Dear Members of DG CNECT A.2,

Enel SpA, a multinational company in the energy sector, highly appreciates the EC proposal for a regulation aimed to create the conditions for an ecosystem of trust for Artificial Intelligence products and services, on the EU market.

At Enel, we use Artificial Intelligence (AI) to make the energy and power systems more efficient, more predictable and more sustainable, for instance making easier for our business customers to play a more active role in the liberalized energy market.

In Enel's view, to establish a legislative framework which would harmonize rules for placing AI on the European market, within safe and ethical boundaries, the following set of provisions deem consideration and further action:

I. Review of definitions, with focus on requirements for high-risk AI systems (Article 1 to Article 14)

The AI Regulation considers 'high-risk' systems, posing significant risks to the persons, AI systems intended to be used as safety components in the management and operation of critical infrastructures (supply of gas, heating and electricity); **as well as essential private and public services** (Annex III.5). Enel would like to highlight that other legislative dossiers under definition are dealing with similar terms to "essential private and public services" and "critical infrastructures" such as:

- 'essential entities' and **'**operators of essential services' (both proposed at the recast of the NIS Directive),
- 'critical entities' and 'essential services' (proposed in the Directive for Resilience of critical entities)
- 'critical assets' (included at ACER framework guideline for a network code on cybersecurity),
- 'essential business processes' (at the recommendations for a network code on cybersecurity);

The relation of the listed terms with essential private and public services is not clear, and therefore nor obligations for companies in the energy sector. In addition, the lack of an EU common restricted list of infrastructures considered critical, will add uncertainty and bring an inhomogeneous implementation of the Regulation on AI on the energy sector. To avoid possible future imbalances in the application of the AI Regulation (e.g. smart meters could be considered critical infrastructures in a certain number of Member States but not in all), we call the Commission for a EU restricted approach that would enhance clarity, compliance and a level implementation of the Regulation. Moreover, we call the Commission for monitoring for a homogeneous implementation of the AI Regulations in all Member States in order to avoid any difference that could impact on critical services delivery and on related supply chains (that can include cross-border participants).

Hence, Enel believes necessary to better define a concrete methodology to assess what action on a safety component or on an essential service might be considered 'high-risk'. Poor categories and definitions might deter private investments and become a competitive disadvantage to European companies.

Within this view, the different classes of use-cases must be integrated. As an example of a use case related to critical infrastructure which might not be considered of high-risk, predictive maintenance of components might be remarkable.

With the aim of considering the multiple specifities of the energy sector, Enel calls on the Commission to open the work on a methodology for a likely future expansion of the list of high-risk AI systems, to public feedback by means of an open consultation, and take it into consideration before it will be adopted. Furthermore, when updating the list in Annex III by adding high-risk AI systems, Enel considers that the Commission shall take into account the measures for prevention of such risks, among the criteria for the assessment.

Apart from the consideration of what AI systems might be classified as 'high-risk', Enel would like to point out that certain terms at the Regulation require further clarification or an adequate definition:

- **'high-quality'** datasets to test bias: given the crucial function of this definition for the future trust and development on AI, the distinction from what is high-quality from what is not, should be carefully defined.
- **'substantial modifications'** to high-risk AI systems during their life cycle, will require re-certification. To level the AI certifications market and ensure that certain modifications get back on certification schemes in the whole EU, what is a substantial modification should be appropriately defined under the AI Regulation.
- **'unicorn'** should be added to Article 3, given that the definition was settled on 2003 and unicorn was created as definition 10 years later.
- The definition of '**biometric categorisation system'**, to be complete should include more categories such as:
  - physiological: fingerprints, height, weight, colour and size of the iris, retina, outline of the hand, palm of the hand, vascularisation, the shape of the ear, the physiognomy of the face
  - behavioural: the vocal imprint, graphic writing, signature, typing style on the keyboard, body movements
- The definition of a **'publicly accessible space'** and of what is considered **'public security'**, need clarification. By way of illustration, the Regulation leaves unclear if, in case of an attack to an electric network through an AI system, the incident will be categorized as a threat for public security.

II. Cybersecurity requirements (Article 15 and Article 42)

Following the last considerations on public security and cybersecurity, Enel highly encourages the Commission to avoid the development of heterogeneous cyber security requirements, by choosing a unique actor (e.g. ENISA) that will identify and/or will define the adequate cybersecurity standards, to be used for:

- software development, that could positively affect the supply chain, using SSDLC (Secure Software Development Lifecycle) built on the 'security by design' paradigm[1],
- a risk-based delivery of AI service, for which Enel has already adopted similar guidelines; also for critical infrastructure and data protection.

In general, Enel strongly advices that security standards must exclude certifications, and shall be adopted only on a voluntary basis.

In article 42, '*Presumption of conformity with certain requirements*', it is explained that the fulfilment of the measures reported in article 15 are no longer necessary if the product is certified according to the certification defined by (i) '*Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA'* (the European Union Agency for Cybersecurity) and on (ii) *'information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*'. The adoption of certification schemes could become a constraint (nowadays the fulfilment of article 15 and certification schemes are considered alternatives), and if relevant actors opt for a certification scheme such as '*the Common Criteria'* (sponsored by Germany and France) or a similar one. In fact, '*the Common Criteria'* is not only a long, onerous and costly product certification scheme, but it is also very rigid and therefore unsuitable to the rapid evolution of digitalisation. In other words, **indistinctively,** ***a*** **small or** huge functional modification of a product could require a reboot of the certification process, with the consequent impacts.

III. Transparency obligations and codes of conduct (Article 52 and Article 69)

Enel deems fundamental that natural persons will be informed when they are interacting with an AI system. This need is particularly evident in the case of emotion recognition systems, a biometric categorization system, AI systems that generate or manipulate images, audio or video content.

Enel considers paramount to define clearly and list all the categories of AI systems that should be introduced in article 52. To do so, Enel recommends to start with the definition of the impacts aimed to avoid, and later define the measures that should be put in place.

Transparency and explainability are key, while Europe's proactive AI regulation, could also consider new civil liability laws for products that contain AI, aligning liabilities between EU

[1] In the "Strategia nazionale per l'intelligenza artificiale", published last September, the Italian Government promotes an approach by AI technology providers based not only on the principle of ethics by design but also on trustworthiness by governance, capable of ensuring reliability to the entire IA product cycle, both they are static systems (once trained, they are deterministic in their executive phase), and even more in the case of systems with continuous learning and evolution.

Member States to avoid incongruity among the Union. Besides, liabilities should be clarified for each stage of the development life cycle of AI systems:

- at the **learning phase**, there should be a very clear definition of liabilities,' ensuring the data quality minimize the risk of biases. For High-Risk AI systems the learning should be always 'supervised and the **cybersecurity assurance** level should be the highest.
- during **the running phase** there would be new emerging biases, hence it is highly recommended to clarify liabilities for these checks.
- to enhance trust, the **supply chains of high-risk AI systems** should be transparent and contain a clear definition of responsibilities and liabilities.

IV. Support measures for innovation art 53-55

On AI topics we need to foster experimentation and innovation to guarantee always state-of-the-art technologies. To correctly evaluate the goodness of an experimentation, a benchmark with traditional approaches should be provided, just to support reliability and trust of the results. Both the innovative and traditional approach should use the same set of data, validated from a data owner, who is responsible of them and of metadata. Data owner will guarantee data quality and regulate the access to them for the different users.

As last remark, Enel would like to reiterate its support to the Commission proposal on an AI Regulation, representing a fundamental cornerstone of the EU digital strategy aimed to promote human-centred norms and EU standards on the global stage, while ensuring not only the security and resilience of its digital supply chains, but also the delivery of global solutions.

These goals will be achieved by alignment between the various approaches of the Regulation adopted in different Member States, and national policies (e.g. the Italian '*Strategia nazionale per l'intelligenza artificiale*', and the Spanish '*Estrategia Nacional de Inteligencia Artificial*'). Therefore clarification or a single identification methodology for what is considered high-risk AI systems in the energy sector should be established, leading to a more predictable identification and closer alignment of Member States.