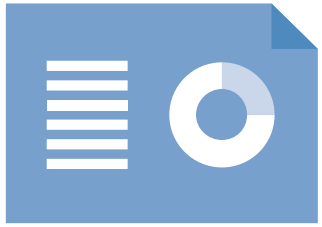
MeVitae

Artificial Intelligence (AI) Data Protection Audit Report

November 2021

Information Commissioner's Office

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.

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 MeVitae 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 MeVitae processing of personal data within the AI system, focusing principally on MeVitae's Blind Recruiting product. The ICO has further tailored the controls in scope to take into account the organisational structure of MeVitae, the nature and extent of MeVitae's processing of personal data within the AI system and whether MeVitae 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 MeVitae.

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

- A: Governance
- B: Transparency
- C: Lawful Basis
- D: Contracts and 3rd Parties
- E: Data Minimisation

- F: Individual Rights
- G: Staff Training
- H: DP Risk Management
- I: Security and Integrity
- J: Trade Offs
- K: Statistical Accuracy
- L: Discrimination and Bias
- M: Human Review

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

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore MeVitae agreed to conduct the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 25 October to 27 October. The ICO would like to thank MeVitae for its flexibility and commitment to the audit during difficult and challenging circumstances.

Where weaknesses were identified recommendations have been made to promote compliance with data protection legislation. In order to assist MeVitae 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. MeVitae priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Overview of System and Data Processing

MeVitae were founded in 2014 with the aim of developing artificial intelligence tools to mitigate bias and discrimination from the hiring process. Their principle product, Blind Recruiting, is advertised as removing more than 22 potential points of bias from a CV, cover letter, or application form, such as age, gender, location, nationality etc, with the client being able to preselect which data points will be redacted. This tool is designed to integrate seamlessly with their client's applicant tracking system, and as such MeVitae operate as data processors for their clients. Blind Recruiting operates by identifying and removing information that might lead to bias or discrimination by the hiring manager – the submitted CV, cover letter, or application form is processed by the system and a new version is created with those data points removed. A copy of the altered application is provided automatically to both the client and the data subject, and the client can access an unredacted version of the application at any time if the data subject raises any concerns. The tool is marketed towards organisations with over 1000 staff, and can fully anonymise 600 applications in 6 seconds.

MeVitae do not retain data processed via Blind Recruiting for more than 72 hours unless there are any issues with an individual application not being correctly anonymised that require the data to be retained for longer, and they do not use it for any purposes other than providing the services for which the tool is contracted. No data gathered via the tool is processed for the purposes of training their machine learning models.

As a standard requirement of their client contracts, MeVitae require their clients to be transparent that job applications will be processed via MeVitae's software, and also place responsibility on their clients for providing the appropriate level of human review and an initial point of contact for job applicants with questions or problems. MeVitae are also clear that their software does not make any decisions, and simply provides information to their clients for human decision makers to act on.

Training data is collected via web scraping – identifying and gathering CVs that have been uploaded and made public by individuals around the world. This does not include gathering any information from social media such as LinkedIn, instead looking for instances where individuals have made public their whole CV as a clear document.

Audit Summary

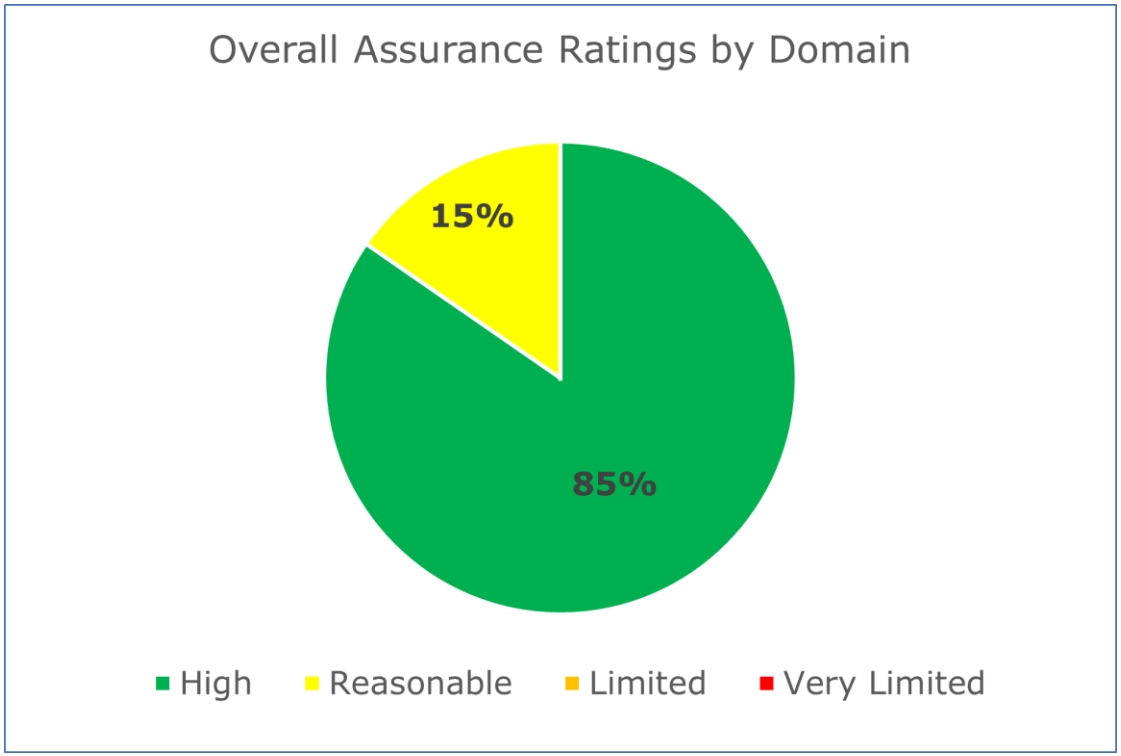
Domain	Assurance Rating	Overall Opinion
Governance	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
Transparency	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Lawful Basis	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.
Contracts & 3rd Parties	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.

Domain	Assurance Rating	Overall Opinion
Data minimisation	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.
Individual Rights	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.
Staff Training	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
DP Risk Management	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.
Security & Integrity	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.

Domain	Assurance Rating	Overall Opinion
Trade Offs	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.
Statistical Accuracy	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.
Discrimination & Bias	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.
Human Review	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.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Graphs and Charts



The above graph shows a breakdown of the overall percentages for Assurance Ratings across all domains covered by this audit.

Overall Number of Recommendations per Priority Ratings	
Urgent	0
High	6

Medium	4
Low	1

Areas for Improvement

- MeVitae should continue to work towards implementing their planned training programme for all staff.
- MeVitae should review their approach to DPIAs in line with ICO guidance.