Making a positive difference for energy consumers

AI Reg Lab: High-level findings for licensees and stakeholders

Publication date: 29 April 2026

AI Reg Lab February 2026

The Ofgem AI Regulation Lab (AI Reg Lab) held on 25 February 2026 brought together an energy sector company and its innovation partner with Ofgem's Emerging Technologies team and independent experts to explore the responsible use of artificial intelligence (AI) in the energy sector.

To support transparency and shared learning, Ofgem committed to publishing findings from each AI Reg Lab engagement.

This AI Reg Lab focused on a pilot AI use in critical national infrastructure (CNI): a generative AI system that would help classify and structure legacy asset data, identify and fill information gaps, including through synthetic data, and build a hierarchical asset model.

The longer-term aim of this AI use is to improve the asset management in support of predictive maintenance and digital twin development, while meeting the safety, security and governance standards that apply to CNI.

The AI Reg Lab sessions surfaced several themes including safety and security, governance, data including synthetic data, and human capabilities.

The AI Reg Lab is a practical exercise that provides energy sector applicants with:

- an opportunity to stress test their hypothetical or real AI uses against our current AI guidance and broader energy regulatory framework
- the chance to explore the potential risks and impacts of their AI use
- a guided discussion of the regulatory implications of the AI use with an independent panel of AI and regulatory experts.

Participation in the AI Reg Lab does not imply regulatory authorisation, nor does it imply Ofgem's endorsement of any AI use. These summary findings have been anonymised for external publication and do not include confidential operational, security, or commercially sensitive information; any examples are generalised and are not attributable to specific organisations, sites, systems, or individuals.

Themes and key findings:

- **AI governance and assurance are critical, including in CNI:** Participants emphasised that AI benefits, such as efficiency, better decision support, and improved asset insight, only become realised once safety and security expectations are demonstrably met. Governance and assurance remain essential across the full AI lifecycle.
- **Security by design needs to extend to AI-specific- threats:**

Participants placed strong emphasis on resilience to cyber threats and adversarial inputs, particularly where 'off the -shelf' or public large language models (LLMs) may be used. It was also highlighted the need to protect both the AI model pipeline and operational systems, and to be clear about how vulnerabilities are identified, tested, and managed when using LLMs.

- **Synthetic data is both a key opportunity and a key risk:**
  Because the AI use could generate or infer missing information, robust criteria are needed to validate synthetic data and safeguard against manipulation. In safety-critical contexts, it was noted that there is a risk of synthetic data introducing safety-critical errors or creating misplaced confidence where the 'truth' of the underlying data quality is uncertain, enhancing the need for validation and other safeguards.
- **Data governance must demonstrate accuracy and traceability:**
  Where AI restructures legacy records and creates new entries, this requires evidence of accuracy, reliability, and traceability, including clear identification and distinguishability between authoritative data and AI--generated inferences. Concerns were also raised -about data leakage and cross-tenant risks in cloud environments, particularly for confidential datasets including energy and geospatial information.
- **Building a robust, consistent understanding of AI system performance is essential:**
  This requires understanding and demonstrating that the AI system performs reliably across diverse asset types and data conditions, including scenarios involving synthetic or incomplete data.
- **Transparency, explainability and auditability are operational requirements:**
  Engineers need to understand how the AI system generates asset classifications, decompositions, and predictions well enough to use them safely. This includes clear rationale, confidence levels, and information on uncertainty, as well as full audit trails and change traceability so users can see what the system changed, why, and how reliable it is likely to be.
- **Human accountability and organisational readiness are critical**:
  Human oversight over decisions must remain intact, with operators empowered and adequately skilled to challenge AI system outputs. The discussions also highlighted practical readiness issues, including skills gaps, governance structures, and knowledge retention where experienced staff hold essential 'corporate memory'.
- **Third-party-dependency risk needs consistent assurance:**
  Use of third-party tools, including cloud-based- LLMs and related components, such as hosting services and vector databases, raises questions about assurance, penetration testing, data location, and sovereignty. It was emphasised that supply chain governance must be clear and consistent if AI is to be deployed safely at scale.

- **Environmental sustainability of AI systems is emerging as a core consideration:**
  Participants noted the need to consider AI energy use and emissions across the lifecycle, from proof of concepts through to scaling the AI use and within associated operations, so that environmental impacts are understood alongside operational value of the AI use.

The themes discussed are being carefully considered as part of regular review of our regulatory approach to AI use in the energy sector, including our AI guidance first published in May 2025.

Safe and responsible AI has significant potential to transform the energy sector and deliver real benefits for consumers. At the same time, it brings risks that must be proactively and carefully managed.

In addition to Ofgem's regulatory oversight role, it is for participants in the AI Reg Lab to ensure their own compliance of their AI uses with any applicable rules, regulations and laws.

These AI Reg Lab findings reflect views expressed by participating parties at the February 2026 Ofgem AI Reg Lab and do not represent the views, policies or regulatory positions of Ofgem. These summary findings do not constitute or imply compliance advice or authorisation, nor do they constitute endorsement of any specific AI systems, technologies or use cases (hypothetical or actual). All AI uses have been anonymised to preserve confidentiality and avoid attribution to any individual or organisation.

Submissions to our AI Reg Labs are accepted on a rolling basis.

We invite licensees, with their innovation partners, if relevant, to submit their AI uses, hypothetical or real, to the AI Reg Lab: Ofgem AI Reg Lab call for submissions | Ofgem

To be considered for participation in the 24 June 2026 AI Reg Lab, submissions must be received by 11.59pm on Friday 29 May 2026.