Consultation

AI Assurance Consultation

Publication date:	18 November 2026
Response deadline:	15 January 2027
Contact:	Jonathan Thurlwell
Lead:	Kerry Sheehan
Team:	Emerging Technologies
Email:	EmergingTechnologies@ofgem.gov.uk

© Crown copyright 2026

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.

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

Foreword **5**

Executive summary **6**

What this is not 6
Alignment and governance 6

1. Introduction **7**

Purpose of this consultation 7
Context and related publications 8
Consultation stages 8
How to respond 8
Your response, data, and confidentiality 9
How to track the progress of a consultation 9

2. Summary of the call for input responses **11**

Overview of engagement 11
What we asked 11
What stakeholders told us 11

3. Proposed approach **14**

Objectives 14
Status 14
Who is it for 14
Guiding Principles 14
Lifecycle approach 14

4. Proposed content of the guidance **15**

Outcome areas 15
Cross-cutting areas 16
Possible guidance inclusions 18

5. Alignment with other initiatives **19**

Sector-relevant rather than AI-specific 20

6. Engagement and governance **21**

Stakeholder engagement 21
Transparency 21
Review and continuous improvement 21

7. Consultation questions **21**

8. Conclusions and next steps 23

Send us your feedback 23

Appendix 1. Privacy policy 24

Personal data 24

Foreword

Great Britain's energy sector is changing, and Artificial Intelligence (AI) is becoming part of how we plan, operate and protect it.

Used well, AI can improve reliability and resilience of the energy sector and help lower costs to consumers. However, used without confidence in what it delivers, AI can put consumers, energy resilience and critical national infrastructure at risk.

Our recent call for input on AI assurance in the energy sector showed strong interest in AI assurance, and in a shared understanding of what good outcomes look like.

Respondents told us they would like information on how to show that their AI systems deliver safe, fair and effective outcomes in practice.

As AI systems become more capable and autonomous, robust assurance will be increasingly important to maintaining trust, resilience and accountability.

This consultation sets out our proposal for good practice, outcomes-based AI assurance guidance for the GB energy sector, in the first instance.

AI assurance guidance would complement our existing guidance on the ethical use of AI in the energy sector and the wider regulatory framework. It would not impose any new requirements, and compliance with the guidance would not in itself constitute regulatory approval. Licensees and regulated persons are reminded that they are required to comply with all applicable regulatory obligations when using AI.

As the use of AI continues to develop, we will keep this guidance under review and will consider whether additional measures may be appropriate in the future.

Our aim is to support responsible AI innovation, build confidence in its use, and protect consumers and the resilience of the energy system.

We invite you to review the proposals and share your views.

Akshay Kaul

Director General for Infrastructure

Executive summary

Ofgem is consulting on proposals for voluntary AI assurance guidance for the energy sector. It focuses on the outcomes AI systems should deliver and highlights how those outcomes are being achieved in practice.

The proposed good practice guidance would complement Ofgem's ethical AI guidance, existing regulatory requirements, and, where applicable, obligations under the Network and Information Systems (NIS) Regulations. It is intended to support organisations in implementing proportionate AI assurance practices alongside existing assurance and reporting requirements, including those that may evolve over time, and does not replace or supersede those obligations.

The proposed guidance would be:

- Organised around outcomes of safe, secure, resilient, reliable and effective, fair for consumers, accountable and governed, transparent and explainable, and environmentally sustainable.
- Proportionate to risk, impact, complexity, including for smaller organisations
- Clear on what good practice can look like for each outcome, without prescribing exact methods.
- Alignment with existing cyber, safety, data protection and consumer protection requirements, and with relevant standards.

What this is not

- Any AI assurance guidance would not introduce new legal or regulatory requirements.
- It does not mean Ofgem approves or endorses any AI system or assurance approach.
- Licensees remain responsible for complying with the regulatory framework and other applicable legislation.

Alignment and governance

The AI assurance guidance would complement Ofgem's AI technical sandbox and AI Reg Lab, as well as wider government and cross-sector work on AI assurance. Evidence from the AI technical sandbox and the AI Reg Lab could inform the AI assurance guidance and any subsequent reviews.

We will engage with stakeholders throughout and publish the outcome of this consultation.

1. Introduction

Artificial intelligence is increasingly being used across Great Britain's energy sector, creating opportunities to improve efficiency, resilience and customer outcomes. As AI adoption grows, organisations should be able to demonstrate, through credible evidence, that their AI systems are safe, secure, fair and effective.

This consultation seeks views on proposed good practice, outcomes-based AI assurance guidance for the energy sector. The guidance would support organisations in adopting proportionate AI assurance practices and complement Ofgem's existing ethical AI guidance and wider regulatory framework. It would not introduce new regulatory requirements, nor would following it constitute regulatory approval.

The proposals are intended to support the safe, secure and responsible deployment of AI, increase confidence in AI governance and assurance, and help ensure that the benefits of AI are delivered for consumers and the wider energy system.

Purpose of this consultation

1.1 AI is increasingly being used across Great Britain's energy sector, from forecasting and network planning to pricing and customer service. As AI use and complexity grows, organisations should assure, with credible evidence, that their AI systems deliver safe, secure, fair and effective outcomes in practice.

1.2 This consultation builds on our call for input on AI assurance in the energy sector, published 17 June 2026. It sets out proposals for voluntary, outcomes-based AI assurance guidance.

1.3 The AI assurance guidance would complement Ofgem's published ethical AI use in the energy sector guidance and the existing regulatory framework. It would introduce no new requirements and following it would not constitute regulatory approval.

1.4 This consultation supports Ofgem's priorities to protect consumers, enable investment and innovation, and maintain a resilient and secure energy system. By promoting the safe, secure and responsible adoption of AI across the energy sector, the proposals aim to increase confidence in the governance and assurance of AI systems while supporting innovation. In turn, this can help ensure that AI delivers positive outcomes for consumers, including more resilient energy services, better customer experiences and a more efficient energy system.

Context and related publications

Context

1.5 The adoption of AI across the energy sector is increasing, bringing both opportunities and new risks. AI assurance is an emerging and evolving field that seeks to provide confidence that AI systems are delivering intended outcomes while managing relevant risks.

1.6 This consultation seeks views on our proposal to develop AI Assurance Guidance for the GB energy sector and seeks stakeholder views on the potential scope, content and application of such guidance.

Related publications

- Ofgem's ethical AI use in the energy sector guidance, 2026
- Ofgem's call for input on AI assurance in the energy sector, 2026
- the government's AI roadmap, 2021
- the government's trusted third-party AI assurance roadmap, 2025
- the government's AI Opportunities Action Plan, 2025
- Information Commissioner's Office's (ICO) guidance, including AI and data protection guidance, 2023
- practical approaches and research developed by the Alan Turing Institute on evidencing and demonstrating trustworthy AI in practice, 2026
- Organisation for Economic Co-operation and Development (OECD) AI Principles, 2024
- AI Standards Hub (AISH), a UK initiative dedicated to the evolving and international field of standardisation for AI technologies

Consultation stages

Stage 1 Consultation open: 18 November 2026

Stage 2 Consultation closes (awaiting decision). Deadline for responses: 11.59pm, 15 January 2027

Stage 3 Responses reviewed and published: March 2027

Stage 4 Consultation decision and final guidance published: March 2027

How to respond

We want to hear from anyone interested in this consultation. Please send your response to EmergingTechnologies@ofgem.gov.uk with the subject line 'AI Assurance Guidance Consultation' by 11.59pm, 15 January 2027.

We have asked for your feedback in each of the questions throughout. Please respond to the consultation questions in section 7 as fully as you can and include evidence examples and case studies where applicable.

We will publish non-confidential responses on our website.

We plan to hold consultation workshops during the consultation. Details will be published on the Ofgem website.

Your response, data, and confidentiality

You can ask us to keep your response, or parts of your response, confidential. We will 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.

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 will contact 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.

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 United Kingdom'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 section 105 of the Utilities Act 2000. Please refer to our Privacy Notice on consultations, see Appendix 1.

If you wish to respond confidentially, we will keep your response confidential, but we will publish the number, but not the names, of confidential responses we receive. We will not 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.

How to track the progress of a consultation

1. Find the web page for the call for input you would like to receive updates on.
2. Click ‘Get emails about this page’, enter your email address and click ‘Submit’.
3. You will receive an email to notify you when it has changed status.

Consultation AI Assurance Consultation

A consultation has three stages: ‘Open’, ‘Closed (awaiting decision)’, and ‘Closed (with decision)’.

2. Summary of the call for input responses

We received 65 responses from a broad range of stakeholders across the energy, technology, cyber security, assurance, academic and consumer sectors. Responses showed strong support for Ofgem providing AI assurance guidance, provided it builds on existing standards, frameworks and industry practices rather than creating a new regulatory regime.

Some stakeholders highlighted that in their individual view AI assurance maturity varies across the sector. Some stakeholders also emphasised the importance of proportionate, risk-based approaches. Respondents stated that assurance should focus on evidence of how AI systems perform in practice, including testing, monitoring, governance and oversight. There was particular support for enhanced assurance where AI is used in critical infrastructure or could have significant impacts on consumers or energy system resilience.

Responses also highlighted the value of external assurance, alignment with emerging standards, and the need to strengthen AI assurance capabilities across industry and at the regulator.

Overview of engagement

2.1 The call for input on AI assurance in the energy sector ran from 17 June 2026 to 12 August 2026. We received 65 responses from a diverse range of stakeholders, including licensees, energy sector participants, operators of essential services, AI developers, AI assurance providers, AI security companies, technology vendors, academics, consumer groups and other experts. This ensured the proposals were informed by both organisations deploying AI within the energy sector and those developing, evaluating and assuring AI technologies.

What we asked

2.2 We asked about current AI assurance practices, risks and challenges, critical infrastructure, consumer protection, cyber security, proportionality, external/independent assurance and standards and future guidance.

What stakeholders told us

Support for AI assurance guidance

2.3 There was broad support for Ofgem providing AI assurance guidance, particularly where it can help organisations navigate emerging risks, improve consistency across the sector, and clarify regulatory expectations. Respondents generally

favoured building on existing frameworks, standards and assurance practices rather than creating a new regime.

Current maturity

2.4 The maturity of AI assurance practices across the sector appears variable. While some organisations have begun incorporating AI into existing assurance, risk and compliance processes, many are still developing approaches to testing, monitoring, auditing and evidencing trustworthy AI performance. Respondents noted that assurance practices will need to evolve alongside increasingly autonomous and complex AI systems.

Practice, evidence and sufficiency

2.5 Respondents emphasised that assurance should focus on evidence of performance in practice rather than solely on documentation or policy compliance. Key forms of evidence include testing and validation results, monitoring and auditing data, incident reporting, decision logs, and demonstration of effective governance and human oversight. Assurance was generally viewed as an ongoing process rather than a point-in-time assessment.

Proportionality

2.6 There was strong support for a risk-based and proportionate approach. Assurance expectations should reflect the risk, autonomy, scale, and potential impact of the AI system, with more rigorous assurance requirements applied to higher-risk use cases. Respondents generally favoured outcomes-based approaches over prescriptive requirements where possible.

Critical infrastructure

2.7 Respondents highlighted the need for enhanced assurance where AI is deployed in critical infrastructure, operational technology environments, or functions that could affect energy system resilience, security, safety, market operations or consumer outcomes. Greater scrutiny, resilience testing and ongoing monitoring were seen as appropriate for these use cases.

External assurance and standards

2.8 Some respondents supported leveraging existing standards, assurance frameworks and independent assessment mechanisms. External assurance was viewed as particularly valuable for higher-risk systems, helping to provide independent challenge, increase trust and improve transparency. Several

respondents noted the importance of interoperability with evolving international standards and regulatory approaches.

Skills and capabilities

2.9 Many responses identified capability and skills gaps as a significant challenge. Organisations require expertise spanning AI, cybersecurity, safety, assurance, governance and risk management. Respondents highlighted the importance of developing internal capability within both industry and regulators, alongside mechanisms for accessing independent technical expertise.

3. Proposed approach

Objectives

3.1 The guidance aims to:

- help organisations build internal capability, confidence and oversight
- support proportionate risk management and good practice
- help organisations communicate AI assurance to stakeholders, including consumers
- support energy sector innovation and responsible AI use.

Status

3.2 Voluntary good practice. The AI assurance guidance would supplement Ofgem's ethical AI guidance, align with existing energy, cyber, safety and consumer protection regulation and does not alter any existing licensee obligations.

3.3 External or independent assurance may support confidence in AI systems, but it does not transfer accountability. Responsibility for ensuring AI systems deliver safe, secure, resilient, fair and effective outcomes remains with the licensee or relevant duty holder.

Who is it for

3.4 Licensees, market participants, operators of essential services and duty holders, with relevance to technology providers, AI developers, assurance professionals and consumer groups.

Guiding Principles

3.5 Proportionality, accountability, energy system safety and resilience, fairness, consumer protection, proportionate transparency, alignment with existing regulation, and a focus on outcomes.

Lifecycle approach

3.6 AI assurance should be proportionate, iterative and continuous throughout the design, development, deployment, operation and retirement of AI systems.

4. Proposed content of the guidance

4.1 We are proposing to develop good practice AI assurance guidance for the energy sector and are seeking views on its scope and content. This consultation does not seek views on the full guidance text. Instead, we are consulting on the areas the guidance should cover and how it can support proportionate and effective AI assurance across the sector.

Outcome areas

4.2 For each outcome, the guidance would set out what the desired outcome means, what credible evidence could look like and what proportionate looks like, outlined in Table 1.

Table 1

Outcome	What it means	Assurance could include
Safe	AI use does not compromise safety-critical operations	System-level testing, integration with operational controls
Secure and resilient	Withstands cyber, operational and AI-specific threats	Adversarial testing, NIS and NCSC alignment, incident records
Reliable and effective	Performs as intended in real conditions	Monitoring, drift detection, performance against objectives
Fair for consumers	Equitable outcomes, including for vulnerable consumers	Impact assessments, outcome monitoring across consumer groups
Accountable and governed	Clear ownership and human oversight	Decision logs, escalation records, senior management/Board reporting
Transparent and explainable	Proportionate to use and audience	Documentation, consumer-facing information
Environmentally sustainable	Sustainable outcomes in practice	Proportionate monitoring and measurement of energy, resource use and relevant lifecycle impacts

Cross-cutting areas

4.3 Stakeholders identified several cross-cutting areas that may influence how organisations adopt, govern and assure AI systems across different uses and organisational contexts. These could include AI supply chains, systemic and concentration risks, standards and assurance frameworks, skills and capabilities, transparency, governance, proportionality and regulatory coordination.

4.4 The cross-cutting themes identify strategic issues that may influence the adoption, governance and assurance of AI across the energy sector. To support implementation in practice, stakeholders may wish to consider whether the AI assurance guidance should include additional material on the following assurance-related topics, which align with and help operationalise those themes.

AI supply chain and dependency assurance:

4.5 Approaches for identifying, managing and obtaining assurance over risks arising from third-party AI supply chains and dependencies, including foundation models, cloud services, data sources and other critical components supporting AI systems, and how organisations obtain assurance where key capabilities are externally provided or operated.

Systemic and concentration risk considerations:

4.6 Consideration of how reliance on common AI technologies, suppliers, models or infrastructure may contribute to systemic vulnerabilities, concentration risks and wider sector impacts.

Standards and interoperability:

4.7 How recognised standards, frameworks and guidance, for example ISO/IEC 42001 and ISO/IEC 23894, can support consistent and proportionate assurance approaches.

Evidence:

4.8 What constitutes credible, reliable and decision-useful outcomes evidence, including the role of internal assurance, independent assurance and operational evidence generated through testing, monitoring and deployment.

Skills and capability for assurance:

4.9 The skills, expertise and organisational capabilities required to undertake, interpret and govern AI assurance activities effectively.

Communication and transparency:

4.10 Approaches for communicating assurance findings, risks and residual uncertainties to boards, senior managers, consumers and other stakeholders in a clear and proportionate manner.

Accountability and governance:

4.11 Clear accountabilities for AI oversight, assurance decisions, risk acceptance, escalation and reporting, including roles for senior management and boards where appropriate.

Regulatory coordination:

4.12 Consideration of how AI assurance activities interact with relevant regulatory requirements, standards and guidance, and how organisations can support consistent compliance across multiple regulatory frameworks.

Proportionality:

4.13 How much outcomes evidence is sufficient for different risk levels, use cases, deployment contexts and organisational functions.

Continuous assurance:

4.14 AI assurance is iterative and ongoing throughout the AI system lifecycle rather than a point-in-time exercise. This could include:

- Monitoring after deployment
- Trigger points for reassessment
- Incident-driven reviews
- Model updates and change management
- Revalidation where operating conditions, data, intended use or risk profiles materially change

Autonomy and oversight:

4.15 Additional assurance considerations for agentic and highly autonomous AI systems, including:

- Human oversight and accountability arrangements
- Intervention and override mechanisms
- Testing of decision-making boundaries and autonomy limits
- Ongoing monitoring and reassessment.

Possible guidance inclusions

4.16 To inform discussion, the following sets out a non-exhaustive list of possible areas for inclusion within the AI Assurance Guidance. Stakeholders are invited to provide views on these proposals and identify any further areas that may warrant consideration:

- illustrative risk tiers and examples of proportionate assurance for different AI use cases
- data assurance, including data quality, provenance, representativeness and data from physical systems and sensors
- testing, evaluation and auditability approaches
- real-time monitoring, ongoing assurance and lifecycle management
- integration with existing safety, security and operational frameworks
- additional considerations for critical infrastructure and operational technology environments
- assurance considerations for procured, third-party and supply-chain AI
- considerations for agentic and highly autonomous AI systems
- incident management, learning and information sharing
- independent assurance and challenge for higher-risk use cases
- organisational skills, capabilities and competencies for AI assurance
- worked examples and case studies demonstrating proportionate assurance approaches.

5. Alignment with other initiatives

5.1 To promote coherence, minimise duplication and support consistent implementation across the sector, any AI Assurance Guidance should seek to align with relevant initiatives, standards, frameworks and guidance, including but not limited to:

- **UK and international AI assurance, standards and governance initiatives:**

  AI assurance guidance should, where appropriate, align with relevant UK and international frameworks, standards, guidance and regulatory initiatives relating to AI assurance, governance, cybersecurity, data protection, competition, testing and evaluation. This includes established and emerging work from recognised standards bodies, technical authorities, regulators and assurance organisations.

  Alignment would promote consistency, interoperability and coherence across the wider AI governance landscape, enabling organisations to build on existing good practice and established assurance approaches rather than creating parallel or duplicative requirements, while helping to identify any material assurance gaps associated with the use of AI in the energy sector.

- **Ofgem Ethical AI Guidance:** Clear alignment should be maintained between Ofgem's ethical AI use in the energy sector guidance and AI assurance guidance, with the two designed to work together as a coherent guidance document to support practical implementation, reduce regulatory burden, avoid duplication, and help enable responsible AI innovation across the energy sector.
- **AI Reg Lab:** The guidance should draw on insights and learning from Ofgem's AI Reg Lab and other Ofgem sandboxes, particularly in areas such as transparency, explainability, fairness, accountability and emerging AI risks.
- **UK government policy:** Alignment should be maintained with the government's AI Opportunities Action Plan, and AI assurance initiatives[1], including Introduction to AI Assurance (DSIT) - foundational UK AI assurance guidance Introduction to AI assurance - GOV.UK and wider AI governance developments to support regulatory coherence and a pro-innovation approach.
- **Data protection and privacy:** The guidance should complement existing Information Commissioner's Office (ICO) AI guidance and data protection, avoiding conflicting expectations and enabling organisations to meet both assurance and data protection requirements efficiently.

[1] Trusted third-party AI assurance roadmap - GOV.UK

- **Cyber security and resilience:** Alignment should be maintained with NCSC's AI security guidance and wider cyber resilience expectations, recognising the importance of secure AI deployment within critical infrastructure and operational environments.
- **Standards, assurance frameworks and international developments:** The guidance should consider existing standards and frameworks, including but not limited to ISO/IEC 42001:2023, ISO/IEC 23894:2023, the UK's AI Principles, and relevant work undertaken by the Alan Turing Institute and other guidance from other regulators, to support consistent, proportionate and risk-based approaches to AI governance and assurance.
- **AI Standards Hub (AISH) resources and standards** AI Standards Hub | The Alan Turing Institute
- **Competition and Markets Authority (CMA):** AI Foundation Models initial review and associated update paper
- **National Physical Laboratory (NPL):** Consideration of NPL's work on AI measurement, testing, evaluation and assurance, including the Centre for AI Measurement, to support the use of scientifically robust approaches to assessing AI systems.
- **Future-proofing:** The guidance should remain adaptable to evolving standards, regulation and technological developments, including increasingly autonomous and agentic AI systems.

Sector-relevant rather than AI-specific

5.2 Consideration should be given to alignment with existing energy sector regulation, engineering assurance practices, safety management systems and relevant HSE approaches to support integration with existing governance and risk management processes, including but not limited to:

- **Cyber Assessment Framework (CAF)** and associated NCSC guidance for critical infrastructure.
- **NIS Regulations** / cyber resilience frameworks where AI is deployed in operational environments.
- Relevant energy-sector digitalisation initiatives and cyber-security requirements.

6. Engagement and governance

Stakeholder engagement

6.1 Opportunities for stakeholders to provide feedback via email and formal consultation responses, alongside stakeholder workshops during the consultation period, to help inform the development and refinement of the guidance.

Transparency

6.2 Publication of non-confidential consultation responses and a summary of consultation findings, including an explanation of how stakeholder feedback has informed the final guidance.

Review and continuous improvement

6.3 A process for periodically reviewing and updating the AI assurance guidance and interwoven ethical AI guidance to ensure they remain aligned with developments in AI technology, energy sector use cases, standards, regulation and the evolving AI assurance profession.

7. Consultation questions

7.1 These questions are not exhaustive. Respondents are welcome to provide views on any other relevant issues/areas.

Questions

Overall approach and assurance outcomes:

Q1. Are the proposed assurance outcomes appropriate and complete? What outcomes are missing, could be combined, or require further clarification?

Evidence, proportionality and risk:

Q2. For each proposed assurance outcome, what forms of evidence would provide the most credible and proportionate basis for demonstrating that the outcome has been achieved in practice?

Q3. How should organisations determine whether assurance activities and evidence are sufficient and proportionate to the risks, impacts, autonomy and intended use of an AI system?

Q4. What examples, use cases or case studies would be most valuable in demonstrating proportionate AI assurance across different risk levels and deployment contexts?

High-risk deployments and critical infrastructure:

Q5. What additional assurance outcomes, controls or assessment methods should apply to AI systems used in critical infrastructure, operational technology environments, safety-critical functions, or other high-impact use cases?

Q6. What assurance expectations should apply where organisations rely on third-party, externally developed, hosted or embedded AI systems and services?

Alignment and practical implementation:

Q7. Would the proposed AI assurance guidance create any issues in terms of its interaction with existing AI guidance, standards and regulatory initiatives? Are there any areas where alignment could be improved, or where duplication, inconsistency or ambiguity may arise?

Q8. Which of the proposed guidance inclusions would be most useful? Is there anything missing that should be included?

Q9. What additional tools, examples, templates or implementation support would assist organisations in adopting the guidance in practice?

Future developments and wider feedback:

Q10. What additional considerations should Ofgem consider for emerging technologies, including agentic AI, increasingly autonomous systems, and evolving AI assurance practices?

Q11. Do you have any other comments on the proposed guidance, consultation process or implementation approach?

8. Conclusions and next steps

- Consultation period: 8 weeks, to include stakeholder workshops.
- Review and analysis of responses
- Consultation decision and final guidance published: March 2027

Send us your feedback

We believe that consultation is at the heart of good policy development. We are keen to receive your comments about this consultation. We would also like to get your answers to these questions:

- Do you have any comments about the quality of this document?
- Do you have any comments about its tone and content?
- Was it easy to read and understand? Or could it have been better written?
- Are its conclusions balanced?
- Did it make reasoned recommendations?
- Do you have any further comments?

Please send your feedback to stakeholders@ofgem.gov.uk

Appendix 1. Privacy policy

Personal data

The following explains your rights and gives you the information you are entitled to under the General Data Protection Regulation (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 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

We will not share your personal data with third parties. See Your response, data, and confidentiality for further information on how we publish responses.

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

We will retain consultation responses for 12 months after work on the subject is complete, after which we will destroy or anonymise data.

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
- 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, view our Ofgem privacy policy.