The European Association of the Electricity Transmission and Distribution Equipment and Services Industry

POSITION PAPER

3 November 2022

T&D Europe comments on the EU Data Act legislative proposal

T&D Europe, the European Association of the Electricity Transmission and Distribution Equipment and Services Industry, would like to use this opportunity to raise our concerns on the EU Data Act, as it impacts our current and future service business based on IoT.

Key points:

1. The Data Act assumes that the IOT asset provider is the data holder. The **assumption "manufacturer = data holder" fails to reflect the realities of our industry. It is overly simplified.** In the B2B space, unlike the B2C space, the "**user**" of the physical asset typically is the "data holder" and not the manufacturer.

2. **Access to data / data sharing stipulations of the Data Act are too broad, too vague** and/ or regulate aspects of business that so far were governed by contractual and entrepreneurial freedom. Additionally, the **protection of trade secrets, intellectual property (IP) and cricital infrastructure** must be ensured.

3. **The Data Act introduces far-reaching obligations** (access by design, making data available free of charge to data users and third parties) to the manufacturers of connected products as the "data holders, which seem unreasonable, unbalanced, and potentially incur costs.

4. **Data Act offers only ambiguity and vagueness** where precise definitions and classifications are urgently needed.

Data will play an ever-increasing role in the energy sector

Therefore, it is important to get the Data Act right. Unfortunately, the proposal of the Data Act falls short. It **fails to reflect current industrial realities**, potentially endangering the aspirations of the Data Act and threatening the global competitiveness of the EU industry.

T&D Europe aisbl
BluePoint Building
Boulevard A. Reyers 80
1030 Brussels - Belgium
+32 2 206 68 67
secretariat@tdeurope.eu
www.tdeurope.eu
T&D Europe is registered under
the European Union 'Transparency Register'
ID number 90453504235-64 **VAT** BE 0898 208 617

Data Act Misses Industrial Realities:

1. The Data Act assumes that the IOT asset provider is the data holder. The **assumption "manufacturer = data holder" fails to reflect the realities of our industry. It is overly simplified.** In the B2B space, unlike the B2C space, the "**user**" of the physical asset typically is the "data holder" and not the manufacturer.

   Even if all primary and secondary components and the software service are being provided by one corporation (manufacturer and software service provider), this corporation is not allowed to access customers' data without a contractual agreement

   > **Example:** A manufacturer sells equipment to a corporation - his customer. The manufacturer subsequently enters a (service) contract to support this customer in optimizing and increasing the efficiency of the operation / process. To provide this service the customer and manufacturer enter a bilateral agreement that not only specifies the service but also which process / operational data the customer will make available to the manufacturer. The customer trusts the manufacturer to work in his core process / operation. Reducing processing times by a split second saves a lot of money for the customer in his manufacturing process. This is the IP of the customer and the manufacturer; it is a competitive advantage that needs to be protected!

   Industrial reality: T&D manufacturers and their customers enter contractual agreements, including public tenders, which govern the sharing of data.

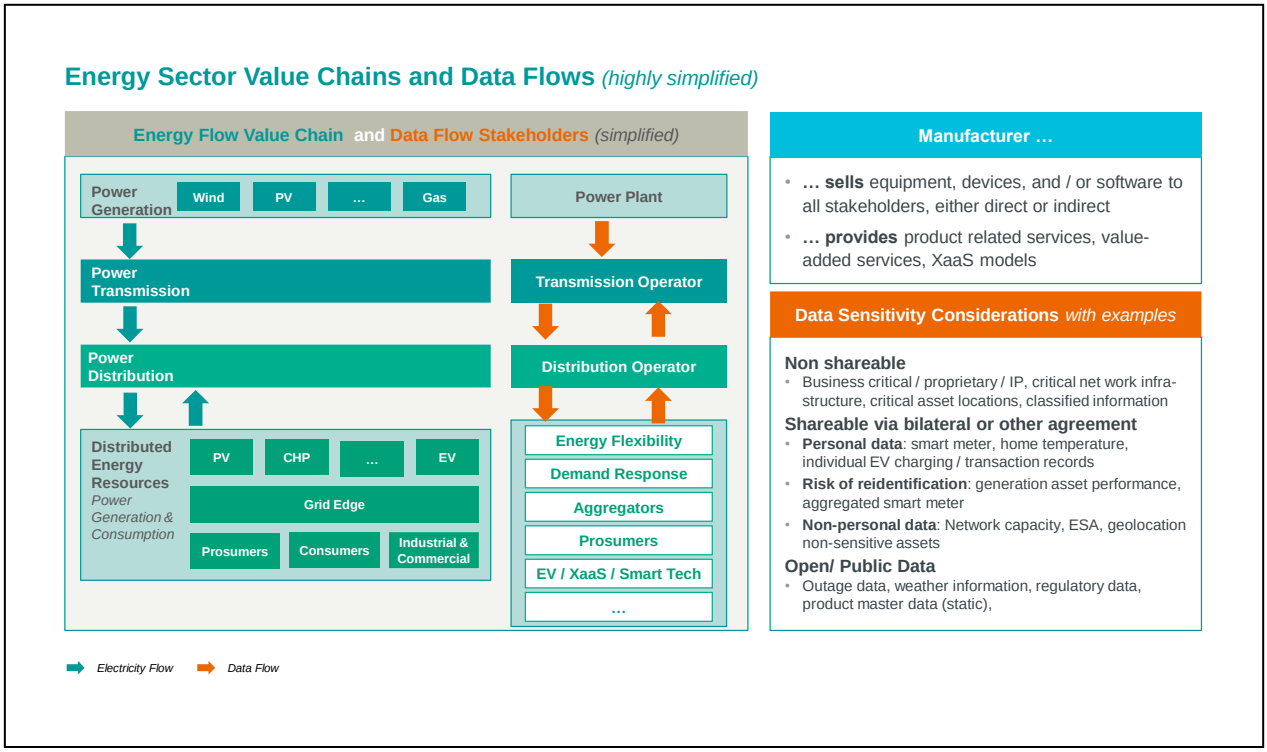
   - Specifies the type of data, who should handle it, and wo can have access.
   - Ensures fulfilment of all legal requirements, incl. protection of IP and trade secrets.
   - Framework to protect critical infrastructure or cover international data flows.

   The proposal for the **Data Act over-simplifies and misstates the relationship between the T&D manufacturers and the customers**. Complex industrial value chains are neither reflected nor considered in the proposal for the Data Act. Industrial data relationships are much more complex than anything in a B2C environment.

   Especially in the **energy sector** the environment is highly complex, as the simplified graphic below outlines. Basically, 3 different levels of data sensitivity and sharing rules apply:

   - Electrical Grid - critical infrastructure

- Industry (heavy, process), Infrastructure/Commercial Buildings - B2B approach
- Household level - B2C approach



2. **Access to data / data sharing stipulations of the Data Act are too broad, too vague** and/ or regulate aspects of business that so far were governed by contractual and entrepreneurial freedom. Additionally, the **protection of trade secrets, IP and cricital infrastructure** must be ensured.

   We believe that it is **excessive** that a manufacturer who does not hold the data is required to share all data, whereas the user / operator / service provider, i.e. the stakeholder who actually holds the data is not required to share data. The Data Act does not include any stipulations where the data holder must share back data with the manufacturer, who also has legitimate interests.

   Data sharing does not come for free. Furthermore, all data sharing requirements must consider data sensitivity and must comply with potentially conflicting considerations, such

as the need to protect critical infrastructure (considerations of energy security), the General Data Protection Regulation (GDPR), as well as the need to protect intellectual property and trade secrets. Some of the shared data could give insights into the design of primary assets and disclose manufacturers' know-how.

3. **The Data Act introduces far-reaching obligations** (access by design, making data available free of charge to data users and third parties) to the manufacturers of connected products that seem unreasonable, unbalanced, and potentially incur costs.

   Smart devices do not come for free. Additionally, upgrading already installed connected devices incurs significant cost and burden. This is unrealistic and not economical.

   - Impact to potential new fields of business for growth: If SaaS offerings are inside the scope of the Data Act, it creates legal uncertainty for businesses.
   - The provision that customers can switch service providers with only 30 days' notice ignores current contractual realities in B2B transactions.
   - Lacking an opportunity to recover investment via new service models, because data must be shared free of charge, could undermine the willingness to innovate.

   To summarize: If forced to share the data under these conditions, manufacturers may avoid generating this data to protect their IP / know how.

4. **The Data Act proposal creates more ambiguity and vagueness** where precise definitions are urgently needed:

   - **Data holder concept** is misunderstood and not specified. Need clarification: data holders versus users. "Data processors" or "data operators of data spaces"?
   - **Data does not equal data**, which makes these discussions so difficult and conflicting. The Data Act does not make any distinctions and misses an opportunity to provide clarity.
   - Need clear **definitions / distinction between shareable data** and **non-shareable data,** between highly sensitive, security, business or personal critical data (data around critical infrastructure or data that constitute IP or trade secrets), data that require sharing consent, and shareable, open data. The lack of clear definitions /

data sensitivity categories results in lots of new expressions and word creations. These do not facilitate the process of delivering on the aspiration.

- SaaS models must be out of scope.
- The definition of Product does not take into account software as a product, it considers it just a related service.
- The Data Act does not specify whether provisions under Switching Between Data Processing Services would force manufacturers to use a cloud agnostic architecture. If so, this could have a huge impact on developing cloud offerings.

In its current form the proposal for the Data Act misses an opportunity, which could potentially jeopardize the objectives of the Data Act in fostering a data economy.

Industrial realities and industrial data flows must be acknowledged, respected, and incorporated in the overall aspirations of the Data Act. B2B is not B2C!

Below is more detailed input on the following chapters:

Chapter I. General Provisions

Article 2 – Definitions

1) Data: The definition of "data" is quite wide and rather vague. The proposal does not consider that data generated by the use of or incorporated in industrial machinery may differ in terms of their degree of maturity/processing (raw data vs. analysed or processed data).

2) Product

It's unclear which physical asset components (e.g., sensors) fall under the definition of a product, especially in light of the accompanying Recitals 14 and 15.

Software should be included in the definition of standalone product and not just related service.

3) Related service

The definition should focus on service being essential for a product's "basic function" rather than "a function". It does not contain a clear demarcation between related services and stand-alone software.

5) User & 6) Data holder

The proposal reflects an over-simplified picture of the relationship between T&D Europe manufacturers and customers. The "user" of a physical asset is regularly the "data holder". The proposal states in its Explanatory Memorandum that *"the manufacturer or designer of a product or related service typically has exclusive control over the use of data generated by the use of a product or related service"* (p. 13). This is, however, not true for the T&D sector. The formula "manufacturer = data holder" fails to reflect the realities in our industry. Rather, the user typically is the data holder.

A more precise definition of the "data holder" [cf. Art. 2 (6)] is required as the one who de facto holds the data, pointing out that in the vast majority of industrial use cases this role is simultaneously with the user of the component in question.

The definition should take into account that the Client (the user and data holder) might be in itself providing a service with the Product, therefore, there are other levels of users.

The proposal also does not provide definitions of the terms "manufacturer" and "service provider", although they will be equally covered by the scope of the EU Data Act, Art. 1 (2) (a).

Chapter II. B2C and B2B data sharing

There is no clear distinction between B2C and B2B applications.

Service providers will benefit from data access rights while product manufacturers will not have similar rights, which will distort the competition and market balance. There is a lack of consideration for loss of competitive advantage as a result of (non-European) competitors benefiting from data access through the Data Act without reciprocal rights.

The Act could also undermine the service providers' business if they are required to disclose data free of charge to the user, because they will not be able to monetise their investments. This would jeopardize the objectives of the proposal to promote investments in innovations and the development of digital services.

Electrical components follow a very specific design that must meet the special requirements in the industry sector. Modifications to the product design may significantly jeopardize the product's functionalities. The provisions in Article 3 on access by design sound very impractical, vague, and too broad. Products can often produce more data than required for regular usage, but this requires investments that must be protected. To make it “easily, securely and directly accessible” to all users, extra effort during the development process is required, which makes products more expensive and may lead to problems regarding functional safety and security in many industrial applications.

Trade Secrets (Article 4.3)

Trade secrets need to be fully protected, and data considered as trade secrets should remain outside the scope (important to foster investments and innovation regarding generation and processing of data). It is essential that trade secrets are not disclosed to third parties.

The protection should not only cover trade secrets but also safeguard machine builders / component providers – often SMEs – from having to disclose data that allows conclusions on core domain know of their applications (algorithms, machine configurations). Under other circumstances such highly confidential know-how would also not be made available to market participants.

The provisions in Article 5 on sharing data with 3rd parties need to be strictly limited as data sets may include proprietary IP and trade secrets that must not be disclosed to 3rd parties.

Data holders should be able to claim damages for data misuse, e.g., for developing a competing product (mere deletion of the data is not sufficient).

Chapter III. Obligations for Data Holders

In Article 9, the notion “free of charge” data access must be clarified. It must also be clarified who will determine what constitutes reasonable compensation.

Chapter V. B2G data sharing

The data provision obligations to the public sector in this chapter are unclear and potentially very broad (Art. 14), while compensation mechanisms need to be clarified (Art. 20).

Chapter VI. Switching between data processing services

The current definition is too broad. SaaS applications should be excluded from the scope of the Data Act as this would prevent many business models.

Obligations to have a maximum termination period of 30 days to transfer all data to a competing service provider would considerably weaken the competitiveness of European cloud service offerings. The combination of easy switchability and short-term customer contracts reduces investment incentives.

Furthermore, it is unclear whether the provisions here would de facto force us to use a cloud agnostic architecture. If so, this could have a huge impact on developing cloud offerings.

Chapter VII. International contexts non-personal data safeguards

The chapter creates additional hurdles for seamless data flows and needs to be evaluated in detail.

Chapter VIII. Interoperability

This chapter lacks references to existing proven interoperability standards. Preference should be given to internationally recognized and proven standards which are industry-driven and sector-specific.

For further details, please read our suggestion for amendments to specific articles of the legislative proposal's text.