Ofcom
making communications work for everyone

General policy on ensuring compliance with security duties

Consultation on Ofcom's draft general statement of policy under section 105Y of the Communications Act 2003 (Ofcom's "procedural guidance") and

Consultation on Ofcom's draft guidance on resilience requirements in sections 105A to D of the Communications Act 2003 (Ofcom's "resilience guidance")

General policy on ensuring compliance with security duties – Welsh translation

CONSULTATION:

Publication date: 8 March 2022
Closing date for responses: 17 May 2022

Contents

Section

Annex

Published as separate annexes:

Overview

Following on from the requirement under section 105Y of the Communications Act 2003, this document sets out our proposed guidance on our general policy with respect to the exercise of our functions under sections 105I and 105M to 105V of the 2003 Act. It also proposes an update to our existing guidance on security requirements in sections 105A to D of the 2003 Act made necessary by the changes arising out of Telecommunications (Security) Act 2021, so it focuses on how providers should approach their resilience obligations under the new framework.

What we are proposing

We are consulting on the draft statement of our general policy under section 105Y of the Communications Act 2003 (the "2003 Act") regarding how we will exercise our new functions to seek to ensure that providers comply with their new security duties under the revised security framework.

Our proposed statement explains the procedures that we generally expect to follow in carrying out our monitoring and enforcement activity. We are also providing general guidance about which security compromises we would normally expect providers to report to Ofcom and the process for reporting them.

A key objective of our monitoring role over the first few years of the regime is to determine if each provider is implementing appropriate measures with sufficient pace, as they continue to work towards full compliance. Where we find areas of concern, we will seek to work with providers to ensure appropriate and proportionate measures are implemented in accordance with the security duties. We expect that this collaborative approach will foster more compliant behaviours and reduce the volume of breaches under the 2003 Act, as well as reducing the need for regulatory investigations. We will stand ready to engage our suite of enforcement powers as needed.

In addition, we are consulting on updated guidance on security requirements in sections 105A to D of the 2003 Act made necessary by the changes arising out of Telecommunications (Security) Act 2021.

The new security framework replaces existing sections 105A-105D of the 2003 Act, placing new security duties on providers of public electronic communications networks and services, both in the 2003 Act itself and in regulations. This is supplemented by statutory codes of practice which give guidance on the measures to be taken under sections 105A to 105D.

Given this new framework, we are proposing to update our existing guidance on sections 105A to D of the 2003 Act, in particular recognising that much of this guidance is no longer required given the draft Code of Practice on which Government is currently consulting. In effect, this means that **we are proposing to retain this guidance only insofar as it relates to the sub-category of security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality.**

We have also taken this opportunity to update the guidance to take account of the revised framework, as well as to reflect the changing nature of resilience risks and Ofcom's experience of incident reporting and investigation.

1.1 The Telecommunications (Security) Act 2021 (the "**Security Act**")[1] introduces a revised framework for protecting the security and resilience of public electronic communications service and networks in the UK.

[1] Telecommunications (Security) Act 2021 (legislation.gov.uk)

1.2 The previous framework is set out in sections 105A-105D of the Communications Act 2003 (the "**2003 Act**") and complemented by Ofcom's guidance which was last updated in 2017 ("**Ofcom's 2017 Guidance**").[2]

Security duties and guidance under the revised framework

1.3 The new framework replaces sections 105A-105D of the 2003 Act and is expected to come into force from 1 October 2022.[3] It places new security duties on providers of public electronic communications networks and services ("**providers**"), including:

- the overarching security duties set out in the 2003 Act (sections 105A and 105C);
- duties to take specified measures imposed by the Secretary of State by regulations (sections 105B and 105D); and
- duties to report security compromises to Ofcom and to inform users (sections 105J and 105K).

1.4 The revised framework also provides for two forms of guidance for providers:

a) The Secretary of State's guidance on the measures to be taken by providers under sections 105A to 105D. The Secretary of State has powers to give such guidance by issuing codes of practice under section 105E of the 2003 Act;

b) Ofcom's general policy on how we will exercise our functions under sections 105I and 105M to 105V to seek to ensure compliance with the security duties. The 2003 Act (section 105Y) places a duty on Ofcom to publish a statement setting out such general policy and to have regard to it in exercising our relevant functions.

Ofcom's role

1.5 Ofcom has a general duty under section 105M of the 2003 Act to seek to ensure that providers comply with their security duties. This gives Ofcom a clear remit to work with providers to improve their security and monitor their compliance.

1.6 Ofcom also has certain reporting functions concerning security-related matters. In particular, Ofcom has a duty to inform the Secretary of State about certain risks of security compromise under section 105L, and also must prepare and send to the Secretary of State:

- security reports under section 105Z; and
- infrastructure reports under section 134A which include the extent to which providers are complying with the security duties.[4]

[2] Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003- 2017 Version; ofcom-guidance.pdf
[3] Subject to the commencement date to be specified by the Secretary of State in regulations.
[4] See, in particular, section 134B(1)(ha) and section 134B(2)(fa). In addition, Ofcom may prepare and publish additional reports under section 134AA of the 2003 Act.

DCMS consultations on the Regulations and the Code

1.7 As mentioned above, the Secretary of State has powers to impose specific security measures on providers by making regulations and give guidance on the measures to be taken by issuing codes of practice. In exercise of these powers, DCMS is currently consulting on:

- draft regulations which the Secretary of State intends to make under sections 105B and 105D (the "**Regulations**");[5] and
- a draft code of practice which the Secretary of State intends to issue under section 105E to give guidance for providers with relevant turnover in the relevant period of more than or equal to £50m (the "**Code**").[6]

Ofcom's procedural guidance

1.8 The revised framework gives Ofcom a general duty under section 105M of the 2003 Act to seek to ensure that providers comply with their security duties. To allow Ofcom to fulfil this role, the 2003 Act gives Ofcom powers to monitor and enforce industry's compliance with their security duties (sections 105I and 105N to 105V). In particular, it allows Ofcom to:

- require providers to share information that Ofcom considers necessary for the purpose of carrying out its security functions (section 135, as amended by the Security Act[7]);
- direct providers to explain any failure to act in accordance with guidance given by the Secretary of State in a code of practice (section 105I);
- carry out, or commission others to carry out, an assessment of whether a provider is complying with the security duties (section 105N);
- give assessment notices (section 105O), including issuing an assessment notice which requires a provider to comply with a duty urgently (sections 105P and 105Q). Assessment notices may include requiring providers to complete system tests, make staff available for interview and permit persons authorised by Ofcom to enter operators' premises[8] to view information, equipment and observe tests;
- enforce compliance with the security duties (section 105S), including by imposing penalties (section 105T) and directing a provider to take interim steps (sections 105U and 105V).

1.9 Under section 105Y of the 2003 Act Ofcom has a duty to publish a statement of their general policy with respect to the exercise of their functions under sections 105I and 105M

[5] DCMS consultation on "The Electronic Communications (Security Measures) Regulations 2022", which are still in draft form, is available at: https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice

[6] https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice.

[7] See, in particular, section 135(3)(iza)-(izc), section 135(3A)(za) and section 135(3C) of the 2003 Act.

[8] The 2003 Act (section 105R) places a duty on Ofcom to publish a statement in our annual report setting out the number of occasions on which premises have been entered pursuant to a duty imposed in an assessment notice.

to 105V of the 2003 Act. Annex [A5] contains our draft general statement of policy under section 105Y of the 2003 Act, setting out how we propose to exercise our new powers.

1.10 In particular, our draft general statement of policy under section 105Y of the 2003 Act, explains the procedures that we are generally expecting to follow in carrying out our monitoring and enforcement activity. It also provides general guidance about which security compromises we would normally expect providers to report to Ofcom and the process for reporting them. This guidance on providers' duties to report security compromises is intended to replace the incident reporting guidance which is currently set out in Ofcom's 2017 Guidance. In addition to the above, our draft general statement provides guidance about Ofcom's approach to sharing information with other public bodies, including DCMS, the National Cyber Security Centre and the Information Commissioner.

Ofcom's resilience guidance

1.11 The Security Act introduces the definition of a "security compromise". The guidance set out in Annex [A6] applies to the sub-category of security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality (referred to hereafter as "Resilience Incidents").

1.12 Given the new framework described above, we are proposing to update our existing 2017 guidance on sections 105A to D of the 2003 Act, in particular recognising that much of this guidance is no longer required given the draft Code on which Government is currently consulting. Our updated guidance is set out in Annex [A6]. This guidance is intended to update the resilience-related guidance which is currently set out in Ofcom's 2017 Guidance.

1.13 Ofcom's current guidance, insofar as it relates to security compromises other than Resilience Incidents, will be superseded by the Code.

1.14 Ofcom's current guidance about incident reporting will be replaced by Ofcom's guidance on the reporting of security compromises (including Resilience Incidents) included in Ofcom's statement of general policy.

1.15 The proposed updated guidance now describes how we intend to use our powers and sets out the sources of guidance which we will consider when carrying out our functions in relation to resilience. It also provides some general observations and specific incident scenarios which will inform our approach to resilience. In recognition of this, we are proposing to recast what was general guidance as guidance on resilience requirements in sections 105A to D of the Communications Act 2003. As and when Government decisions are made arising out of the UK Government's National Resilience Strategy Review , Ofcom would expect to review and update or revoke it as appropriate.

Purpose of this consultation

1.16 The consultation period will run for 10 weeks following the publication of this document. During that time, we would welcome responses to this consultation on the proposed (draft) statement of general policy and (draft) guidance on resilience set out in Annex A5 and Annex A6 respectively by [17 May 2022].

1.17 Respondents to this consultation are invited to comment on Ofcom's proposals by responding to the questions set out in Annex [A4].

Next Steps

1.18 After considering the responses, we plan to issue our final statement of general policy and our final guidance on resilience in Autumn 2022, after the publication of the Code by DCMS.

A1. Responding to this consultation

How to respond

A1.1 Ofcom would like to receive views and comments on the issues raised in this document, by 5pm on 17 May 2022.

A1.2 You can download a response form from https://www.ofcom.org.uk/consultations-and-statements/category-1/ensuring-compliance-with-security-duties. You can return this by email or post to the address provided in the response form.

A1.3 If your response is a large file, or has supporting charts, tables or other data, please email it to securityconsultation@ofcom.org.uk, as an attachment in Microsoft Word format, together with the cover sheet. This email address is for this consultation only, and will not be valid after 17 May 2022.

A1.4 Responses may alternatively be posted to the address below, marked with the title of the consultation:

Cindy Hau
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

A1.5 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:

- Send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files. Or
- Upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.

A1.6 We will publish a transcript of any audio or video responses we receive (unless your response is confidential)

A1.7 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt if your response is submitted via the online web form, but not otherwise.

A1.8 You do not have to answer all the questions in the consultation if you do not have a view; a short response on just one point is fine. We also welcome joint responses.

A1.9 It would be helpful if your response could include direct answers to the questions asked in the consultation document. The questions are listed at Annex A4. It would also help if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.

A1.10 If you want to discuss the issues and questions raised in this consultation, please contact Cindy Hau on 020 7981 3212, or by email to securityconsultation@ofcom.org.uk.

Confidentiality

A1.11 Consultations are more effective if we publish the responses before the consultation period closes. In particular, this can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish all responses on the Ofcom website as soon as we receive them.

A1.12 If you think your response should be kept confidential, please specify which part(s) this applies to, and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A1.13 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A1.14 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our Terms of Use.

Next steps

A1.15 Following this consultation period, Ofcom plans to publish a statement in Autumn 2022.

A1.16 If you wish, you can register to receive mail updates alerting you to new Ofcom publications.

Ofcom's consultation processes

A1.17 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex A2.

A1.18 If you have any comments or suggestions on how we manage our consultations, please email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and residential consumers, who are less likely to give their opinions through a formal consultation.

A1.19 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

Corporation Secretary
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA
Email: corporationsecretary@ofcom.org.uk

A2. Ofcom's consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

A2.1 Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

A2.2 We will be clear about whom we are consulting, why, on what questions and for how long.

A2.3 We will make the consultation document as short and simple as possible, with a summary of no more than two pages. We will try to make it as easy as possible for people to give us a written response. If the consultation is complicated, we may provide a short Plain English / Cymraeg Clir guide, to help smaller organisations or individuals who would not otherwise be able to spare the time to share their views.

A2.4 We will consult for up to ten weeks, depending on the potential impact of our proposals.

A2.5 A person within Ofcom will be in charge of making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom's Consultation Champion is the main person to contact if you have views on the way we run our consultations.

A2.6 If we are not able to follow any of these seven principles, we will explain why.

After the consultation

A2.7 We think it is important that everyone who is interested in an issue can see other people's views, so we usually publish all the responses on our website as soon as we receive them. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents' views helped to shape these decisions.

A3. Consultation coversheet

BASIC DETAILS

Consultation title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

CONFIDENTIALITY

Please tick below what part of your response you consider is confidential, giving your reasons why

Nothing ☐

Name/contact details/job title ☐

Whole response ☐

Organisation ☐

Part of the response ☐

If there is no separate annex, which parts? _____

_____

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

DECLARATION

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom seeks to publish responses on receipt. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Signed (if hard copy)

A4. Consultation questions

Questions concerning Ofcom's draft general statement of policy under section 105Y of the Communications Act 2003 (see Annex A5)

Consultation question 1: Do you have any comments on our proposed approach to compliance monitoring?

Consultation question 2: Do you have any comments on our proposed approach to testing?

Consultation question 3: Do you have any comments on our proposed approach to enforcement?

Consultation question 4: Do you have any comments on our proposed approach to reporting security compromises?

Consultation question 5: Do you have any comments on our proposed approach to information sharing?

Consultation question 6: Do you have any other comments on our draft statement of general policy set out at Annex A5 to this consultation?

Questions concerning Ofcom's draft guidance on resilience requirements in sections 105A to D of the Communications Act 2003 (see Annex A6)

Consultation question 7: Do you have any comments on our proposed approach to resilience set out in section 4 of the draft guidance at Annex A6 to this consultation?

Consultation question 8: Do you have any comments on our proposed resilience guidance set out in section 5 of the draft guidance at Annex A6 to this consultation?

Consultation question 9: Do you have any other comments on our draft guidance set out at Annex A6 to this consultation?