ICO Corporate Affairs policy

Communicating audits
- compulsory (under an Assessment Notice) and consensual

1 Introduction

This policy is aimed at ICO staff. It provides a set of internal guidelines for communicating our audit activities generally, reflecting our Assessment Notices Code of Practice, Audit: Guide to ICO privacy and electronic communications regulations audits and our Corporate Plan.

2 General communication principles

2.1 Publicity for data protection and freedom of information issues is a valuable means of educating audiences and raising awareness of rights and obligations. The ICO aims to get publicity, such as media coverage, for its activities, and the default position is to be transparent and open about our work. The default assumption is therefore that wherever possible we will communicate our audit activities. However, this has to be balanced with the need to secure the cooperation of data controllers with consensual audits which may require us to limit our communications.

2.2 The Good Practice department will keep other parts of the ICO (eg Corporate Affairs, Enforcement, Strategic Liaison, Policy Delivery and Complaint Handling) informed of audit activities in advance of the event and will work together to plan the

communications treatment. Audits will necessitate liaison with relevant departments who will work together and keep each other informed. This allows the opportunity to identify issues likely to be of significant external interest and for communications to be developed. For example, if an audit identifies issues with guidance notes then one of the outcomes of the audit may be that guidance notices are reworked.

3 Communicating audit activities

3.1 Obligations for compulsory audits: Assessment Notices in accordance with our Code of Practice PECR Compulsory Audits in accordance with our Guide to ICO privacy and electronic communications regulations audits.

- The Assessment Notices Code of Practice and the Guide to ICO privacy and electronic communications regulations audits will be made publicly available via the Information Commissioner's website (Assessment Notices Code of Practice section 2.4, Guide to ICO privacy and electronic communications regulations audits section 2.3).
- Details of Assessment Notices and compulsory Letters of Engagement for compulsory audits under the privacy and electronic communications regulations will be published on the Information Commissioner's website (Assessment Notices Code of Practice section 3.1, Guide to ICO privacy and electronic communications regulations audits section 1.5).
- Details of cancellations of Assessment Notices will be published on the Information Commissioner's website (Assessment Notices Code of Practice section 3.3).

- An Executive Summary report will be produced by the ICO for publication (Assessment Notices Code of Practice section 5.1, Guide to ICO privacy and electronic communications regulations audits section 2.3). While the data controller will be given the option to comment on the report before publication, they cannot prevent the ICO from publishing it (the ICO will, however, listen to representations regarding security, confidentiality etc).
- Basic details of the audit and the Executive Summary report will be made available on the Information Commissioner's website for a year. They may also be available on request afterwards, and will be considered on a case by case basis for release under a freedom of information request. (Assessment Notices Code of Practice section 5.2, Guide to ICO privacy and electronic communications regulations audits section 2.3).
- If the data controller has made a formal response to the report, the ICO will provide, on request, a link from the relevant part of the ICO website to the data controller's website (Assessment Notices Code of Practice section 5.2, Guide to ICO privacy and electronic communications regulations audits section 2.3).
- The Commissioner may make general references to assessments and the conclusions drawn from them in his annual or other reports (Assessment Notices Code of Practice section 5.2, Guide to ICO privacy and electronic communications regulations audits section 2.3).

3.2 Obligations for consensual audits – in accordance with our Code of Practice

- We will not proactively publish any details of any consensual audit before completion of the report (Assessment Notices Code of Practice, Appendix A, section 3, Guide to ICO privacy

and electronic communications regulations audits, Appendix B section 5.4).

- The ICO will produce a full audit report and an Executive Summary. The ICO will expect to publish the Executive Summary on our website and will encourage the data controller to allow us to do so. However, in contrast to compulsory audits, the data controller can prevent the ICO from publishing the report. In these cases, we will put a note on the ICO website saying that the data controller asked us not to publish it (Assessment Notices Code of Practice, Appendix A, section 3, Guide to ICO privacy and electronic communications regulations audits section 2.3). The reports – full and summary - will still be subject to case by case consideration if requested under the Freedom of Information Act.
    - Details of consensual audits and Executive Summaries of consensual audit reports will be available on our website for one year after publication. The Executive Summary of data protection audits may be available for longer if a data controller has consented to a follow up audit report being published: see section 3.3).

3.3 Follow up audit reports

- We will not proactively publish any details of any consensual follow up audit before completion of the report.
- Where a follow up audit is undertaken, a report and Executive Summary of this report will be produced. The follow up Executive Summary will include a copy of the Executive Summary of the original consensual audit report as an appendix. The ICO will expect to publish the follow up Executive Summary on our website and will encourage the data controller to allow us to do so. However, the data controllers can prevent the ICO from publishing the reports.

In these cases, we will put a note on the ICO website saying that the data controller asked us not to publish it. The follow up reports – full and summary – will still be subject to case by case consideration if requested under the Freedom of Information Act.

- Details of consensual follow up audits and Executive Summaries of consensual follow up audit reports will be available on our website for one year after publication.

4 When we are likely to publicise compulsory audits

We would normally liaise with the audited organisation before publicising the audit or its outcomes. However, some stories will get into the news without the ICO proactively intervening and liaison will not always be possible. Promises about publicity, or the lack of it, outside of the provisions of the Code of Practice or the Guide to ICO privacy and electronic communications regulations audits, must not be made by ICO staff to data controllers, as this is not necessarily in the ICO's control and could lead to damaging the ICO's reputation.

4.1 Before the audit

- If it's already a news story, we would probably publicise the fact we're undertaking an audit.

4.2 After the audit

- Where there's an opportunity for education/prevention.
- If the findings highlight it's new, extreme, a first etc (standard news criteria).

- If it meets a communications, corporate or information rights objective.
- If it would help others to learn from the audit findings to publicise it.
- If there are aggregate stories showing trends etc.
- Where publicity is likely to deter others.
- Where publicity would be in the public interest.

4.3 When we are not likely to publicise compulsory audits

- Where the purpose of the audit or the audit findings are not of substantial public interest.
- When we have several similar stories and time or news constraints mean we have to choose.
- If it is too dull or technical to make the news.

5 When we are likely to publicise consensual audits

In similar circumstances as described above, but in consultation with the data controller.