Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Darren Tierney
Director General – Propriety and Ethics
Cabinet Office
70 Whitehall
London
SW1A 2AS

Our reference: ICO/O/ED/L/COR/0295
By email

19 July 2021

Dear Darren,

RE: ICO audit of Cabinet Office FOI Clearing House

At our meeting on 11 June, we discussed the benefits of an audit of the Clearing House functions run by the Cabinet Office. Unlike our powers under Data Protection (DP) legislation, an audit covering Freedom of Information (FOI) matters can only be conducted on a consensual basis. I am therefore writing formally to request Cabinet Office's consent for this work to begin.

Benefits of an audit

As we discussed, an audit along the lines set out below would be an opportunity for the Cabinet Office to get an independent view of the Clearing House's practices and the extent to which they are compliant with DP and FOI legislation. Where issues or weaknesses are identified, you would receive tailored recommendations to improve compliance.

In addition, by allowing an independent regulator to examine the Clearing House's processes and procedures the Cabinet Office can be seen to be submitting themselves to external scrutiny. We will also publish an executive summary report, providing greater transparency to those who make FOI requests to central government departments and to the wider public.

Since our meeting in June, I am aware that the Public Administration and Constitutional Affairs Select Committee has announced an inquiry into the role of the Clearing House[1]. Our audit report could also provide valuable evidence to that process.

[1] https://committees.parliament.uk/work/1348/the-cabinet-office-freedom-of-information-clearing-house/

Scope of the audit

We agreed when we met that my team would share some initial thinking on how the proposed audit could work, in case there were any clarifications needed before I wrote to you formally. Following that sharing of initial thinking on 24 June, no such questions have been raised from your side and I hope that we can therefore agree the next steps relatively quickly. This will ensure that the findings from any audit can inform parliamentary committee's work.

In terms of scope, the audit would cover aspects of both DP and FOI. As the Clearing House is not a public authority in its own right, but rather a function within the Cabinet Office as public authority, our standard audit toolkit is not a perfect fit. We do however want to ensure the best possible scrutiny model, so we will create a bespoke audit scope – this is most likely to entail something that is closer to a process audit incorporating controls from a number of our standard toolkits. At this stage, we would anticipate covering aspects of our Governance & Accountability, Records Management, Security of Personal Data, Information Sharing, and Training & Awareness toolkits. I have set out some initial guidelines on areas of coverage in an annex to this letter.

As a consensual audit under the FOI legislation, the precise final scope can be discussed and agreed in advance with your team as part of the next steps. Similarly, our teams can agree the practicalities of conducting the audit in light of the social distancing and workplace guidelines that are in place when it happens. I hope we can find a scope that allows for an audit that ensures the public's confidence in its rigour.

In terms of timings, given the launch of the parliamentary inquiry, I hope that we can begin work on the audit relatively quickly. The audit itself would involve, as per standard practice on our more regular data protection audits, the provision of documentary evidence, such as policy documents, in advance of a week of interviews with key staff.

I hope that is helpful in terms of setting the scene and that it will allow you to take things forward internally. If you require anything further, please do not hesitate to contact me. I would be happy to arrange a call with representatives of our Regulatory Assurance audit team if that would assist.

Yours sincerely,

Elizabeth Denham CBE
UK Information Commissioner

Annex – summary of areas of focus in an ICO audit

Governance & Accountability
Scope: 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.
Risk: Without robust governance and accountability processes for evaluating the effectiveness of information governance policies and procedures there is a risk that personal data may not be processed in compliance with the regulations resulting in regulatory action and/or reputational damage.
Domains Include: • Management Structures • Policies and Procedures • Training • Data Protection Compliance & Assurance • Data Processor Contracts • Record(s) of Processing Activities • Lawful Basis • Transparency • Data Protection by Design and Default • Data Protection Impact Assessments • Personal Data Breaches

Records Management
Scope: 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.
Risk: In the absence of appropriate Records Management processes, there is a risk that records may not be processed in compliance with the UKGDPR and other national data protection legislation, resulting in regulatory action by the Information Commissioner's Office, reputational damage to the data controller and/or damage and distress to individuals.
Domains Include: • RM Organisation • Collection of Data • Creation of Records • Governance of Records Management • Access to Physical Records • Access to Electronic Records • Retrieval of Physical Records • Maintenance and Accuracy of Records • Retention of Physical and Electronic Records • Disposal of Electronic Records

- Disposal of Physical Records
- 3rd Party Disposal
- Right to be Forgotten

Information Security
Scope: There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Risk: Without appropriate measures there is a risk of non-compliance with the UKGDPR and other national data protection legislation. This may result in damage and/or distress for individuals who are the subject of the data, and reputational damage for the organisation as a consequence of this and any regulatory action taken by the Information Commissioner.
Domains Included: • Organisation of Information Security • Mobile and Remote Working • Asset Management • Removeable Media • Access Control • Physical Security • Operations Security • IT Supplier Relationships • Incident Management • Business Continuity Management • Compliance

Data Sharing
Scope: The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.
Risk: The failure to design and operate appropriate data sharing controls is likely to contravene the principles of data protection legislation, which may result in regulatory action, reputational damage to the organisation and damage or distress for those individuals who are the subject of the data.
Domains Included: • Informed Decision Making • Fair Processing Information • Assessing the Legality, Risks and Benefits (DPIAs) • Information Sharing Agreements and Logs • Data Adequacy, Quality and Retention • Security • Disclosures • Bulk Transfers of Personal Data

Training and Awareness
Scope: 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.
Risk: If staff do not receive appropriate training, in accordance with their role, there is a risk that personal data will not be processed in accordance with the UKGDPR and other national data protection legislation resulting in regulatory action and/or reputational damage to the organisation.
Domains Included: • Training Programme • Induction Training • Refresher Training • Specialised Training • Follow-up • Monitoring and Reporting • Staff Awareness