ROUNDTABLE
FOR EUROPE'S ENERGY FUTURE

POSITION PAPERS

Dear reader,

In the following you will find position papers of the Roundtable for Europe’s Energy Future on cyber security and data ownership. We hope you will find it interesting and useful.

The *Roundtable for Europe’s Energy Future* meets twice per year to contribute to the development of an interconnected grid with empowered markets and consumers. The *Roundtable for Europe’s Energy Future* consists of CEOs from leading European energy companies, TSOs and technology providers (Elia Group, MAVIR, National Grid, RTE, Statnett, Statkraft, TenneT, ABB, GE, Amazon Web Services & APG). The *Roundtable* has been functioning since 2011 and is listed in the EU Transparency Register.

The Secretariat of the Roundtable is headed by Tor Eigil Hodne, Director of Statnett EU Office Tor.Hodne@statnett.no. Website: http://www.energy-roundtable.eu

Data ownership

The Roundtable for Europe's Energy Future (REEF), embraces technological developments related to data and is willing to support political discussions on catching up with this fast evolution. Indeed, **customers and companies not dealing with data as their core business must be in a position to be well informed on data ownership and access during their decisions**. On the other hand, the **companies building business and developing technologies based on the confidentiality, integrity and availability of data also need investment security** because of possible later unauthorised disclosure, loss of integrity and/or non-availability of data. Therefore, data ownership, confidentiality, integrity and availability need to be clarified and future-proof.

The concept of '**data ownership**' is far less controversial for companies **than access to and the (re-)use of data**. Today, access and re-usage of data **is managed via contractual law**. The REEF recommends to **strengthen this concept with a Code of Conduct** for the Industry to create a common market standard. The GDPR names Code of Conducts as an adequate instrument. **Non-legislative measures** (and especially cross-sectoral non-legislative measures) are to be **preferred at this stage** of the development of the markets. This would help clarifying for instance:

- Where the border lies between data, set of data and a complete service based on a given database.
- Whether there is a single owner of smart meter data of several million meters, or if the individual customers are the owner of their own data, and thus every other player in the value chain are only parties who request access to the database.
- How data is treated in smart grids with and IoT devices which are not interacting with consumers whatsoever and only handle machine-to-machine-data.
- The opportunities of AI: Machine Learning and Cloud Infrastructures can help for a better, more efficient and stable grid for Europe whist integrating renewable energy.

The Roundtable would therefore welcome a self-regulation body, whose work could then eventually translate into binding rules at EU level. **It must, and will eventually be regulated clearly who has access to which level of aggregation and detail; not to endanger private integrity of individuals, but so as to provide opportunities for data analytics, competitors and possible service providers**.

On the other hand, **for the effective functioning of the electricity industry it is mission critical that the companies responsible for the secure operation of the grid can base their decisions on the highest level of certainty** about the actual, historical and possible future state of the grid. For this purpose access to data is inevitably necessary. Access to data needs to fulfill three functions and keep the balance between them:

1) **Entry barriers** to the market should be **kept low** to make use of the efficiency of competition

2) **Open access** to data can lead to tremendous **innovation gains and can stimulate private investments**

3) **Protect IP rights** and give infrastructure grid provider the ability to utilise their data for smart services, new business models and better customer orientation at all levels.

Minimum requirements on confidentiality, integrity and privacy - as per GDPR - and higher security standards should also be enforced.

In that regards, the **REEF invites the European Commission to continue its efforts to remove existing barriers to the free flow of data and create the right framework for secure and competitive data access and transfer in the power sector**. This could be inspired for instance from the Standards & Interoperability Working Group on Data Format & Procedures of the Smart Grid Task Force.

REEF proposals on Cybersecurity

The Roundtable for Europe's Energy Future (REEF) welcomes the release of the Cyber security Package proposed by the European Commission last September 2017. **Cybersecurity is of utmost importance for energy companies** which operate or contribute to the operation of the European power infrastructure, the backbone of all economic activities and thus a critical European infrastructure. In an increasingly connected world, **the cyber risk is growing and evolving**. It is of utmost urgency that the energy sector properly **anticipates and is equipped** with the means to rapidly react to cyber-attacks in order to protect our economies and our fellow citizens. The Commission's proposals in the Cybersecurity Package go in the right direction in this regard. However, the Roundtable would like to make the following remarks:

- **the regulation should also cover all actors that send data to TSOs and DSOs (such as RES producers, aggregators etc.), as well as all connected objects energy companies work with.** The increasing numbers of distributed resources and connected devices that can interact with the power system as well as bi-directional energy flows mean indeed a much stronger interdependency among market players in terms of cybersecurity. The **quality and security of these actors and objects is very much necessary** as well. If they send corrupted data, they would cause serious malfunctions to the electrical system.

- the REEF also recommends that the voluntary European certification proposed by the EC, instead of replacing the national existing certification schemes for ITC products, processes and services **would set minimum requirements and be complementary to national schemes**. The REEF considers this ongoing harmonisation process, which should help less advanced Member States to reach a common European level of security, with the result of upgrading the protection of all Member States against cyber-attacks, as very positive. However, this harmonisation should not lead to a decrease in the cybersecurity performance already reached in some EU Member-States thanks to their own national cybersecurity Agencies, but should allow for the development of higher standards in parallel, in order to push progressively Europe towards more advanced cybersecurity levels.

- the REEF also considers that the European certification **shall be made mandatory for ICT products, processes and services linked to the <u>operation</u> of the electricity grid,** in order to guaranty the integrity and availability of those critical infrastructures and then adequately protect national economy, public security and sovereignty. As operators of essential services, Transmission System Operators abide by a set of security rules **for the most crucial part of their information system** such as the supervision and control of the power grid. To ensure their cybersecurity in a context where they are strongly reliant on other players, it is key that these rules apply also to ICT products, processes and services linked to the operation of the electricity grid. As a condition to reap the benefits of this mandatory certification, processes should be included as well in the scope of the text for this part of the information system **linked to the <u>operation</u> of the electricity grid**. As a matter of fact, our most critical elements are not stand-alone and the related risks may be mitigated or increased depending if the appropriate process is implemented or not.

- such a European certification should be industry-driven and process-oriented and based on existing and proven high-level security schemes. For digital products and services, they shall be built and designed to meet rigorous compliance standards such as ISO 27001, ISO 9001, ISO 27017, ISO 27018, SOC 1, SOC 2, and Payment Card Industry Data Security Standard (PCI DSS) Level 1. It is important that governments leverage such accreditations so that they can benefit from an efficient and fast compliance process.

- the REEF welcomes also the EC proposal that the EU Cybersecurity Agency would be in charge of organizing yearly pan-European cybersecurity exercise and ensuring better sharing of threat intelligence and knowledge (introduced by the draft revised NIS Directive in April 2018). Strong technical expertise and organisational measures have been developed to reduce vulnerabilities to cyber-attack and security is now more and more integrated from the design phase of architectures and applications. However, **cybersecurity is as much about behavior and controls as it is about technology, certifications or notification**. Managing cyber risk requires also a multidisciplinary approach, beyond technical and digital processing. **Attack simulations need then to be organised both at national and European level to test companies and Member States' reactions in case of massive cyber-attacks**, in parallel to national exercises. Leading National Cybersecurity Agency should be involved in such exercices.

- the REEF welcomes the testing of the cyber resilence of IT products, services and processes to assess the resistance of the security functionalities against cyber-attacks. However, an evaluation method based on effectiveness test is risky, as a successful test could endanger the European electricity system, possibly resulting in a black-out. The REEF also recommends conducting tests in quasi-real situations on testing platforms. This evaluation method will be as effective and much less dangerous for the electricity system.
Better sharing of threat intelligence and knowledge should also be organized, so that that Members States can learn from the experiences of cyber incidents from other Member States.

- cybersecurity risk management should also be based on data classification in order to adapt controls to the sensitivity and business impact of the data. Data classification involves identifying the types of data that are being processed and stored in an information system owned or operated by an organisation. It also involves making a determination on the sensitivity of the data and the likely impact arising from compromise, loss, or misuse.

Data classification has been used for decades to help organisations safeguard sensitive or critical data with appropriate levels of protection. Regardless of whether data is processed or stored in traditional on-premises systems or the cloud, **data classification is a starting point for maintaining the integrity and availability of data** based on the data's risk impact level. Data classification allows organisations to think about data based on sensitivity and business impact, which then helps the organisation assess risks associated with different types of data. Reputable standards organisations, such as the **International Standards Organisation (ISO) and the National Institute of Standards and Technology (NIST), recommend data classification schemes so that information can be more effectively managed and secured according to its relative risk and criticality, advising against practices that treat all data equally**. Each data classification level should be associated with a baseline set of security controls that provide appropriate protection against vulnerabilities, threats, and risks commensurate with the designated protection level. As a first practical step, the REEF recommends the EU to trigger the initiative of data classification in order to reach a 80% vs 20% of data that would actually really need to be regulated. That regulation would not only tackle end-customer but also B to B environment.