

Consultation

Consultation on Ofgem's NIS Enforcement Guidelines and NIS Penalty Policy

Publication date: 4 October 2021

Contact: Bruno Sheldon
Senior Manager

Team: Enforcement

Response deadline: 30 November 2021

Tel: 020 7901 7441

Email: NISEGconsultation@ofgem.gov.uk

Overview:

The Network and Information Systems Regulations 2018 (NIS Regulations) came into force on 10 May 2018 for the water, health, transportation, digital and energy sectors. The NIS Regulations impose duties on Operators of Essential Services (OES) and give relevant Competent Authorities (CAs) powers and responsibilities to ensure OES are meeting those duties.

Ofgem has been designated in the NIS Regulations as a CA acting jointly with the Department for Business, Energy and Industrial Strategy (BEIS), for the Downstream Gas and Electricity (DGE) sectors in Great Britain. As part of Ofgem's duty to regulate the way in which businesses in the energy sector behave, it is important that we can act swiftly and decisively to put things right if businesses fail to meet their obligations.

We are seeking views on the draft NIS Enforcement Guidelines (and draft NIS Penalty Policy which is annexed to the main guidelines document) from OES and all other parties with an interest in our enforcement work under the NIS Regulations. The aim of these guidelines is to provide greater clarity, consistency and transparency to our enforcement policies and processes, and to describe the framework we have in place to maximise the impact and efficiency of our enforcement work under the NIS Regulations. The responses will help us to ensure that our enforcement processes, and penalty policy, are relevant and clear in describing how we will use our enforcement powers under the NIS Regulations.

© Crown copyright 2021

The text of this document may be reproduced (excluding logos) under and in accordance with the terms of the [Open Government Licence](#).

Without prejudice to the generality of the terms of the Open Government Licence the material that is reproduced must be acknowledged as Crown copyright and the document title of this document must be specified in that acknowledgement.

Any enquiries related to the text of this publication should be sent to Ofgem at: 10 South Colonnade, Canary Wharf, London, E14 4PU. Alternatively, please call Ofgem on 0207 901 7000.

This publication is available at www.ofgem.gov.uk. Any enquiries regarding the use and re-use of this information resource should be sent to: psi@nationalarchives.gsi.gov.uk

Contents

Executive summary	4
1. The guidelines	6
2. Consultation questions	9
3. Context and related publications	10
4. Next steps	11

Executive summary

The Gas and Electricity Markets Authority (the Authority) regulates the gas and electricity markets in Great Britain. The Office of Gas and Electricity Markets (Ofgem) carries out the Authority's day-to-day work and investigates matters on its behalf.

As the sector regulator, we have duties to identify and respond to conduct in the gas and electricity sector that may be unlawful, anticompetitive, or otherwise harm consumer interests.

Our role is to protect consumers now and in the future by working to deliver a greener, fairer energy system.

We do this by:

- working with Government, industry and consumer groups to deliver a net zero economy at the lowest cost to consumers;
- stamping out sharp and bad practice, ensuring fair treatment for all consumers, especially the vulnerable; and
- enabling competition and innovation, which drives down prices and results in new products and services for consumers.

The NIS Regulations and Ofgem's role

The aim of the NIS Regulations is to drive improvement in the protection of the network and information systems that are critical for the delivery of the UK's essential services.

Designated operators of essential services (OES) must comply with a number of security duties set out in the NIS Regulations. These include taking appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies. OES must also take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

The Authority acting jointly with the Secretary of State for Business, Energy and Industrial Strategy (BEIS) is the CA responsible for regulating the activities of OES in the DGE sectors in England, Wales and Scotland. The Authority (through its executive arm, Ofgem) is responsible for enforcing compliance with the NIS Regulations in the DGE sectors. This includes investigating potential non-compliance and serving Enforcement Notices and Penalty Notices. Certain compliance and enforcement matters in the DGE sectors are normally handled by BEIS (covering OES designation and related issues). Further details of compliance and enforcement matters that BEIS is responsible for can be found in the draft BEIS guidance which is also out for consultation.

What are we consulting on?

The purpose of this consultation is to seek views on the draft NIS Enforcement Guidelines and NIS Penalty Policy from OES and all other parties with an interest in our enforcement work under the NIS Regulations. The guidance provides information on the processes and procedures Ofgem will generally apply when taking enforcement action under the NIS Regulations in relation to OES in the DGE sectors. For further information on the content of

the guidelines, and on how to respond to this consultation, please refer to information set out below.

The consultation is open until 30 November 2021. Responses should be sent to NISEGconsultation@ofgem.gov.uk.

In addition to this consultation, please note that Ofgem has also published a call for input on its proposed NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain. When finalised this guidance will replace the existing Competent Authority Guidance for Downstream Gas and Electricity in Great Britain. Also, BEIS is consulting on an updated version of its Policy Guidance for the Implementation of the Network and Information Systems Regulations for the Energy Sector in Great Britain.

1. The guidelines

What are we consulting on?

- 1.1. The proposed NIS Enforcement Guidelines are published alongside this consultation. The guidelines are divided into 9 sections with the addition of our proposed NIS Penalty Policy, which is presented in Annex 1 of the main guidelines document.

Section 1: Introduction

- 1.2. The introductory section provides background information on Ofgem's role, objectives and responsibilities. It also provides an overview of the content of the NIS Enforcement Guidelines.

Section 2: Our enforcement powers

- 1.3. Section 2 describes the powers we have under the NIS Regulations to support our enforcement work. These include powers to assist us in our investigative work and to deliver enforcement outcomes, including issuing Enforcement Notices and Penalty Notices.

Section 3: Opening a case

- 1.4. This section describes how we propose to identify and decide whether to open an enforcement case into a potential contravention or failure under the NIS Regulations. We describe the sources of information we most frequently rely on, and how we will handle that information. We explain how we propose to prioritise cases and the factors that are important in helping us determine whether to open a NIS enforcement case.
- 1.5. In some situations our concerns may be resolved satisfactorily via "Alternative Action". This is action we can take without opening an enforcement case, or in lieu of formal enforcement action, to resolve issues or concerns. We describe tools that we propose to use and the criteria that should normally be fulfilled before "Alternative Action" is considered an appropriate means of resolution.

Section 4: Conducting investigations

- 1.6. Section 4 sets out the general procedures we propose to follow once we have decided to open an enforcement case. It explains how we will notify the relevant OES, maintain contact and gather information.

Section 5: Serving Enforcement Notices

1.7. This section describes how and when we may serve an Enforcement Notice. We describe the circumstances in which we may issue an Enforcement Notice and provide information about how decisions to serve Enforcement Notices are to be made. This section also provides information on how OES can respond to an Enforcement Notice.

Section 6: Serving Penalty Notices

1.8. Section 6 describes the circumstances in which we may serve Penalty Notices. It describes how we propose to make penalty decisions and how OES can respond. We also explain how we can enforce penalties and where the proceeds of penalties go.

Section 7: Closing cases

1.9. An enforcement case may be closed at any point. For example, a case may not be pursued if we decide that the issue no longer meets the criteria identified for opening a case. Section 7 describes the circumstances in which we might close an enforcement case.

Section 8: Approach to publishing information about enforcement action

1.10. In this section we describe our approach to making details of cases public. While aiming to be as transparent as possible, we place importance on concerns around confidentiality, any potential impact on our ability to investigate and other concerns such as security. Security is a particularly relevant factor for NIS enforcement work given the issues involved. We will have regard to national security matters and other relevant considerations when reaching decisions about making case details public.

Section 9: Appeals

1.11. Section 9 describes the appeals process under the NIS Regulations and how OES can access it. OES have the right to appeal against certain decisions under the NIS Regulations; this includes our decisions to serve Enforcement Notices and Penalty Notices. Appeals should be made to the First-tier Tribunal (General Regulatory Chamber) in accordance with the provisions of the NIS Regulations and the Tribunal's applicable rules.

Annex 1 – NIS Penalty Policy

1.12. This Annex sets out our proposed NIS penalty policy. It describes the factors we will normally consider when determining the amount of a financial penalty under the NIS Regulations. There are 5 steps in the penalty policy. This first sets out how we will first identify the applicable penalty category. That is followed by an assessment to identify where the penalty sits within the applicable category. Steps 3 and 4 allow for adjustments based on any relevant aggravation/mitigating factors and deterrence while the final step is there to ensure the overall penalty amount is appropriate and proportionate.

2. Consultation questions

Section summary

We invite respondents' thoughts, where possible with appropriate evidence, on the proposed NIS Enforcement Guidelines and NIS Penalty Policy. We specifically invite responses to the following questions:

Questions:

Question 1:

With respect to the NIS Enforcement Guidelines, are the enforcement procedures for the DGE subsector clearly presented? We invite respondent's views on any aspect of the draft guidelines, including any suggestions for changes or additions.

Question 2:

With respect to the NIS Penalty Policy at Annex 1, are the processes for determining penalties clearly presented? We invite respondent's views on any aspect of the proposed penalty policy, including any suggestions for changes or additions.

3. Context and related publications

3.1. The below documents may assist you with responding to this consultation.

Enforcement Guidelines

- The current Sectoral [Enforcement Guidelines](#), revised in 2017.

Penalty Statement

- The current [Sectoral Penalty Statement](#), published in 2014.

Consultation on changes to Ofgem's Enforcement Guidelines and Sectoral Penalty Statement

- The proposed [updated Sectoral Enforcement Guidelines and Penalty Statement on](#) which we are currently consulting.

BEIS consultation

- BEIS is currently consulting on its [policy guidance for implementation of the Network and Information Systems Regulations](#) for the Energy Sector in Great Britain

Ofgem NIS Policy Guidance

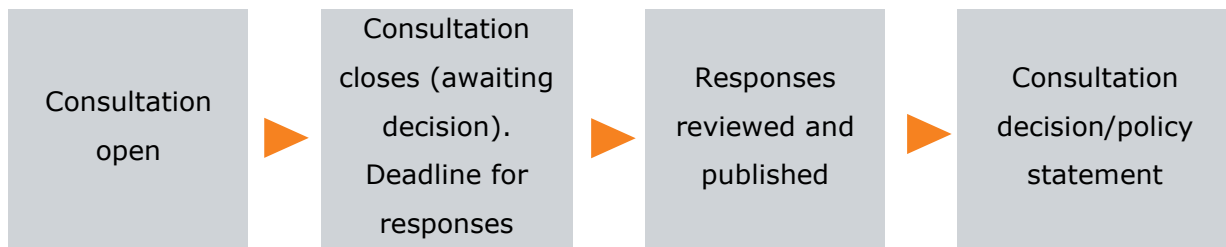
- Ofgem Competent Authority Guidance for Downstream Gas and Electricity in Great Britain; this is Ofgem's current [NIS policy guidance](#)
- There is currently a call for input to receive views on Ofgem's proposed NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in GB which, when finalised, will replace Ofgem's existing NIS policy guidance.

4. Next steps

How to respond

- 4.1. Please send your responses to NISEGconsultation@ofgem.gov.uk on or before 30 November 2021.
- 4.2. If you have any questions about the consultation, please contact us on the above email address.
- 4.3. We want to hear from anyone interested in this consultation. Please send your response to the person or team named on this document's front page.
- 4.4. We may publish non-confidential responses on our website at www.ofgem.gov.uk/consultations. Please note the further information on confidentiality at paragraph 4.5 below.

Consultation stages



Your response, data and confidentiality

- 4.5. Given the sensitive nature of NIS related matters, you may wish to ask us to keep your response, or parts of your response, confidential. We'll respect this, subject to obligations to disclose information, for example, under the Freedom of Information Act 2000, the Environmental Information Regulations 2004, statutory directions, court orders, government regulations or where you give us explicit permission to disclose. If you do want us to keep your response confidential, please clearly mark this on your response and explain why.
- 4.6. If you wish us to keep part of your response confidential, please clearly mark those parts of your response that you *do* wish to be kept confidential and those that you *do not* wish to be kept confidential. Please put the confidential material in a separate appendix to your response. If necessary, we'll get in touch with you to discuss which parts of the

information in your response should be kept confidential, and which can be published. We might ask for reasons why.

4.7. If the information you give in your response contains personal data under the General Data Protection Regulation (Regulation (EU) 2016/679) as retained in domestic law following the UK's withdrawal from the European Union ("UK GDPR"), the Gas and Electricity Markets Authority will be the data controller for the purposes of GDPR. Ofgem uses the information in responses in performing its statutory functions and in accordance with relevant statutory provisions (e.g. section 105 of the Utilities Act 2000). Please refer to our Privacy Notice on consultations, see Appendix 1.

4.8. If you wish to respond confidentially, we'll keep your response itself confidential (subject to the points noted above), but we will publish the number (but not the names) of confidential responses we receive. We won't link responses to respondents if we publish a summary of responses, and we will evaluate each response on its own merits without undermining your right to confidentiality.

General feedback

4.9. We believe that consultation is at the heart of good policy development. We welcome any comments about how we've run this consultation. We'd also like to get your answers to these questions:

1. Do you have any comments about the overall process of this consultation?
2. Do you have any comments about its tone and content?
3. Was it easy to read and understand? Or could it have been better written?
4. Were its conclusions balanced?
5. Did it make reasoned recommendations for improvement?
6. Any further comments?

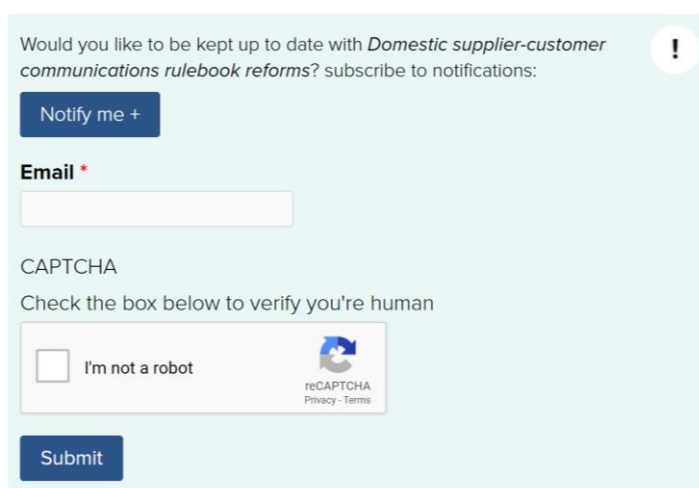
Please send any general feedback comments to stakeholders@ofgem.gov.uk


How to track the progress of the consultation

You can track the progress of a consultation from upcoming to decision status using the 'notify me' function on a consultation page when published on our website.

[Ofgem.gov.uk/consultations](https://www.ofgem.gov.uk/consultations).

Notifications




Would you like to be kept up to date with *Domestic supplier-customer communications rulebook reforms*? subscribe to notifications: 

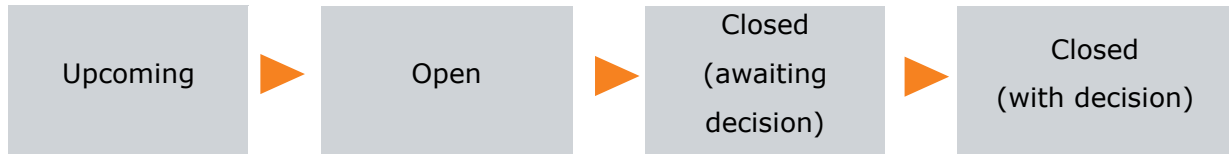
Email *

CAPTCHA

Check the box below to verify you're human

I'm not a robot  reCAPTCHA
Privacy - Terms

Once subscribed to the notifications for a particular consultation, you will receive an email to notify you when it has changed status. Our consultation stages are:



Appendix 1 – Privacy notice on consultations

Personal data

The following explains your rights and gives you the information you are entitled to under UK GDPR.

Note that this section only refers to your personal data (your name address and anything that could be used to identify you personally) not the content of your response to the consultation.

1. The identity of the controller and contact details of our Data Protection Officer

The Gas and Electricity Markets Authority is the controller, (for ease of reference, "Ofgem"). The Data Protection Officer can be contacted at dpo@ofgem.gov.uk

2. Why we are collecting your personal data

Your personal data is being collected as an essential part of the consultation process, so that we can contact you regarding your response and for statistical purposes. We may also use it to contact you about related matters.

3. Our legal basis for processing your personal data

As a public authority, the UK GDPR makes provision for Ofgem to process personal data as necessary for the effective performance of a task carried out in the public interest. i.e. a consultation.

4. With whom we will be sharing your personal data

As we are acting jointly with the Department for Business, Energy and Industrial Strategy (BEIS) as a competent authority for the Downstream Gas and Electricity (DGE) sectors in Great Britain, it may be necessary to share details of consultation responses with BEIS.

5. For how long we will keep your personal data, or criteria used to determine the retention period.

Your personal data will be held for up to one year after the consultation is closed.

6. Your rights

The data we are collecting is your personal data, and you have considerable say over what happens to it. You have the right to:

- know how we use your personal data
- access your personal data

- have personal data corrected if it is inaccurate or incomplete
- ask us to delete personal data when we no longer need it
- ask us to restrict how we process your data
- get your data from us and re-use it across other services
- object to certain ways we use your data
- be safeguarded against risks where decisions based on your data are taken entirely automatically
- tell us if we can share your information with 3rd parties
- tell us your preferred frequency, content and format of our communications with you
- to lodge a complaint with the independent Information Commissioner (ICO) if you think we are not handling your data fairly or in accordance with the law. You can contact the ICO at <https://ico.org.uk/>, or telephone 0303 123 1113.

7. Your personal data will not be sent overseas

8. Your personal data will not be used for any automated decision making.

9. Your personal data will be stored in a secure government IT system.

10. More information For more information on how Ofgem processes your data, click on the link to our "[Ofgem privacy promise](#)".