eurelectric
powering people

Classification of AI systems as high-risk under the AI Act

A Eurelectric consultation response paper

July 2025

Eurelectric represents the interests of the electricity industry in Europe. Our work covers all major issues affecting our sector. Our members represent the electricity industry in over 30 European countries.

We cover the entire industry from electricity generation and markets to distribution networks and customer issues. We also have affiliates active on several other continents and business associates from a wide variety of sectors with a direct interest in the electricity industry.

We stand for

The vision of the European power sector is to enable and sustain:
- A vibrant competitive European economy, reliably powered by clean, carbon-neutral energy
- A smart, energy efficient and truly sustainable society for all citizens of Europe

We are committed to lead a cost-effective energy transition by:

investing in clean power generation and transition-enabling solutions, to reduce emissions and actively pursue efforts to become carbon-neutral well before mid-century, taking into account different starting points and commercial availability of key transition technologies;

transforming the energy system to make it more responsive, resilient and efficient. This includes increased use of renewable energy, digitalisation, demand side response and reinforcement of grids so they can function as platforms and enablers for customers, cities and communities;

accelerating the energy transition in other economic sectors by offering competitive electricity as a transformation tool for transport, heating and industry;

embedding sustainability in all parts of our value chain and take measures to support the transformation of existing assets towards a zero carbon society;

innovating to discover the cutting-edge business models and develop the breakthrough technologies that are indispensable to allow our industry to lead this transition.

Dépôt légal: D/2025/12.105/34

WG Sustainable Network Technology
WG RES & Storage
WG Thermal & Nuclear
WG Hydro

Jessica GARCIA,
Policy Advisor Distribution and Market Facilitation
– jgarcia@eurelectric.org

Consultation response on classification of AI systems as high-risk under the AI Act

A Eurelectric consultation response

July 2025

EXECUTIVE SUMMARY

Eurelectric welcomes the opportunity to respond to the public consultation on high-risk classification under the Artificial Intelligence Act, which entered into force on 1 August 2024. The association has chosen to prioritise section 2 and 4 of the consultation.

Defining safety components

- Limit the "high-risk" definition to AI systems that **directly** impact safety components in electricity supply– and exclude supportive or peripheral algorithms.
- By clearly defining safety component, avoid unintended consequences of a broad interpretation of Art 3(4), which increases compliance without added safety.

Clarify roles and definitions

- Confirm if an entity using a high-risk AI system internally becomes both provider and deployer, and thus responsible for a Fundamental Rights Impact Assessment (FRIA) and other duties.
- Clarify terms like "input data" (Art. 26.4), "putting into service," and "substantial modification."

Reduce administrative burden

- Current documentation and logging demands may invalidate business cases and delay machine learning (ML) model development.
- In practice, compliance could force the shutdown of useful algorithms due to lack of resources.

Section 2.B. Questions in relation to critical infrastructure (Annex III, point 2)

The classification of AI systems as high-risk under Point 2 of Annex III to the AI Act targets AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity. According to Article 3(14), 'safety component' means a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property. The underlying rationale is that the failure or malfunctioning of those safety components mentioned in point 2 may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities (Recital 55).

Point 2 of Annex III therefore covers the following distinct use cases:

- AI systems intended to be used as safety components in the management and operation of critical digital infrastructure.
- AI systems intended to be used as safety components in the management and operation of road traffic.
- AI systems intended to be used as safety components in the management and operation of the supply of water.
- AI systems intended to be used as safety components in the management and operation of the supply of gas.
- AI systems intended to be used as safety components in the management and operation of the supply of heating.
- AI systems intended to be used as safety components in the management and operation of the supply of electricity

Question 10. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems related to critical infrastructure and the use of AI system as safety component.

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3) AI Act.

Name and description of the system	The system is considered high-risk	Motivate your previous answer	The AI system performs profiling of natural person	The AI system meets at least one of the exception criteria of Article 6(3)	Motivate your previous answer and specify any exception criteria that it meets, if applicable
Free text	*Choose:* Yes, completel Partially No Unsure	*Free text*	*Choose:* Yes No Unsure	*Choose:* Yes No Unsure	*Free text*
Classification of emergency calls: The AI system in question evaluates calls and classifies them to dispatch emergency services. For example, if there is a power outage, the AI would triage so the DSO is the first to respond and call emergency services. This functionality improves a function that is today automatised.	No	It is crucial to provide a detailed list of emergency call triage scenarios/areas in the upcoming guidelines on high-risk AI. This should not be considered a security component of a product covered by Union harmonisation legislation listed in Annex I nor does it require a conformity assessment under Article 6(1). While this functionality may appear to relate to the management of critical infrastructure—such as electricity supply—it is important to clarify that this should not be considered a safety component. In this context, it is crucial to distinguish between AI systems that merely assist in triage and those that act as safety components **directly** managing or operating critical infrastructure.	No	Yes	3a) the AI system is intended to perform a narrow procedural task E.g. **Prioritising** emergency calls based on the criticality of the situation.
Autonomous management of smart grids: E.g. Thanks to the ability of algorithms to monitor	Partially	A utility company implements an autonomous management system for its smart grid using artificial intelligence	No	Unsure	3b)the AI system is intended to improve the result of a previously completed human activity.

and manage consumption in real time, smart grids can respond quickly to changes in demand, minimising energy waste and improving the resilience of the electrical system.		(AI). In this context, it is essential to determine whether **certain specific applications** could be considered safety components and would fall within the scope of a safety component under Article 6(2).			3c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review.
Automated trading algorithms (algotrading) as assistant: an AI system which can function as support to energy traders and ensure the market responds quickly to changes in demand, minimising energy waste and improving the resilience of the electrical system. The algorithms allow for the optimisation of energy trading operations, the management of energy asset portfolios, and more accurate price and demand predictions.	No	These algorithms are playing an increasingly important role in wholesale and retail electricity markets as assistant traders. Due to this activity not relating to safety components as defined in Art 6(2), it should not be considered high risk under the AI act.	No	Yes	Even if it would be considered high-risk AI, the application would fall under two derogations: 3b) the AI system is intended to improve the result of a previously completed human activity; 3c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review.
Staff-scheduling AI: If a power sector company uses an algorithm to ensure the proper staffing of wind turbine technicians for operating. By the EU definition one could probably argue that algorithm is used for "management and operation of critical infrastructure".	No	This should not be considered falling under the classification of High risk in art 6, as it does not directly impact the management of operation of critical infrastructure.		Yes	3a) the AI system is intended to perform a narrow procedural task
Predictive Maintenance: For grid operations, image and other sensing technology (such as LiDAR) is used to identify	No	This use case should not fall under the definition of high-risk AI, since a system failure would not	No		

grid components requiring maintenance.		directly contribute to equipment wear. Moreover, this AI system operates alongside other safety measures and technologies, such as redundancy (n-1 strategy in energy distribution), the ability to reroute to alternative infrastructure, and routine human inspections. Typically, the AI system serves to complement and enhance existing safety mechanisms. As it does not introduce new risks, it should not be regarded as a high-risk AI system.			

Question 11. If you need further clarification on the concept of a **safety component** in the management and operation of critical infrastructure in the areas mentioned in *Point 2 of Annex III* to the AI Act, please specify and explain the use case where you need further clarification on.

We welcome further clarification of the concept, as several definitions in the Act diverge. Recital 55 is clearer and more precise than the legally binding Art. 3(14). Key points needing clarification:

1. **Direct/indirect impact.** Safety components should be defined as those **directly impacting** the management and operations of critical infrastructure.

2. Exclude systems **enhancing current safety measures**. For instance, systems that control the activation of fire alarms based on AI pattern recognition can enhance current safety measures. These should be distinguished from other safety mechanisms that might decrease or put into risk safety levels.

3. Define **"large scale risk"** in Art 6(2) and **"significant risk of harm"** in Art 6(3). 'Large scale' could align with thresholds in the CER Directive (Art. 7), matching AI risk to critical entity resilience assessments.

4. Clarify if Recital 55 covers critical digital infrastructure and/or electricity supply. If it means "AND," the reference to 'critical digital infrastructure' in Directive 2022/2557 Annex point 8 excludes the power sector, though it also operates digital infrastructure.

5. Art 8(2) is unclear on how detailed AI/ML governance must be. For example, predicting turbine power output may involve 10–20 algorithms (weather, market, grid, etc.). It's unclear if each must be governed separately or can be managed as one use case. Allowing bundling could ease compliance and speed innovation without affecting safety.

1500 character(s) maximum

Question 13. If you see the need for clarification of the high-risk classification in *Point 2 of Annex III to the AI Act* and its **interplay with other Union or national legislation**, e.g. to Directive (EU) 2022/2555 (NIS2)?, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay.

To ensure the effective implementation of the AI Act, it is crucial to clarify the definition of critical infrastructure, and the high-risk scenarios associated with it, in line with the definitions and sectoral scope outlined in point 1 of the Annex to Directive (EU) 2022/2557. Specifically, it is essential to determine how and when these provisions apply to the energy sector, which is explicitly listed under point 1 ("Energy") of the Directive's Annex. This clarification will help ensure consistent interpretation across Member States and avoid legal uncertainty regarding the classification of AI systems used in the management and operation of energy-related infrastructure.

Moreover, alignment with Directive (EU) 2022/2555 should also be ensured, in order to clearly determine when the applicability of this definition is excluded—specifically in the case of components intended solely for cybersecurity purposes. As Recital 55 states, "components intended to be used solely for cybersecurity purposes should not qualify as safety components." This, together with existing Health and Safety and Data Protection regulations, should serve to standardise and harmonise common requirements, while clearly delineating responsibilities and specific obligations for identifying, assessing and managing high-risk AI scenarios.

1500 character(s) maximum

Section 2.C. Questions in relation to education and vocational training

Question 16. If you see the need for clarification of the high-risk classification in *Point 3 of Annex III to the AI Act* and its **interplay with other Union or national legislation**, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay.

AI systems can be used for professional training purposes during employees' careers, for instance for skills assessment systems based on the processing of personal and sensitive data. This involves a large-scale data processing, that can lead to carrying out a Digital Privacy Impact Assessment (DPIA). In the case of outsourced vocational training programs, the users might face difficulties to comply with this obligation.

Hence, we ask for a clarification on roles when using AI in these contexts. Measures which could facilitate this include:

- A requirement from vocational training institutions on an opt-out option from modules in programs involving High risks AI systems
- Considering the fulfilment of the DPIA as part of the risk assessment requirements by the training institutions

1500 character(s) maximum

Section 4 - Questions in relation to requirements and obligations for high-risk AI systems and value chain obligations

A. Requirements for high-risk AI systems

The AI Act sets mandatory requirements for high-risk AI systems as regards risk management (Article 9), data and data governance (Article 10), technical documentation (Article 11) and record-keeping (Article 12), transparency and the provision of information to deployers (Article 13), human oversight (Article 14), and robustness, accuracy and cybersecurity (Article 15).

Providers are obliged to ensure that their high-risk AI system is compliant with those requirements before it is placed on the market. Harmonised standards will play a key role to provide technical solutions to providers that can voluntarily rely on them to ensure compliance and rely on a presumption of conformity. The Commission has requested the European standardisation organisations CEN and CENELEC to develop standards in support of the AI Act. This work is currently under preparation.

Question 35. Beyond the technical standards under preparation by the European Standardisation Organisations, are there further aspects related to the AI Act's requirements for high-risk AI systems in Articles 9-15 for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

To support effective implementation of the AI Act, clearer guidance is needed on developing Guidelines, Recommendations, and Best Practices, particularly regarding impact assessments and exemptions for high-risk systems (Annex III). A template should be provided for deployers managing both ML and GenAI systems, covering the technical and organisational measures necessary to ensure compliance with the AI system's instructions, including ensuring data is relevant and sufficiently representative for its intended purpose.

Article 9.2(b): Clarification is needed on how to determine "reasonably foreseeable misuse."

Article 9.5: More detail is requested on interpreting "acceptable risk." Should this vary by sector? How should individual risks (e.g. health, safety, fundamental rights) be balanced with systemic risks?

Article 9.8: Clear criteria are needed to define appropriate testing metrics and probabilistic thresholds for high-risk AI systems. What evidence is required to justify their suitability for the intended purpose?

Article 10: Clarification is required on what qualifies as "strictly necessary" for data processing and how providers should document this. Given the diversity of data governance approaches, consistent criteria or references would reduce subjectivity in applying the requirement for training, validation, and testing data to be relevant and sufficiently representative.

Article 15.3 / Recital 74 / Article 15.2: Guidance is requested on how to communicate accuracy levels and related metrics in instructions for use. Are there recommended formats or standard metrics to avoid misunderstandings?

Article 14.1: What constitutes “effective” human oversight? How can this be measured and documented to demonstrate compliance?

Article 12.2(a): More clarity is needed on what counts as a "substantial modification." Can specific examples or criteria be provided?

Article 12.3(a): For systems running continuously or over long periods, how should the start/end time logging be handled? What is the expected level of granularity?

3000 character(s) maximum

Obligations for deployers of high-risk AI systems
Article 3(4) defines a deployer as a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

Deployers of high-risk AI systems have specific responsibilities under the AI Act. Transversally, Article 26 obliges all deployers of high-risk AI systems to:

- Take appropriate technical and organisational measures to ensure that AI systems are used in accordance with the instructions accompanying the AI systems;
- Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support;
- Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system;
- Monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72;
- Keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system of at least six months.

Additionally, Article 26 foresees the following obligations in specific cases:

- For high-risk AI system at the workplace, deployers who are employers shall inform workers’ representatives and the affected workers that they will be subject to the use of the high-risk AI system;
- Specific authorization requirements and restrictions apply to the deployer of a high-risk AI system for post-remote biometric identification for law enforcement purposes;
- Deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system.

Question 37. Are there aspects related to the AI Act’s obligations for providers of high-risk AI systems for which you would seek clarification, for example through guidelines? If so, please elaborate on which specific questions you would seek further clarification.

Clear guidance is needed regarding the requirements and scope of the "quality management system" as set out in Article 17.

1500 character(s) maximum

Question 39. Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems listed in Article 26 for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

Clarification requested on Art. 26(4) – input data and deployer responsibilities

The concept of "input data" in Article 26(4) of the AI Act requires further clarification.

As currently stated, the article suggests that if a deployer has control over any part of the training of a high-risk AI system, they must ensure the input data is "relevant and sufficiently representative" for the intended purpose. This appears to indirectly reference concepts addressed in Article 10, which uses more explicit terms like training, validation, and testing data.

It is unclear whether the deployer's involvement in further training activities would result in a shift in legal responsibility, potentially reclassifying the deployer as a provider due to modifications made post-deployment. This seems to partially reflect Recital 109 but needs explicit clarification. Clear guidance is needed on how to determine when a deployer's activity qualifies as a "substantial modification," and how responsibility is assigned in such cases.

Alternatively, if "input data" refers to the data entered during the regular operation of a high-risk AI system (i.e., to generate outputs), then Article 26(4) would imply that deployers are required to ensure this operational input data is also relevant and sufficiently representative. This would closely align the deployer's obligations with those defined for providers under Article 10, raising questions about the boundaries between the two roles.

Clarifying roles: provider vs. deployer

The AI Act makes a clear distinction between "providers" and "deployers." A provider is defined as any natural or legal person who places an AI system on the market or puts it into service. However, clarification is needed on what exactly constitutes "putting into service" in practice.

For entities that do not develop general-purpose AI models but purchase or access them as services to create specific use cases, it is especially relevant to understand whether they qualify as providers or deployers. Diverging interpretations among AI Pact participants highlight the need for uniform guidance.

Transparency obligations and access to information

The AI Act and the GDPR both impose transparency obligations. However, a gap exists between the information available to providers and deployers. For example, only operating instructions must be shared with deployers— even though technical documentation could strengthen their control and oversight.

Further clarification is requested of the extent to which providers must share system-level information with deployers. It should be specified whether industrial secrecy or confidentiality can justify withholding such information, potentially limiting a deployer's ability to fulfil its obligations under the AI Act.

Outsights definition
We welcome guidelines defining the right level of oversights to implement, based on a scale of the AI systems autonomy. A precise description of the expected oversights would be valuable.

3000 character(s) maximum

Question 40. Are there aspects related to the obligations for deployers of high-risk AI systems listed in Article 26 which require clarification regarding their interplay with other Union legislation?

If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.

Guidance is needed on how AI systems may affect fundamental rights, including a clear list of which specific rights could be impacted and in what ways.

3000 character(s) maximum

Moreover, according to Article 27, deployers of high-risk AI systems that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an **assessment of the impact on fundamental rights** that the use of such system may produce. The AI Office is currently preparing a template that should facilitate compliance with this obligation.

Article 27 specifies that where any of its obligations are already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.

Question 41. Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems for the fundamental rights impact assessment for which you would seek clarification in the template?

Clarification is needed regarding situations in which a legal entity develops a high-risk AI system that falls within the scope of the Fundamental Rights Impact Assessment (FRIA) obligation and subsequently puts this system into service exclusively for its own internal use. In such cases, the entity effectively assumes the dual role of **provider**—by developing and putting the system into service—and **deployer**—by using it under its own authority. It should be explicitly confirmed whether, in this configuration, the legal entity is fully responsible for complying with the obligations assigned to both roles under the AI Act, including the execution of the FRIA.

3000 character(s) maximum

Question 42. In your view, how can complementarity of the fundamental rights impact assessment and the data protection impact assessment be ensured, while avoiding overlaps?

A specific mention to the establishment of Guidelines, Recommendations, and Best Practices for Risk Impact Assessments in AI and Data Protection.

To ensure legal certainty and regulatory consistency, it is essential to develop and adopt clear guidelines, recommendations, and best practices for conducting risk impact assessments in the field of artificial intelligence and data protection. These instruments should be aligned with the provisions of Regulation (EU) 2016/679 (GDPR), particularly regarding Data Protection Impact Assessments (DPIAs), and should provide practical criteria for identifying, evaluating, and mitigating risks to fundamental rights.

Such alignment would help harmonise methodologies across Member States, facilitate compliance for organisations, and ensure that AI systems are assessed under a coherent framework that integrates both AI-specific and data protection obligations.

3000 character(s) maximum

Finally, deployers of high-risk AI systems may have to provide an explanation to an affected person upon their request. This right is granted by Article 86 AI Act to affected persons which are subject to a decision, which is taken on the basis of the output from a high-risk AI system listed in Annex III and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights.

Eurelectric pursues in all its activities the application of the following sustainable development values:

Economic Development

- Growth, added-value, efficiency

Environmental Leadership

- Commitment, innovation, pro-activeness

Social Responsibility

- Transparency, ethics, accountability

Union of the Electricity Industry - Eurelectric aisbl
Boulevard de l'Impératrice, 66 – bte 2 - 1000 Brussels, Belgium
Tel: + 32 2 515 10 00 - VAT: BE 0462 679 112 • www.eurelectric.org
EU Transparency Register number: 4271427696-87