Joint declaration on aspects related to the upcoming EU Action Plan on digitalizing the energy sector

As the European Commission stated in March 2020 with the EU industrial strategy[1], Europe must leverage the potential of the digital transformation, which is a key enabler for reaching the Green Deal objectives.
The energy industry, represented by the signatories, recognizes the enabling role of digital technologies for the green transition and **to increase Europe's digital sovereignty**.

On the green transition, the European Commission stepped up the ambition for 2030 when in July 2021, the "Fit for 55 Package" was published. It also escalated its efforts on the digital transition when the European Commission announced last March the Digital Decade Principles. Nevertheless, the link between these two mutually reinforcing transitions should be strengthened.

Hence, **the upcoming Action Plan on** digitalisation **of the energy** sector**, should be the new sectorial EU digital initiative and technological framework enabling trustful and digitally enabled interactions.** For this reason, the energy industry has elaborated key recommendations on the main drivers of digitalisation of the power sector:

Data access, control and sharing leveraged on interoperability

- The upcoming legislation to define an interoperable framework for an easier data access and exchange using harmonized EU standards if no global standards are applicable – stemming from **the interoperability requirements and procedures for access to data of Art. 23/24 of the Electricity Directive – linked to the European Energy Data Space-, shall serve as a reference for data exchange in the energy sector**, to avoid having multiple platforms and rules. A clear data classification schema should be the foundation for defining rules for data sharing, data access and data protection (in terms of cybersecurity and non-personal data) and data quality. An open and transparent process involving all the main stakeholders (aggregators, retailers, generators, DSOs, TSOs, etc) to jointly define **such "data classification schema"**, shall not jeopardize the development of energy services but establish:
  1. which are the **'highly sensitive data'** that shall be exempted from being shared such as: (i) configuration parameters and settings, logs, software levels; (ii) detailed geographical information about the network structure (transmission and distribution level), restoration or system defence plans (Regulation (EU) 2017/2196 establishing a network code on electricity emergency and restoration), contingencies (Regulation (EU) 2017/1485 establishing a guideline on electricity TSO) and, (iii) technical supervision and control data regarding central remote management of end-point devices,
  2. which are the **critical and sensitive data**[2] that require to be aggregated and anonymized due to their impact on critical services supply, on fundamental rights, and on legislative obligations,
  3. which **data can be exchanged without specific data protection measures**, by means of B2B or B2C agreements, in order to develop new businesses and,
  4. which **data that can be considered 'public'** or, can be shared for free or at cost-reflective fee.

[1] European Green Deal for the European Union and its citizens (COM (2019) 640 final)
[2] "Sensitive data" means "commercially sensitive information", not including the particular categories of personal data under Article 9 of the GDPR

- At the same time, the classification schema should define, for each one of the previous types of data, who are the possible data recipients (which public authorities and, private actors)
- **Risk analyses and cost-benefit evaluations based on the data classification schema, will enhance participation in data sharing**, including energy-related data from connected devices. When the data is not sensitive, an easier access to markets data will also be relevant for the deployment of innovative energy services supporting consumers' participation and contribution towards the decarbonisation objectives. Otherwise, these data should be anonymized and aggregated per geographical area, to avoid any malicious purpose.
- **Costs to create a fair data-sharing ecosystem**, such as changing data formats, anonymizing, and assuring the transfer of data **shall be also recognised and allowed to be part of the general remuneration scheme**, in cases of data transfers to any third party. Any extra charge shall be managed at national level, and avoid creating barriers for innovation, or discriminating among different types of market participants.
- Moreover, **targeted incentives should be elaborated to promote the uptake of data-sharing** solutions across the energy system, and for participating in future markets for digital energy services.
- As a general rule, and as recommended in the EU Strategy for Data, to develop competitive markets for digital energy services, **the sharing of privately held data should be done on a voluntary basis** to secure fair competition. Nevertheless, data access obligations shall differentiate between the kind of data and purpose of the sharing.
- Finally, **the drafting of voluntary compensation guidelines involving all impacted actors, shall enhance participation in data-sharing**. The guidelines shall refer to one of the public goals defined by the EU Commission, considering factors such as the size of the company, an index to the market value of the data, energy sector-specific considerations, and the purpose of obtaining the data.

Privacy and Data Protection

- Policy measures are needed to ensure that new markets, products, and services based on energy data are open and competitive, while ensuring data protection, privacy, and cybersecurity. **Privacy rules must allow for greater innovation** and facilitate eligible parties' access to consumer data, provide permission from consumers and respecting security and promoting a privacy by design approach. This will allow the growth of the data economy.
- **The legislation on e-Privacy must be updated to allow for greater innovation**. The current proposal of the Council of the EU on e-Privacy would introduce barriers, first for system operators to provide current and future essential services and secondly, for retailers to encourage consumers' engagement in flexibility services provision and energy markets.
- Utilization rights of the energy industry should be recognized for information of the end-user[3], when it is processed solely for the purpose of performing or improving its services to achieve the policy objectives set out in the European Green Deal. A possible mean to implement this exemption would be including this proposal in the Data Act, instead of the exemption given at Article 11 for use allowance in case data processing did not cause '*significant harm*').

[3] Joint declaration of four EU Associations on serious concerns about the actual proposal for an e-Privacy Regulation: https://cdn.eurelectric.org/media/5297/e-privacy__vdn_signed-2021-030-0232-01-e-h-3F3519C5.pdf

- To increase legal certainty**, legally secure anonymisation, facilitation of data pooling and aggregation principles and standards must be swiftly developed to enable effective data sharing while preserving data privacy and protection.**

Cybersecurity

- **Consistency, harmonization and efficiency among the requirements deriving from the Digitalisation of the Energy Action Plan and from legislation on cybersecurity** (e.g. Cybersecurity Act, Network Codes for cross-border electricity and gas, NIS 2.0, DORA, upcoming rules for connected products and related services at the upcoming Cyber Resilience Act, relevant international guidelines and standards) **need to be ensured while embracing synergies** (incident & information sharing procedures) to enhance the coordination and incident response capabilities, as well as limiting administrative and financial burdens.
- **Create common terminologies for cyber incident reporting**: scope of reporting, thresholds for incidents, reporting timeframe, use of information reported. Generally, legislation should be precise in the security goals entities need to achieve and less prescriptive in the ways of how to achieve them.
- A 'holistic' approach is required both in evaluating the impacts of requirements coming from all legislative acts and the related burdens.
- Regarding certification schemes, we recommend a maturity-based approach with a set of minimum requirements that shall be defined on the European level.
- Ensure stakeholder participation regarding sector-specific standards as well as the definition of "state of the art technology".
- **Where appropriate, products, services, and processes embedded in digital supply chains must be fully compliant with Article 51 of the Cybersecurity Act.** Consequently, these shall be:
    - based on up-to-date software and hardware that do not contain known vulnerabilities,
    - secure by default and by design, and
    - provided with mechanisms for secure updates (reference to e-Privacy updates)

Technological sovereignty

- **To increase the uptake and trust on emerging digital technologies** such as the Internet-of-Things (IoT), cloud services, and Artificial Intelligence (AI) **an enabling regulatory framework is needed**. In this context:
    - The proposed Regulation on AI does not currently include a common definition for infrastructure considered critical and requires a clearer definition of the safety components. Furthermore, the definition of systems considered high-risk, shall be limited to the use-cases with a direct impact on customers.
    - Common codes of conduct for cloud computing service providers and portability rights on data and services, must be considered for reducing the 'vendor lock-in' risks (SWIPO CoC).
    - Increasing connectivity requires further digital infrastructure, which shall contribute to EU climate efforts, and shall lead to more flexibility in the energy sector.
    - **The EU should enhance its critical digital infrastructure promoting the development of multi-country projects and investments such as Industrial Clouds IPCEIs**. Besides, support to actual initiatives such as Gaia-X federated cloud architecture, may support the EU Commission goal to achieve digital sovereignty.