Audit: a guide to ICO privacy and electronic communications regulations audits

ico.
Information Commissioner's Office

Contents

1. Introduction

1.1 Role of the Information Commissioner

On 26 May 2011, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (PECR) came into force. These amend the Privacy and Electronic Communications (EC Directive) Regulations 2003. The Information Commissioner (the Commissioner) already has some powers under the 2003 regulations. The amended regulations enhance these powers, and provide the Commissioner with powers to audit the measures taken by a public electronic communications service (as defined by section 32 of the Communications Act 2003 and hereafter referred to as 'service provider') to safeguard the security of that service (regulation 5(6)).

The Commissioner sees auditing as a constructive process with real benefits for service providers and so aims to establish, wherever possible, a participative approach. He will usually seek the consent of a service provider to a 'consensual' audit however where service providers are unwilling to engage **and** risks have been identified, the Commissioner will use his powers under the amended regulations to conduct a 'compulsory' audit.

1.2 Objectives of audit activities

The purpose of this manual is to set out the procedures that will be followed for both consensual and compulsory audits in line with the powers under the amended regulations. These procedures will be reviewed in light of experience and how these audits work in practice.

The primary objective of an audit is to ensure that the service provider has taken appropriate technical and organisational measures to safeguard the security of the public electronic communications service they provide. These measures shall at least:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;
- protect personal data, stored or transmitted, against accidental or unlawful destruction, accidental loss, and unauthorised or unlawful storage, processing, access or disclosure; and
- ensure the implementation of a security policy with respect to the processing of personal data.

1.3 Risk-based approach

In line with the 'Regulators' Compliance Code' the Commissioner will adopt a risk-based, proportionate and targeted approach to prioritise its audit activities.

As the powers of compulsory audit in the regulations cover all service providers the use of a risk based prioritisation process allows us to focus our efforts to the activities where we can make the biggest impact. This risk based prioritisation will be refined in the light of the developing audit experience of the Information Commissioner's Office (ICO).

The risk based prioritisation involves the identification and measurement of the capacity to harm and, if such capacity exists, an evaluation of the likelihood of the occurrence of that harm.

In determining the risks associated with non compliance and hence the selection of service providers for audit, the Commissioner will consider the following factors:

- the compliance 'history' of the service provider based on complaints made to the Commissioner and the service providers' responses;
- 'self reported' breaches and the remedial actions identified by service providers;
- communications with the service provider which highlight a lack of compliance controls;
- business intelligence such as news items in the public domain which highlight security risks as well as information from other regulators;
- information published by the service provider which highlights issues in the measures taken to safeguard the security of their service;
- internal / external audits conducted on service providers related to the processing of personal data;
- notification details and history;
- the implementation of new systems or processes where there is a public concern that the security of the service may be at risk;

- the volume and nature of personal data being processed;
- evidence of recognised and relevant external accreditation;
- the perceived impact on individuals of any potential non-compliance; and
- other relevant information eg reports by 'whistleblowers'.

In determining the impact on individuals the Commissioner will consider the following factors:

- the number of individuals potentially affected;
- the nature and sensitivity of the data being processed;
- the nature and extent of any likely damage or distress caused by non compliance.

1.4 Consensual audit

In the first instance the Commissioner will seek to conduct a 'consensual' audit. When the prioritisation process, as outlined in section 1.3 above, identifies a service provider for inclusion in the audit programme, the ICO will write to the organisation with a Letter of Invitation (**Appendix A**). This is in line with the Commissioner's wish to establish, wherever possible, a participative approach.

Once the service provider accepts the invitation, the details and the scope of the audit will be defined and formalised in a Consensual Letter of Engagement (**Appendix B**).

1.5 Compulsory audit

A compulsory Letter of Engagement will normally be deemed necessary by the Commissioner when:

- a prioritisation has been conducted as outlined in section 1.3 above; and
- the service provider has, within six weeks, failed to respond to a written request from the Commissioner to undertake an audit or has refused consent to such an audit, without adequate reasons.

In exceptional circumstances, the Commissioner may issue a compulsory Letter of Engagement where there are other compelling reasons to do so.

If the service provider has not entered into a commitment to allow the audit to take place on specified dates that are acceptable to the ICO within this timescale, a Compulsory Letter of Engagement will be served (**Appendix C**).

This Compulsory Letter of Engagement will set out that the audit visit will be carried out on dates specified in the letter (usually within 90 days). The letter will identify the purposes, objectives and scope of the audit. It will also identify any requests for additional assistance which, in the view of Commissioner, will facilitate the effective conduct of the audit. By way of example this might include the identification, by the service provider, of a 'single point of contact' or members of staff the audit team may require access to.

During the course of a compulsory audit, the service provider is required to comply with the Commissioner's request to inspect premises, documentation and equipment; and make available the relevant and appropriate staff for interview.

Details of Compulsory Letters of Engagement will be published on the Information Commissioner's website.

2. Audit process

Audits undertaken by the Commissioner will be conducted in two phases: an off site 'adequacy' audit and an on site 'compliance' audit. Prior to each audit, and where appropriate, a meeting will be arranged with relevant stakeholders to discuss the arrangements and scope of the audit. Where this is not practical we may seek to do this via a telephone conference.

2.1 Adequacy review

The 'adequacy' audit will normally be conducted off site, prior to the audit visit and will consist of a review of relevant policies, procedures, guidance and training material. The key consideration will be how these documents provide a framework for compliance with Regulation 5 in relation to the obligations to safeguard security of data. Any significant findings will be detailed in the Audit Report. These documents and the output from the review will provide the framework for the 'compliance' audit.

The review of these documents is normally done off site in order to minimise the disruption to business and to ensure that time on site is efficient and effective. To reduce the burden on service providers we can receive these documents electronically through our secure network and regularly receive sensitive documentation this way. Wherever possible we try and take a collaborative approach and on

occasion where it more effective to view particular documentation on site then we have the flexibility to do so.

The length of time necessary to conduct the 'adequacy' audit will vary based on the volume and complexity of material provided.

Access will be required to the specified documents and information, which define and explain how the service provider intends to meet these obligations and the governance controls in place to measure compliance. This could include for example:

Strategies	Policies	Procedures
Guidance	Codes of Practice	Training Material
Protocols	Frameworks	Privacy Statements
Privacy Impact Assessments		Control Data
Job Descriptions		Terms of Reference

Access may also be required to specified personal data, or classes of personal data, and to evidence that it is being handled in line with the policies and procedures in as much as they deliver compliance with regulation 5. The level of such access will be proportionate to that required to assess compliance.

Access will not be required to information which is subject to legal privilege or information which:

- has a high level of commercial sensitivity; and/or
- is exempt from Part V of the Data Protection Act 1998 by virtue of a certificate under section 28 (national security).

2.2 Audit visit

The 'compliance' audit will be focused on the security measures in place to safeguard personal data and conducted on the service provider's site(s) over a number of days.

The number of 'on site' days will vary based on the scope of the audit, the organisational structure and the location of sites. For the majority of staff identified for interview, no more than an hour of their 'face to face' time will be required. The Commissioner will take all reasonable steps necessary to minimise the impact on normal business activity.

Inspections and examinations are key review elements of the audit. They identify objective evidence of compliance and how policies and

procedures have been implemented and effectively mitigate security risks to personal data.

These reviews of personal data, and associated logs and audit trails, will consider electronically stored and processed data, including data stored centrally, locally and on mobile devices and media.

The scope of the audit is limited to obligations under Regulation 5, and is documented and agreed in the Letter of Engagement. Examples of the areas of focus for the audit include:

- Security governance arrangements
- Information security frameworks and policies
- Risk management procedures
- Organisational structures and ownership
- Asset management systems and procedures
- Incident management and breach inventory and notification processes (see Appendix E)
- Training and awareness
- Third party contracts
- Physical security
- Identify access management
- Network access controls
- Remote working procedures and systems
- System monitoring
- Web applications
- Anonymisation of data
- Encryption and deletion of data
- Logging, monitoring and audit trials

The review may evaluate physical and IT-related security measures.

The compliance audit may cover management/control information used to monitor and record how personal data is being processed and measure how a service provider meets its obligations under regulation 5.

It may also involve sitting with staff to demonstrate 'practice' or the sampling of controls by auditors. This might involve providing auditors with manual copies of data. In this case, the extent to which information is taken off site will be kept to a minimum and such information will only be retained by the ICO so far as it is necessary to complete the audit and any identified follow up action. Any direct access to records would be limited, would be done locally and would be for a limited and agreed time.

The visit will also consist of a series of interviews. Interviews will comprise discussions with the:

- service provider's staff; and
- service provider's contractors.

Departmental managers, operational staff, support staff (eg IT staff, security staff) as well as staff involved with information and safeguarding the security of the data may be considered as interview candidates.

Discussions will be scheduled and agreed with the service provider as far as practicable before the on-site audit takes place. A schedule of areas to be covered will be provided to the service provider prior to the audit and the level and grade of staff eg managers, operational staff etc will be discussed and agreed. Individuals should be advised, by the service provider, in advance of their required participation.

Questions will be used to understand individual roles and the processes followed or managed specifically with reference to the handling of personal data and the security of that data. Some questions may relate to data protection training and awareness but they will not be framed as a test nor are they intended to catch people out.

Interviews may be conducted at an individual's desk or in a separate room dependent upon circumstances and whether there is a need to observe the working environment or examine information and records. Interviews will normally be 'one-to-one' but sometimes it may be appropriate, because for example of shared responsibilities, to include a number of staff in an interview. Notes will be taken by the auditors during the interviews.

Given the nature of interviews the Commissioner does not consider it to be necessary for those subject to interview to be accompanied by third parties but he will not object where it is reasonably recommended.

Every effort will be taken to restrict interviews to staff identified within the agreed schedule, but where it is clear in the course of the audit that access to additional staff may be necessary to address unresolved questions, this will be arranged with the service provider. In a similar way the schedule should not preclude confirmatory conversation with a consenting third party; for example where the third party is in close proximity to a desk side discussion.

Interviews are to help in assessing compliance. They do not form part of, or provide information for, any individual disciplinary or criminal investigation. Should evidence of criminal activity by an individual emerge during an interview, the interview will be halted.

Individuals' names may be used in distribution lists and acknowledgements sections of reports but will not be referenced in the body of any report. Job titles may be used where appropriate.

The findings of the audits will be documented in an Audit Report with opportunities provided for the service provider to comment on accuracy and respond to the recommendations. Informal feedback on preliminary findings may also be provided by auditors during the course of an audit.

2.3 Audit report

The audit report gives an audit opinion as to whether or not a service provider has complied or is complying with regulation 5. It will further report levels of assurance in respect of the mitigating measures and controls. The findings will be presented by the way of:

- a summary of findings;
- an audit opinion;
- detailed findings against predefined risks; and
- associated recommendations.

The report will include an opinion based on the audit work that the Commissioner's staff have performed. The opinion will consider the governance and associate control arrangements in place at the time of the audit and provide a statement on the status of the service provider's compliance with regulation 5.

Where it is identified in the course of the audit that the service provider has failed to meet the requirements of a Compulsory Letter of Engagement the Commissioner will make a decision as to the material impact on the audit and consequently whether reference will be made to the omission in the report.

A draft report, containing the Commissioner's findings, will be produced after the audit visit. The service provider will be given the opportunity to review the draft for the purpose of identifying any factual inaccuracies and to highlight any pertinent information which might have been omitted. The Commissioner will address any issues identified by the service providers' feedback and update the audit report as appropriate.

The report will also include recommendations about what steps the service provider ought to take or not take to comply with regulation 5. The organisation will be asked to agree the recommendations and complete an action plan indicating how, when and by whom the recommendations will be implemented. The report may also include points of difference which cannot be resolved between the service provider and the Commissioner.

If the service provider fails to respond to the draft report and recommendations within reasonable and defined timescales then the Commissioner will issue the report as a final report and present it to the Chief Executive Officer or equivalent.
The final report (**Appendix D**) will then be issued to the organisation with a draft Executive Summary. The Executive Summary will be a template of high level sections taken from the report and produced in a different format for publication. The organisation will be provided with five working days to agree the summary.

For a consensual audit, if agreement is given the Executive Summary will be published on the ICO website. If there is no agreement the ICO will publish a comment that an audit took place, but the organisation declined to have the Executive Summary published. Where requested, a URL link to the service provider's website will be included to allow the public to view any comments the organisation makes about the audit. Example wording for the website can be found below:

[Date]
The ICO has carried out a PECR audit of [name of org] with its consent.
Read the executive summary of the audit report [link]
Read more about the audit on the [name of org] website [link]

[Date]
The ICO has carried out a PECR audit of [name of org] with its consent.
[Name of org] has asked us not to publish the executive summary of the audit report.

For compulsory audits, following the completion of the audit, the 'Executive Summary' reports will be made available on the Commissioner's website. The Commissioner will previously have taken into account any opinions from the service provider about the suitability for publication of any element.

[Date]
The ICO has carried out a compulsory PECR audit of [name of org].
Read the executive summary of the audit report [link]
Read more about the audit on the [name of org] website [link]

As with consensual audits, the Commissioner will also include links to the service provider's own website should the service provider request the option of making a formal response to the report.

Both consensual and compulsory audit reports will be available on the ICO website for one year after publication. After that, they will be retained in line with the Commissioner's retention policy.

More information regarding the publication of audit reports is available in the 'communicating audits' policy on the ICO website.

Requests made for copies of the full audit report, made under the Freedom of Information Act 2000, will be considered, on a case by case basis, in line with the Commissioner's obligations as a public authority. In such instances the Commissioner will seek the views of the service provider on disclosure, specifically with reference to matters such as possible prejudice to information security or commercial confidentiality.

In the past, we have received and responded to a number of information requests for specific audit reports. We have dealt with requests where we have withheld a report in its entirety, provided a redacted report and provided a report in full.

The basis for this approach is in section 59 of the DPA which relates to information provided to the Information Commissioner and his staff. This states that ICO staff shall not disclose information that:

> relates to an identifiable individual or business; and
> is not at the time of disclosure, and has not previously been, available to the public from other sources

unless the disclosure is made lawfully.

In most cases where the information being requested is an audit report, for the disclosure to be lawful, we would have to have the consent of a representative of the organisation concerned.

The Commissioner may also make general references to audits and the conclusions drawn from them in his annual or other reports.

This guide will be made available on the ICO website.

2.4 Auditors

In the case of a consensual or a compulsory audit, a team of competent auditors will conduct the audit. These auditors will be employed directly by the ICO or contracted to, and under control of the ICO. Auditors will have, or be working towards an audit qualification.

Auditors on occasion may be accompanied by other ICO staff with specific experience of relevance to the service provider being audited.

Auditors and accompanying ICO staff will have signed confidentiality clauses as part of their contract of employment and engagement. Auditors and accompanying ICO staff will be subject to the Official Secrets Act 1989. Auditors are also covered by Section 59 of the Data Protection Act which creates an offense for ICO staff to knowingly or recklessly disclose any information given to the ICO for the purposes of fulfilling its functions. The auditors have also been, or are in the process of being, vetted for Security Clearance and are experienced in dealing with commercially sensitive documents and information.

2.5 Actions resulting from an audit

The Commissioner does not intend that audits will normally lead to formal enforcement action; rather they are seen as a means of encouraging compliance and good practice. However, on issuing the final report the Commissioner will indicate whether it is his intention to follow up the service provider's responses to his recommendations, if any. Follow up may consist of seeking written assurances from the service provider of actions it has taken, or a further audit.

The prioritisation of organisations for inclusion in the audit programme, as outlined in section 1.3, may identify some service providers who have previously been audited. Where this occurs, the Commissioner will routinely examine progress against any previous recommendations made.

In the process of an audit the Commissioner is not prevented from imposing a fixed monetary penalty (£1,000) where a contravention of the regulation 5A is discovered. However he has discretion, based on the circumstances of the case, as to whether he imposes a fixed monetary penalty when he becomes aware of a contravention.

He also has discretion as to whether, when multiple contraventions are discovered, he imposes a single penalty or multiple penalties.

Additionally the Commissioner is not prevented from imposing civil monetary penalties for serious contraventions of PECR discovered during the course of a compulsory audit.

Further detail on the enforcement of the amended regulations is available on the ICO website.[1]

[1] http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/~/media/documents/library/Privacy_and_electronic/Practical_application/enforcing_the_revised_privacy_and_electronic_communication_regulations_v1.pdf

3. Appendices

A. Example letter of invitation
B. Example consensual letter of engagement
C. Example compulsory Letter of engagement
D. Example audit report
E. Breach notification requirements

Appendix A - letter of invitation

Dear Chief Executive Officer

On 26 May 2011, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (PECR) came into force. The amended Regulations provide the Commissioner with powers to audit the measures taken by a public electronic communications service (as defined by section 32 of the Communications Act 2003) to safeguard the security of that service (Regulation 5(6)).

The primary objective of these audits is to ensure that service providers have appropriate technical and organisational measures to safeguard the security of the public electronic communications service they provide. These measures should at least:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;
- protect personal data, stored or transmitted against accidental or unlawful destruction, accidental loss, and unauthorised or unlawful storage, processing, access or disclosure; and
- ensure the implementation of a security policy with respect to the processing of personal data.

The Commissioner sees auditing as a constructive process with real benefits for service providers and so aims to establish, wherever possible, a participative approach. As such, in the first instance the Commissioner's Office (ICO) will approach service providers for their consent to conduct these audits.

However, where service providers are, for whatever reason, unwilling to engage and risks have been identified, the Commissioner will use his powers under the amended Regulations to conduct a 'compulsory' audit. If consent to the audit is not received within six weeks of the date of this letter, the Commissioner may issue a Compulsory Letter of Engagement which will require your organisation to undergo an audit within a specified timescale.

Further information on the ICO's approach to these audits is outlined in our Privacy and Electronic Communications Regulations Audit Manual, available the ICO website.

The audit process is one which can deliver valuable benefits and I hope that you are willing to allow us to undertake a consensual audit. I look forward to hearing from you with your thoughts on how we can work together.

Appendix B - consensual letter of engagement

Information Commissioner's Office Privacy and Electronic Communications Regulations Audit

To:

Date:

From:

1. Background

1.1 The Information Commissioner may audit the measures taken by the provider of a public electronic communications service to safeguard the security of that service Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 Reg. 5(6))

1.2 The Information Commissioner sees auditing as a constructive process with real benefits for service providers and so aims to establish, wherever possible, a participative approach.

1.3 The Information Commissioner, in the interests of clarity, distinguishes between compulsory and consensual Privacy and Electronic Communications Regulations (PECR) audits.

The Information Commissioner has reiterated a desire, in the first instance and as far as is practicable, to conduct consensual PECR audits.

1.4 In [blank], [blank] agreed to a consensual audit by the ICO of the security of its public electronic communications service.

1.5 The primary purpose of the audit is to provide the Information Commissioner and [blank] with an independent opinion of the extent to which [blank], within the scope of this agreed audit, is complying with Regulation 5 of the amended Privacy and Electronic Regulations.

2. Scope

2.1 The audit scope will assess compliance with Regulation 5 of Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

2.2 The ICO will restrict its audit activity to the departments and locations agreed with [blank].

2.3 The audit will not review and provide a commentary on individual cases, other than to the extent that such work may demonstrate the extent to which [blank] is fulfilling its obligations under Regulation 5.

2.4 The ICO, however, retains the right to comment on any other weaknesses observed in the course of the audit that could compromise compliance with Regulation 5.

2.5 The ICO retains the right to issue a fixed monetary penalty for any contravention of PECR discovered during the course of the audit.

3 Performing the audit

3.1 The Audit Team Manager responsible for the audit will meet with representatives of [blank] prior to the audit:

- To gain a strategic overview of the public electronic communications service and any relevant background information.
- To appropriately refine and agree the scope as currently defined.
- To discuss locations identified by the ICO for the visits and the duration of on site work required for each site.
- To identify and agree any policies and procedures that could be provided in advance of the audit site visits, to adequately inform the audit process.

3.2 The ICO would seek to visit key departments and sites within the scope of the audit and organisation as arranged with the [blank].

3.3 In identifying appropriate locations the ICO will consider the following:

- The organisation's feedback on compliance with internal policies and procedures.
- Current and historical complaint information obtained from the ICO's case handling department.
- Security Breach Notification Reports and Logs as provided to the ICO.

3.4 A schedule of meetings and audit activities will be agreed with the nominated single point of contact for the audit and the identified business areas.

3.5 The audit team will meet with relevant managers and staff as appropriate to establish the controls implemented to ensure the organisation complies with its Regulation 5 responsibilities. This will be achieved through discussions with staff members, review of relevant records and a review of the procedures in practice.

3.6 The ICO will require access to relevant key personnel 'desk side' where possible (limited to the scope provided).

3.7 The ICO will consider the extent to which the Internal Audit department include security audits in their programmes of audit or compliance work to avoid duplication of work.

3.8 As far as is practicable and appropriate the ICO will provide regular feedback on audit progress to the nominated single point of contact. The ICO believes that regular feedback should assist both the ICO and the organisation to quickly understand and address emerging issues, concerns or misunderstanding.

4. Audit team

4.1 The following people will be part of the audit team. It is envisaged that three auditors will be used for the on site visit.

	Team Manager (Audit)
	Engagement Lead Auditor
	Auditor

5. Reporting Responsibilities

5.1 Initially a draft report will be issued detailing the audit findings. Input will be sought from the nominated single point of contact to ensure that the report is factually accurate. Following any amendments for accuracy a second draft report will be issued complete with any appropriate recommendations. This draft will be returned by [blank] accepting or otherwise the recommendations and including an action plan against each recommendation. Each action will require the title of the person responsible for the action and a date for completion. Thereafter the final report will be issued to agreed recipients.

5.2 The audit will provide [blank] with an overall opinion based on the work undertaken, using a framework of four categories of assurance, from high level of assurance to very limited assurance. The opinion will be based on the effectiveness of the processes, policies, procedures and practices operating to mitigate any identified risks to complying with Regulation 5 of PECR.

5.3 The ICO will produce an Executive Summary which it will agree with [blank].

5.4 The identity of organisations that are being audited is published on the ICO website as part of proactively communicating the audit work programme. However, the ICO will not proactively publish details of the scope and findings of a consensual audit prior to the completion of the audit.

5.5 Once the audit report and Executive Summary have been completed and agreed the ICO will publish a statement on its website to indicate that a PECR audit has been completed and will seek agreement from [blank] to publish the Executive Summary.

5.6 [Blank] will be informed in advance of the publication date and will be provided with the opportunity to provide a link to its own website for any further organisational comments it wishes make.

6. Timescales

	Responsibilities of the ICO	Responsibilities of [blank]
Date letter of engagement to be agreed:		
Date of on-site visits:		
Date of first draft report:		
Date comments on draft provided:		
Date of second draft:		
Date of second draft with action plan:		
Date of final report and executive summary:		

Note that these are provisional dates which may vary with the agreement of both parties.

7. Contacts

7.1 Key Contacts

[blank]
[blank]

7.2 A separate schedule of the organisation's personnel to be actively involved with the audit site visits will be documented and agreed between the parties in advance of the site visits.

8. Administration

8.1 Individual site arrangements for access and audit will be organised through [blank].

8.2 Where possible interviews will be carried out 'desk side'. With the exception of reviews and interviews undertaken at specialist technical sites which may be conducted at a pre agreed location.

8.3 A room will be made available, where possible, to the Information Commissioner's auditors at sites identified in the schedule to carry out interviews when it is not appropriate to work 'desk side'. Separate accommodation will also be provided for auditors, where possible, for use while they are not conducting interviews / examinations. No remote network access is required.

9. Confidentiality of Information

9.1 No member of the ICO Audit Team will disclose any information:

- which has been obtained by, or furnished to, the Commissioner under or for the purposes of the PECR,
- relates to an identified or identifiable individual or business, and
- is not available at the time of the disclosure, and has not previously been, available to the public from other sources,

unless the disclosure is made with lawful authority.

10. Expected Added Value

10.1 The provision of an independent opinion in relation to compliance with Regulation 5 of PECR and progress towards the implementation of good practice.

10.2 The opportunities for staff to discuss and exchange actual security issues and examples of good practice with the members of the Information Commissioner's audit team.

10.3 The knowledge and experience of the auditors enables a proportionate consideration of the risk and impact of non-compliance to be taken.

10.4 An improved understanding by the ICO of [blank], its structure and the security measures it employs.

Client Comments Agreed by Client Signed: Position: Date:

Appendix C - compulsory letter of engagement

Information Commissioner's Office Privacy and Electronic Communications Regulations Audit

To:

Date:

From:

1. Background

1.1 The Information Commissioner may audit the measures taken by the provider of a public electronic communications service to safeguard the security of that service Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 Reg. 5(6))

1.2 The Information Commissioner sees auditing as a constructive process with real benefits for service providers and so aims to establish, wherever possible, a participative approach.

1.3 The Information Commissioner, in the interests of clarity, distinguishes between compulsory and consensual Privacy and Electronic Communications Regulations (PECR) audits.

The Information Commissioner has reiterated a desire, in the first instance and as far as is practicable, to conduct consensual PECR audits.

1.4 On [blank], [blank] was invited to participate in a consensual audit by the ICO of the security of its public electronic communications service. To date no response has been received and as a result the Information Commissioner is now minded to conduct a compulsory audit of service provider.

1.5 The Regulations require that the service provider shall comply with the requirements of the Information Commissioner as detailed in the scope.

1.6 The primary purpose of the audit is to provide the Information Commissioner and [blank] with an independent opinion of the extent to which [blank], within the scope of this audit, is complying with Regulation 5 of the amended Privacy and Electronic Regulations.

2. Scope

2.1 The audit scope will assess compliance with Regulation 5 of the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

2.2 The service provider is required:

to direct the Commissioner to any documents requested;

to permit the Commissioner to inspect or examine any of the documents to which the Commissioner is directed;

to comply with any request from the Commissioner for a copy of any of the documents to which the Commissioner is directed;

to assist the Commissioner to view any information that is capable of being viewed using equipment on the premises;

to permit the Commissioner to inspect or examine any of the information to which the Commissioner is assisted to view;

to comply with any request from the Commissioner for a copy (in such form as may be requested) of any of the information which the Commissioner is assisted to view;

to direct the Commissioner to any equipment or other material on the premises;

to permit the Commissioner to inspect or examine any of the equipment or material to which the Commissioner is directed; and

to make available for interview the persons of specified descriptions who process personal data on behalf of the service provider and are willing to be interviewed.

2.3 The ICO will restrict its audit activity to the departments and locations agreed with [blank].

2.4 The audit will not review and provide a commentary on individual cases, other than to the extent that such work may demonstrate the extent to which [blank] is fulfilling its obligations under Regulation 5.

2.5 The ICO, however, retains the right to comment on any other weaknesses observed in the course of the audit that could compromise compliance with Regulation 5.

2.6 The ICO retains the right to issue a fixed monetary penalty for any contravention of PECR discovered during the course of the audit.

3 Performing the audit

3.1 The Audit Team Manager responsible for the audit will meet with representatives of [blank] prior to the audit:

- To gain a strategic overview of the public electronic communications service and any relevant background information.
- To discuss locations identified by the ICO for the visits and the duration of on site work required for each site.
- To identify and agree any policies and procedures that could be provided in advance of the audit site visits, to adequately inform the audit process.

3.2 The ICO would seek to visit key departments and sites within the scope of the audit and organisation as arranged with the [blank].

3.3 In identifying appropriate locations the ICO will consider the following:

- The organisation's feedback on compliance with internal policies and procedures.
- Current and historical complaint information obtained from the ICO's case handling department.
- Security Breach Notification Reports and Logs as provided to the ICO.

3.4 A schedule of meetings and audit activities will be agreed with the nominated single point of contact for the audit and the identified business areas.

3.5 The audit team will meet with relevant managers and staff as appropriate to establish the controls implemented to ensure the organisation complies with its Regulation 5 responsibilities. This will be achieved through discussions with staff members, review of relevant records and a review of the procedures in practice.

3.6 The ICO will require access to relevant key personnel 'desk side' where possible (limited to the scope provided).

3.7 The ICO will consider the extent to which the Internal Audit department include security audits in their programmes of audit or compliance work to avoid duplication of work.

3.8 As far as is practicable and appropriate the ICO will provide regular feedback on audit progress to the nominated single point of contact. The ICO believes that regular feedback should assist both the ICO and the organisation to quickly understand and address emerging issues, concerns or misunderstanding.

4. Audit team

4.1 The following people will be part of the audit team. It is envisaged that three auditors will be used for the on site visit.

	Team Manager (Audit)

	Engagement Lead Auditor
	Auditor

5. Reporting Responsibilities

5.1 Initially a draft report will be issued detailing the audit findings. Input will be sought from the nominated single point of contact to ensure that the report is factually accurate. Following any amendments for accuracy a second draft report will be issued complete with any appropriate recommendations. This draft will be returned by [blank] accepting or otherwise the recommendations and including an action plan against each recommendation. Each action will require the title of the person responsible for the action and a date for completion. Thereafter the final report will be issued to agreed recipients.

5.2 The audit will provide [blank] with an overall opinion based on the work undertaken, using a framework of four categories of assurance, from high level of assurance to very limited assurance. The opinion will be based on the effectiveness of the processes, policies, procedures and practices operating to mitigate any identified risks to complying with Regulation 5 of PECR.

5.3 The ICO will produce an Executive Summary which it will agree with [blank].

5.4 The identity of organisations that are being audited is published on the ICO website as part of proactively communicating the audit work programme. However, the ICO will not proactively publish details of the scope and findings prior to the completion of the audit. The Information Commissioner **will** proactively publish details of the compulsory audit upon completion of the audit.

5.5 Once the audit report and Executive Summary have been completed and agreed the ICO will publish a statement on its

website to indicate that a compulsory PECR audit has been completed and will also publish the Executive Summary.

5.6 [Blank] will be informed in advance of the publication date and will be provided with the opportunity to provide a link to its own website for any further organisational comments it wishes make.

6. Timescales

	Responsibilities of the ICO	Responsibilities of [blank]
Date letter of engagement to be agreed:		
Date of on-site visits:		
Date of first draft report:		
Date comments on draft provided:		
Date of second draft:		
Date of second draft with action plan:		
Date of final report and executive summary:		

7. Contacts

7.1 Key Contacts

[blank]
[blank]

7.2 A separate schedule of the organisation's personnel to be actively involved with the audit site visits will be documented and agreed between the parties in advance of the site visits.

8. Administration

8.1 Individual site arrangements for access and audit will be organised through [blank].

8.2 Where possible interviews will be carried out 'desk side'. With the exception of reviews and interviews undertaken at specialist technical sites which may be conducted at a pre agreed location.

8.3 A room will be made available, where possible, to the Information Commissioner's auditors at sites identified in the schedule to carry out interviews when it is not appropriate to work 'desk side'. Separate accommodation will also be provided for auditors, where possible, for use while they are not conducting interviews / examinations. No remote network access is required.

9. Confidentiality of Information

9.1 No member of the ICO Audit Team will disclose any information:

- which has been obtained by, or furnished to, the Commissioner under or for the purposes of the PECR,
- relates to an identified or identifiable individual or business, and
- is not available at the time of the disclosure, and has not previously been, available to the public from other sources,

unless the disclosure is made with lawful authority.

Signed: Position: Date:

Appendix D – example audit report

[Name of Organisation]

Privacy and Electronic Communications Regulations Audit Report

Auditors:

Distribution:

Draft Report:

Final Report:

Date Issued:

Contents

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.
The responsibility for ensuring that there are adequate security arrangements in place rests with the management of [blank].
We take all reasonable care to ensure that our audit 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.

1. Background and Scope

1.1 The Information Commissioner may audit the measures taken by the provider of a public electronic communications service (service provider) to safeguard the security of that service. (Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 Reg. 5(6))

1.2 The Information Commissioner sees auditing as a constructive process with real benefits for service providers and so aims to establish, wherever possible, a participative approach.

1.3 In [blank], [blank] agreed to a **consensual** audit by the ICO of its public electronic communications service.

1.4 An introductory meeting was held on the [blank] with representatives of [blank] to identify and discuss the scope of the audit.

1.5 The audit scope was the compliance with Regulation 5 of the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011. In particular, the extent to which a service provider has taken appropriate technical and organisational measures to safeguard the security of the service.

2. Audit Opinion

2.1 The primary purpose of the audit is to provide the Information Commissioner and [blank], with an independent opinion of the extent to which [blank], within the scope of this agreed audit, is complying with Regulation 5 of the PECR.

2.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with Regulation 5 of the PECR.

Overall Conclusion
Audit grading from section 4

3. Summary of Audit Findings

3.1 Areas of Good Practice.

3.2 Areas for Improvement.

4. Audit Approach

4.1 The audit was conducted following the Information Commissioner's Privacy and Electronic Communications Regulations 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.

4.2 The audit field work was undertaken between the [blank] at [blank].

5. Audit Grading

Colour Code	Audit Opinion	Recommendation Priority	Definitions
	High assurance	Minor points only are likely to be raised	The technical and organisational measures taken by the provider of a public electronic communications service to safeguard the security of that service provide a high level of assurance that processes and procedures are in place and being adhered to. The audit has identified 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.
	Reasonable assurance	Low priority	The technical and organisational measures taken by the provider of a public electronic communications service to safeguard the security of that service provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements.
	Limited assurance	Medium priority	The technical and organisational measures taken by the provider of a public electronic communications service to safeguard the security of that service provide only limited assurance that processes and procedures are in place and are being adhered to. The audit has identified scope for improvement in existing arrangements
	Very Limited assurance	High priority	The technical and organisational measures taken by the provider of a public electronic communications service to safeguard the security of that service provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

6. Detailed Findings and Action Plan

Findings flowing from the audit will be risk categorised using the criteria defined in Section 6. The rating will take into account the impact of the risk and the probability that the risk will occur.

Finding:

Recommendation:

Management response:

The agreed actions may be subject to a follow up audit to establish whether they have been implemented.

7.2 Any queries regarding this report should be directed to [blank]

7.3 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of the selected agencies' and establishments' working practices, policies and procedures. The following staff members were particularly helpful in organising the audit:

- [blank]

Appendix E – Breach notification requirements

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 also include a provision requiring service providers to notify the Information Commissioner when a personal data breach occurs (regulation 5A (2)).

The regulations define a 'personal data breach' as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service.

The regulations specify that the notification to the Commissioner must include at least a description of -

(a) the nature of the breach;
(b) the consequences of the breach; and
(c) the measures taken or proposed to be taken by the provider to address the breach (regulation 5A (4))

and that the notification should be made without undue delay.

In addition to the need to report personal data breaches, the regulations require service providers to maintain an inventory or log of personal data breaches which contains information sufficient to enable the Information Commissioner to verify that organisations have provided him with appropriate notification of breaches (regulation 5A (8)). This inventory must include:

(a) the facts surrounding the breach;
(b) the effects of that breach; and
(c) remedial action taken.

The regulations also require the service provider to notify the subscriber or user if the personal data breach is likely to adversely affect the personal data privacy of the subscriber or user. This notification must contain at least:

(a) a description of the nature of the breach;
(b) information about how to get in contact with the service provider to get more information; and
(c) recommendations on how subscribers can reduce the possible adverse impacts of the breach.

If service providers can demonstrate that appropriate technological measures have been applied to the data to make the data unintelligible to anyone not authorised to access it, they are not required to notify subscribers or users. However, if service providers do not notify subscribers or users, the Commissioner, having considered the likely adverse effects of the breach, may require them to do so.

The process for service providers to notify the Commissioner of a personal security breach under regulation 5A(2) is outlined on the privacy and electronic communications regulations pages of the ICO website.

The Commissioner has the power, under regulation 5B to audit service providers' compliance with these requirements.

Audit approach

Audits of service providers undertaken under regulation 5(6), as described in this manual, will routinely include an inspection of the service providers' inventory of personal data breaches. This will include a review of the service providers' personal data breach inventory, including ensuring that the Commissioner has been notified of breaches, as well as subscriber and user notification where applicable.

Audits of the personal data breach notification requirements may also be undertaken on an ad hoc basis outside the audits undertaken under regulation 5(6), where intelligence indicates a risk that the breach notification may not be accurate or complete. This intelligence may come from a range of sources including one or more of the following:

- complaints received by the Commissioner;
- communications with service providers; or
- business intelligence such as news items in the public domain.

Where intelligence highlights a risk that service providers who should be notifying the Commissioner of personal data breaches have not been doing so, the Commissioner may require the service provider to provide their breach notification inventory by means of an information notice issued under section 43 of the Data Protection Act 1998. Schedule 1 (4) of the regulations enables the Commissioner to issue an 'information notice' to determine whether a person has complied or is complying with the relevant requirements. In this case, a notice would be issued requiring the service provider to send to the Commissioner, in a timescale specified in the notice, their personal data breach inventory in order

for the him to determine that the service provider is complying with the requirement to maintain an inventory of breaches (regulation 5A (8)). Failure to comply with an information notice is a criminal offence.

Actions resulting from an audit

If a service provider fails to comply with the notification requirements, the Commissioner may issue a fixed monetary penalty notice in respect of that failure (regulation 5(C)).

It should be noted that while audits are not intended to lead to enforcement activity, the Commissioner is not prevented from imposing a fixed monetary penalty where a contravention of the breach notification requirements is discovered in the course of an audit. He does have discretion, based on the circumstances of the case, as to whether he imposes a fixed monetary penalty when he becomes aware of a contravention. He also has discretion as to whether; when multiple contraventions are discovered, he imposes a single penalty or multiple penalties.