

Audit and Risk Committee – for assurance

Meeting agenda title: ICO Data Protection Compliance

Meeting date: 20 June 2022

Time required: 5 minutes

Presenter: Louise Byers

Approved by: Louise Byers

1. Objective and recommendation

- 1.1. The purpose of this report is to provide the Committee with assurance regarding the ICO's compliance with the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulation 2003 (PECR).
- 1.2. The recommendation of the report is that the Chair of the Audit and Risk Committee provides assurance to DCMS, via the ALB Audit Chairs letter (on the agenda for this meeting), that the ICO is 'working towards compliance to the data protection act and is following the ICO's accountability framework or similar tool...' and we are also 'working towards our websites and mobile applications being compliant to DPA and PECR, with regards to cookie banner, setting and policy pages and data protection privacy notices.' This wording is the standard wording from the letter template.

2. History and dependencies

- 2.1. The Committee has previously received reports relating to the ICO's compliance with information rights law on 26 April 2021 where an [internal audit report on Information Governance](#) was presented to the Committee. The internal audit found substantial assurance around the effectiveness of the ICO's control framework.

3. Developing a common understanding

- 3.1. Data protection law places specific obligations on organisations, such as responding to individual rights requests, conducting impact assessments and establishing appropriate contractual terms. Additionally, organisations are required to be accountable for their compliance, which can be evidenced through record keeping, appropriate governance frameworks and staff training.

4. Matters to consider to achieve objective

- 4.1. We have a robust governance framework in place to monitor and oversee compliance with information rights law. This includes specific governance forums such as the Information Risk Governance Group, which reports to the Risk and Governance Board, which is responsible for overseeing our compliance with information rights law. We also have senior responsible individuals, such as a Data Protection Officer (DPO) and a Senior Information Risk Officer (SIRO).
- 4.2. To support this governance structure, across the ICO there is a network of Lead Information Management Officers (LIMOs) and Information Asset Owners (IAOs). This network has a responsibility to ensure information assets are held in compliance with the law. This work is coordinated and supported by a dedicated Information Management Team.
- 4.3. We also have a Information Access Team and Information Security Team who work with the Information Management Team to provide a holistic and expert advice and support service for the management of information across the ICO. The teams also fulfil statutory compliance functions, such as the management of personal data breaches and responding to individual requests for information under both the DPA and Freedom of Information Act (FOI).
- 4.4. We have a suite of processes and policies embedded across the ICO to facilitate compliance with information rights law, including Data Protection Impact Assessments (DPIAs), Records of Processing Activity and incident reporting processes.
- 4.5. We have a programme of work to ensure that we are compliant across all information rights legislation which is included in our business plans. This is complemented by assurance work from the Internal Assurance and Compliance Manager.
- 4.6. We are following the ICO's accountability framework and this forms the basis of our information governance work. The accountability framework was produced by the ICO as a regulatory tool to allow organisations to demonstrate accountability and compliance. We have undertaken a review of the implementation of the ICO's accountability framework, and have identified that we are following the recommended approach in the framework. The audit has identified some areas where further work is needed and this is

being undertaken by our information governance teams working with the relevant departments. As a percentage, we have assessed that only 2% of the requirements of the current framework are not being met currently. These do not relate to explicit legislative requirements and instead mainly relates to good or best practice activities, such as conducting user testing of privacy information. In these areas, action plans are in place or are under development.

- 4.7. We regularly review and amend our approach to our online services to ensure compliance with PECR. We have a full cookie notice on our website, as well as a comprehensive privacy notice. We conduct DPIAs to assess impact and risk and use our internal resources and expertise to support this work.

5. Areas for challenge

- 5.1. Does the Committee require any additional assurance on any of data protection or PECR compliance?

6. Communications considerations

- 6.1. There is no need for broader communication of this work at this stage.

7. Next steps

- 7.1. The next steps for this work are:
 - Continue to monitor compliance through our governance structures, specialist teams and network of LIMOs and IAOs.
 - Develop and deliver a risk-based programme of compliance and assurance checks.

Author: Aimee Smith

Consultees: Iman El Mehdawy, Jo Butler

Publication decision: This report can be published internally and externally without redactions.

Outcome reached: