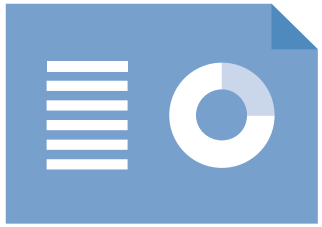
Organisation Name

Artificial Intelligence (AI) Data Protection Audit Report

Date

Executive summary



Background & Scope

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. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

[Detail of circumstances that led to the audit (post May 2018 this may include whether the audit is consensual).]

The ICO recognises that Artificial Intelligence (AI) offers opportunities that could bring marked improvements for society. But shifting the processing of personal data to these complex and sometimes opaque systems comes with inherent risks. The purpose of the audit is to provide the Information Commissioner and <name> with an independent assurance of the extent to which the AI system, 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 <name> processing of personal data within the AI system. The ICO has further tailored the controls in scope to take into account the organisational structure of <name>, the nature and extent of <name's> processing of personal data within the AI system and whether <name> is the developer, is providing AI as a service, or has procured the system for use in their organisation. As such, the scope of this audit is unique to <name>.

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

List in bullet format all areas / domains covered in the audit

- *A:*
- *B:*
- *C:*

<<Include for onsite audit: 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, on-site visits including interviews with selected staff, and an inspection of selected records.

<<Include for remote audit: 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.

<<Include for hybrid audit: 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 to promote compliance with data protection legislation. In order to assist <name> 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. <name> priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Overview of System and Data Processing

Insert:

- an overview of the service / system;
- a summary of the organisation's structure;
- the type and nature of data being processed; and
- the data and user journey e.g. key systems, data sharing, data processors, user terms and conditions etc

Audit Summary

INSERT TABLE FROM 'GRAPHS & CHARTS' TAB

Graphs and Charts

INSERT RELEVANT CHARTS AND GRAPHS FROM 'GRAPHS & CHARTS' TAB.

Areas for Improvement

Insert short summary of key themes that have been identified during the audit where opportunities for improvement have been acknowledged (could be based on Closing Meeting feedback).

Best Practice (*optional)

Where applicable, insert short summary of any best practice (above control measure benchmark) that has been identified during the audit. If no good practice identified, delete section title.

Detailed Findings

Scope area: A. xxxxxxxx

Findings:

Copy and paste the findings text from the working paper directly here. Ensure there is appropriate spacing / paragraphs to break up long sections of text, or different findings.

Example:
The Privacy and Accountability Framework introduces a requirement for product leads to use a Request For Comments (RFC) template, which is shared and managed online, at the project initiation stage and this is complemented by documented policies, while ongoing product development is managed through the Product Release Process. Once a product is live the 'Product Counselling Role' ensures that product variations are reflected in any necessary contract variation.

xxx demonstrated an external facing sub processor list which they feels forms the basis of a RoPA and this is mirrored with an internal version for management of change and Business Processing Operations (BPO) onboarding. There is also a data mapping process demonstrating where processing takes place and where xxx, clients and BPO's sit in that network.

xxx demonstrated multiple channels of communication around a specific project with a clear version control, editing and product history management process with updates and messaging through online project management tools and necessary approval points by the privacy lead. External product updates are communicated through various means, including through contract amendments, product marketing material, customer communications and the public facing developer pages in a clear and navigable dashboard interface.

Advisory notes: insert any advisory notes, observations or links to relevant guidance here

Recommendations:

Insert the relevant report table (or section from the report table) from the Report tab in the working paper here.

Example:

Control measures	Non Conformities	Recommendations	Priority

Change management processes are documented in policy to ensure that new versions or change releases to AI systems are managed effectively by all parties	*nfvo inbwfp iowbnf*	*dvbn owb ow*	*Urgent*
There is a process of communication within the change management process so that all parties understand the impacts of the change(s) and are able to reassess any potential privacy implications	*dnbc owowbonwdbwd wd kjwbd nivhwuoihvwuv iuhvwiubvhweouhro iuhv woeruhv wo o*	*cdbiwudhbgcou hwouwdhuo uoehvcouewhv oow weouihv ohwo*	*High*

Scope area: B. xxxxxxxx

Findings:

Advisory notes: insert any advisory notes, observations or links to relevant guidance here

Recommendations:

Scope area: C. xxxxxxxx

Findings:

Advisory notes: insert any advisory notes, observations or links to relevant guidance here

Recommendations:

Scope area: D. xxxxxxxx

Findings:

Advisory notes: insert any advisory notes, observations or links to relevant guidance here

Recommendations:

Appendix One – Data Flow Diagrams

Insert any relevant evidence, diagrams, screen shots or photographs.

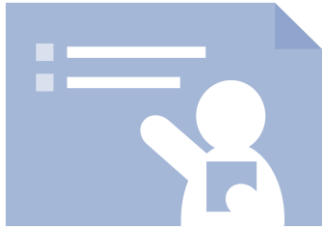
Appendix Two – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations - These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations - These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.

Low Priority Recommendations –

These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Credits



ICO Audit Team

ICO Team Manager - name
ICO Engagement Lead Auditor – name
ICO Lead Auditor - name

Thanks

The ICO would like to thank name and job title of contact for their help in the audit engagement.

Distribution List

This report is for the attention of names and job titles (to incl. point of contact and individual who signed LoE as a minimum).

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the engagement 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 <name>.

We take all reasonable care to ensure that our 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 solely for the use of<name>. The scope areas and controls covered have been tailored to this engagement and, as a result, the report is not intended to be used in comparison with other ICO reports.