach to developing their compliance with Data Protection legislation over the last several years, which has resulted in general compliance with many of the legislative requirements that were reviewed during the audit, in particular for data breach management.

Out of 76 audit controls, across 8 scope areas, 30.1% of controls were fully met, with no risk of noncompliance identified, and so received no recommendation as a result of the audit. In contrast, only 27.6% of controls were given Urgent recommendations which has provided assurance that, whilst there are areas where the Home Office does not currently comply with the requirements of Data Protection legislation, there is a broad level of fundamental compliance across many areas of processing.

Priority Recommendations

Where opportunities for improvement were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Home Office 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 Home Office's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

The priority ratings assigned by the ICO can be interpreted using the following key:

Urgent – An urgent recommendation relates either to a clear breach of a data protection legislation, or to an imminent risk of a personal data breach occurring if the issue is not resolved.

High – A high recommendation relates to the serious likelihood of a breach of the legislation or a personal data breach occurring if the issue is not resolved.

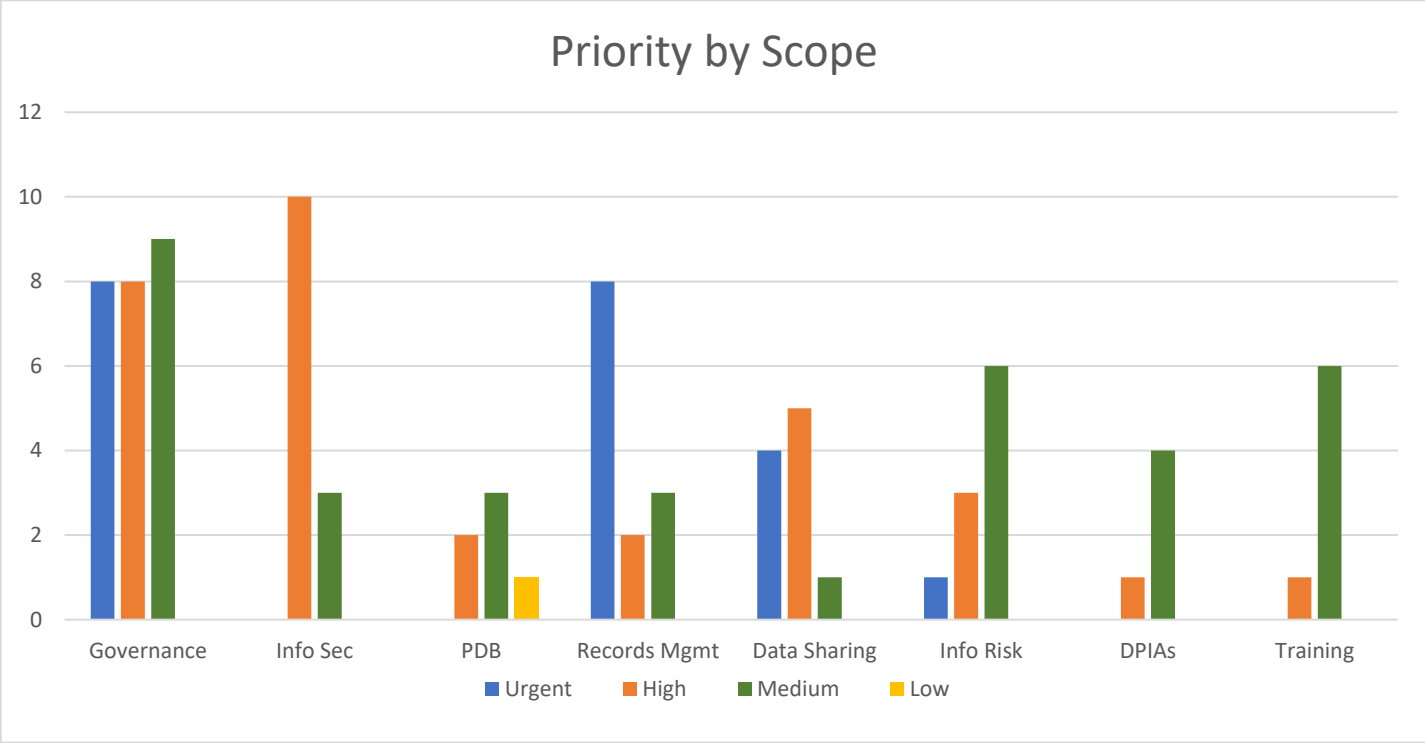
Medium – A medium recommendation relates to the realistic possibility of a breach of the legislation or a personal data breach occurring if the issue is not resolved.

Low – A low recommendation relates to the potential for a breach of the legislation or a personal data breach to occur if the issue is not resolved.

The severity of any potential consequent personal data breach is also factored into consideration when assigning a priority rating.

When developing an action plan for implementing the findings of this audit, the Home Office will be expected to determine delivery schedules justified against both the ICO's priority rating and the Home Office's own risk appetite.

A summary of the ratings assigned within this Report is shown below.



Areas for Improvement

The following is a summary of the key areas for improvement that were identified during the audit. The ICO has made detailed recommendations to assist the Home Office to take action to address these areas.

- The Home Office Record of Processing Activity (RoPA) is not sufficiently detailed to be fully compliant with the requirements of Article 30 of the UKGDPR and Section 61 of DPA18.

- Data mapping being carried out by the Home Office is not yet complete; there is no detailed record of end-to-end processing across all business areas and, in some areas of the Home Office, historical assets have not yet been fully mapped.

- The Home Office Information Asset Register (IAR) does not contain all of the necessary information to provide assurance that the Home Office's processing of personal data is in compliance with the requirements of the legislation, including the proper identification of lawful bases under Articles 6 and 9 of the UKGDPR, and risk assessment of the information assets in line with Articles 5(1)(f) and 24.

- The Home Office could not provide assurance that it is meeting its obligations, under Section 62 of DPA18, to maintain appropriate logs of the use of automated processing systems.

- The Office of the Data Protection Officer (ODPO) does not have sufficient resources to effectively manage all of the work that requires their input. In addition, they are not the only point of contact for IG/ data protection queries and sometimes, as a result, conflicting guidance is provided.

- The Home Office information security policy framework has been historically fragmented and is currently undergoing a comprehensive review and redevelopment to address this area of concern.

- The organisational framework for records management is not sufficient to meet the requirements of the organisation, nor is it consistently applied across the breadth of the Home Office, which may prevent the Home Office from demonstrating compliance with Articles 5(2) and 24 of the UKGPDR.

- There are a large amount of unrecorded and unstructured data and assets in place across the Home Office as a result of historical records management practices, which is being processed in breach of Article 5 of the UKGDPR.

- Retention of data is not being managed in line with the requirements of Article 5(1)(e) of UKGDPR and the Public Records Act, and it was identified that there is an inconsistent approach to retention across the organisation.

- Home Office Privacy Information Notices (PINs) are inconsistent. Some do not provide enough detail on the rights of the individual or set out clearly what they are and how they apply. The visibility of PINS on the website varies between directorates and some are not available in alternative formats or languages.

- There is a heavy reliance on the lawful basis of public task, Article 6(1)(e), and there is a lack of documentation regarding the supporting legislation or relevant common law powers related to this processing.

- In some circumstances where consent is recorded as the lawful basis for processing, the Home Office was unable to provide assurances that the consent was fully compliant with the requirements of Article 7 of the UKGDPR.

- Special category data and criminal offence data are, in some areas of the Home Office, being processed with no lawful basis having been properly documented, contrary to the requirements of Articles 5(2), 9, and 10 of the UKGDPR.

- The Home Office does not carry out a sufficiently granular review of proposed data sharing to ensure that the correct lawful basis is identified to support to sharing of personal data, and in some instances the documentation surrounding sharing arrangements does not record the lawful basis being relied upon.

- The governance of data sharing activities is fragmented, risking a lack of oversight by staff with relevant expertise, and in some cases preventing effective ongoing review and updating of sharing agreements.

- There is no guidance available to inform staff specifically relating to the requirements of international data sharing which means there is a risk of data sharing taking place that is not compliant with legislation, with the only currently available guidance being high level, as part of the general Data Sharing MoU Guidance.

- There is no requirement for the International data sharing team to be informed of all international data sharing activity which means that a central log of sharing activity is incomplete, and oversight of this function cannot be obtained. Without oversight there is no assurance that international data sharing is taking place in a compliant and consistent manner.

Areas of Best Practice

- During the audit the Home Office was found to have a very extensive network of Data Protection specialists embedded throughout all areas of the organisation. At a tactical level, Data Protection Practitioners have proven to be very effective at improving awareness and compliance with various aspects of data protection, such as managing personal data breaches and carrying out data protection impact assessments. These Practitioners are supported, at an operational level, by Data Protection Implementation Leads and Information Asset Owners, who are responsible for managing information risks and driving cultural change. At the centre of the department, there are numerous subject matter expert teams in place to design policy and compliance initiatives that enable the business and this is governed by an effective Data Board with under-pinning DP governance forums.

- The Home Office has also developed a wide-reaching data protection awareness and education programme aimed at all staff and suitable for varying proficiency levels. The foundations of which were built by the ODPO, who developed a suite of eLearning products plus a programme of Masterclasses, which are focused on helping participants develop their knowledge of specific subjects, including personal data breach management, data protection impact assessments, and privacy information notices. In parallel, a cross-functional team coordinated delivery of an inaugural Data and Information Week in January 2021, which contained 20+ sessions with 1,500+ people attending. This departmental initiative has proved popular, helping to spread knowledge and expertise in data protection issues across the Home Office.

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 Home Office.

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