Brussels, September 3rd 2021

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Transparency-Register-ID:
20457441380-38

Additional Remarks

To the European Commission's public consultation on the Data Act and the amended rules on the legal protection of databases

Transparency-Register-ID: 20457441380-38

The German Association of Energy and Water Industries (BDEW) and its regional organisations represent over 1,900 companies. The membership comprises both privately and publicly owned companies at the local, regional and national level. They account for around 90 percent of the electricity production, over 60 percent of local and district heating supply, 90 percent of natural gas, over 90 percent of energy networks and 80 percent of drinking water extraction as well as around a third of wastewater disposal in Germany.

General Remarks

BDEW welcomes the European Commission's intention to adopt a regulation that supports the creation of a fair data economy by ensuring access to as well as use of data, including the sharing of data in B2B and B2G cases, thereby complementing the proposal for a regulation on data governance. Setting clear standards and rules for data provision, data transfer and data use at European level is of utmost importance as data traffic multiplies with the increasing number of digitalization initiatives throughout the European Union. Such initiatives and their respective data can contribute to the achievement of the goals of both the EU's Digital Decade and the European Green Deal. The energy and water sectors contribute to making these targets a reality and therefore also welcome the European Commission's aim to provide guidance for data transfer. This can help to further harmonize data-related activities, where appropriate, and assures that those activities adhere to equal, fair, and transparent standards, terms, and conditions.

Nevertheless, there are sector-specific differences between the Member States which should be taken into account in the Data Act. Consequently, where relevant among the wide range of issues dealt with in the proposal, a directive would offer more freedom to the Member States in the implementation of the act and is preferable over a regulation.

Moreover, data transfer often comprises sectors-specific features rendering a one-size-fits-all approach disproportionate. In general, BDEW welcomes the broad scope of the current consultation, touching upon B2G- and B2B-data sharing to evaluation of smart contracts, IoT-data, cloud services, portability rights, protection of databases and safeguards for non-personal data in international contexts. However, from BDEW's point of view it should be clarified which data the Commission exactly seeks to include in the scope of the regulatory requirements. In doing so, sector-specific circumstances of utility companies – as for example the companies' responsibility to ensure security of supply and the consequent need to protect certain data concerning business secrets or critical infrastructure data as well as the fact that private utility companies can also feature municipal stakeholders which necessarily lets them act on a public and private level at the same time – should be taken into account already at an early stage.

As the European Commission already proposed multiple data related initiatives as part of the Digital Decade (Data strategy, Data Governance Act, Artificial Intelligence Act, revision of the Broadband Cost Reduction Directive, revision of the INSPIRE Directive, HighValueData Act as well as the upcoming proposals for sector-specific data spaces), BDEW asks the Commission to clarify the interaction of these initiatives. The consultation questionnaire for the Data Act refers explicitly only to the data strategy and the Data Governance Act. From BDEW's point of view, coherence between all acts and initiatives has to be guaranteed.

In the following position paper, BDEW would like to make some additional remarks to the consultation which should be taken into account for the proposal of the Data Act.

On part I: Business-to-government data sharing for the public interest

According to the European Commission, access to private sector data can provide public authorities in the EU with valuable insights, for example to improve public transport, make cities greener, tackle epidemics, and develop more evidence-based policies. Therefore, the Commission aims to create a framework to bring certainty to business-to-government (B2G) data sharing for the public interest and help overcome the related barriers. In this context, it remains open how frequently such data can be accessed, in what ways third parties might gain access to the shared data, and in what format data has to be provided.

On question 4: Regarding compulsory data sharing between businesses and public authorities

In principle, we support mandatory B2G data sharing in emergency situations, for crisis management, official statistics, protecting the environment, and a healthier society. Nevertheless, data concerning critical infrastructures and competition-relevant data should be excluded from any mandatory obligation of data sharing as the protection of critical infrastructures is a goal in itself and must not be endangered through extensive open data obligations. Requirements to provide information and data must not lead to a deterioration of the resilience of critical infrastructures. Some data provision obligations already pose a risk on security of critical infrastructures. Therefore, it is of great importance that data that companies are obliged to deliver to public authorities remains inaccessible to third parties. Moreover, any form of data sharing obligation should not result in extended responsibilities for data collection or reporting. Further, the duplication of legal requirements for the sharing of data, especially of data already covered by other European legislation (such as environmental data), should be avoided.

On question 6: Regarding safeguards for B2G data sharing

In addition to the measures proposed in the consultation questionnaire, a timely feedback from public authorities concerning the underlying reasons why a specific data set was requested would be beneficial. Currently in most cases businesses have to deliver large amounts of data without knowing exactly for what reason data was requested and how public authorities further use the requested data. Reporting obligations concerning the use of data should therefore be mandatory for both businesses and public authorities.

Generally, data of critical infrastructures should not be requested. If absolutely needed, this data should be protected by extra safeguards (such as timely destruction and justification).

On part II: Business-to-business data sharing

The European Data Strategy already intended to promote business-to-business (B2B) data sharing, especially in order to benefit start-ups and SMEs, putting emphasis on facilitating B2B voluntary data sharing based on contracts. In the context of the Data Act, the Commission is seeking solutions to promote fairness in contracts governing access to and use of data.

Since data provides the basis for the development of new digital business applications, we welcome the Commission's aim to enhance fairness of data sharing und using. Aside from data shared voluntarily between businesses, the energy and water sectors are subject to many legal obligations to give other companies access to data. In general, these obligations should not be extended and voluntary data sharing on the basis of bilateral contracts should primarily be promoted.

With regard to the objective of facilitating B2B data sharing, it still remains to be clarified in how far meta-data is affected and thereby disclosed in the data sharing process.

On question 9: Regarding the types of companies and of data shared in B2B cases

Usually, data is shared with other companies as part of a legal obligation; this pertains to data for intra-market communication (e. g. customer switching processes, billing processes for electricity or gas etc.), planning data, redispatch processes, geodata, generation and load data provision, transparency requirements for grid operators resulting from tariff/cost regulation. Typically, the companies' data is shared either directly with other companies, for example seeking to co-deploy public utility infrastructures or telecommunication lines, or indirectly via Single Information Points (Geodata platforms, such as the "Infrastrukturatlas" etc.) which are publicly accessible.

On question 10: Regarding services and products based on data sharing existing or under development in our sectors and the data required for them

Data provides the basis for numerous digital business cases within the energy and water sectors. With the rising share of volatile renewable energy in the energy system, more data about energy generation and consumption needs to be analysed and managed. Therefore, digital tools for energy data management are of great importance.

Artificial intelligence applications are also based on data sharing and are, for instance, used within the areas of plant design; maintenance, servicing and plant management; network management as well as energy trading, sales and customer interface. In addition to that, specific services and tools for support of infrastructure planning have been developed on the basis of, among other inputs, publicly available infrastructure data gathered in mainly local and national geodata platforms. Also, services based on data sharing in the context of smart city

projects e. g. about charging stations for electric vehicles etc. have been developed and still are under development.

On part III: Tools for data sharing: smart contracts

Smart contracts are computer programs, which automatically execute data and / or value transfers according to certain predetermined parameters. According to the Commission, smart contracts have important potential in manufacturing 4.0, smart mobility and smart energy, and can play an important role through automating data transfers and data pooling, triggering payments for data transfers and for guaranteeing the implementation of conditions linked to data transfer. We welcome that the Commission considers smart contracts and distributed ledger technologies in general as a beneficial technology for the fostering of data transfers.

On question 18: Regarding smart contracts and distributed ledger technologies

Many companies within the energy sector have already been involved in the development of distributed ledger technology pilots. Especially in cases of market communication, energy trading, integration of electric vehicles in the energy system or the proof of origin of renewable energy can distributed ledger technologies and smart contracts possibly contribute to a faster and simultaneously trustworthy digitalization of the energy system.

On question 19: Regarding the effectiveness of smart contracts for the implementation of data access and the use in the context of co-generated IoT data

The use of smart contracts can be an effective tool if the legal framework conditions are clarified first. Smart contract could be a particularly effective tool especially for processes regarding the billing and control of photovoltaic systems, trading of energy and certificates, and the billing and control of energy/heat water/hydrogen from network operator to and from distribution network operator.

On question 22: Regarding interoperability as an issue for scaling smart contracts and requirements on standardisation

Minimum safeguards for cyber security are welcomed. Ultimately, interoperability is a problem of technically incompatible design choices. This cannot be solved by standardisation without breaking the security guarantee of the smart contracts (i.e., a hard fork of the underlying blockchain). For scaling across different ecosystems, a possible solution could be the use of a trusted official data source (an "oracle").

Therefore, standards in software and hardware are necessary. It is absolutely necessary, that systems with a large amount of participants can be controlled by one contract, for example in the case of smart meter data sharing. This is only possible, if the data actually reaches the data systems and has a specific format in order to keep working with it. Missing data or wrong data can cause manual problems.

On part IV: Clarifying rights on non-personal Internet-of-Things data stemming from professional use

Data stemming from IoT objects (Internet-of-Things) increases in the energy and water sectors along with the growing integration of smart objects and sensor technologies – especially in the context of smart city projects. These projects, as well as the smart-meter (-gateway) rollout, which is currently ongoing in Germany, reinforce the need for clarification on rights of non-personal data.

In general, with regard to the objective of fostering clarity for the sharing of data generated by IoT objects questions concerning the legal ownership of the data still have to be clarified.

On question 24: Regarding the fairness of data concerning the functioning and performance of IoT objects being held by the manufacturer

Data stemming from IoT-objects can certainly create new challenges for market fairness when access to relevant information concerning the functioning and performance is held by the manufacturer of such objects alone.

Machine-2-machine-communication in which machines mutually exchange information, is an important factor for the functioning of a digital industry and is also part of the German energy transition. As of today, the steering of networks is already partly automatized. In the long term, IoT-data will increase due to the need for intelligent networks. Consequently, access to data from IoT-objects will rise simultaneously. This is necessary for reaching the ambitious targets for the integration of decentrally produced renewable energy and the technical realization of an intelligent energy management.

Often, ownership questions of IoT-objects are not conclusively settled, which is why clarification is certainly needed. Nevertheless, for the functioning of IoT-objects it is important that non-personal data can still be analysed by companies providing services via the IoT-object, such as utility companies. In addition, manufacturers have to be able to access information about the functioning and performance of an IoT-object installed, as IoT-object-users often do not have the ability to service these objects themselves. Seeing that data regarding the functioning and performance of IoT-objects falls under the category of non-personal data, access

to this type of data by manufacturers for maintenance reasons only is not controversial. Nevertheless, when using systems from large providers, smaller users are usually not in a position to negotiate special data access rights for their own used systems. Here, data availability should be increased through clearly regulated data access rights at the user level.
This is particularly true in the area of electromobility, where there is a lack of data for better integration of electric vehicles into the energy infrastructure, e.g. for grid-serving load management. Access to vehicle data (e.g. charging progress, amount of energy required, power demanded, etc.) has not always been made sufficiently available by manufacturers via standardised interfaces and is therefore urgently required. This data should be at the disposal of the vehicle user who has to be able to decide to whom data is made available.

On part VI: Completing the portability right under Article 20 GDPR

In its introduction, the Commission summarizes that under Article 20 of the General Data Protection Regulation (GDPR), individuals can decide to port certain personal data to an organisation or service of their choice. Non-discriminatory access to smart metering data is mandated by Article 23 Directive (EU) 2019/944 on common rules for the internal market for electricity. Any data stored in terminal equipment, such as connected objects, can only be accessed in accordance with Article 5 (3) of Directive 2002/58EC (ePrivacy Directive). However, the obligations under Article 20 GDRP do not require the controller to put in place the technical infrastructure to enable continuous or real-time-portability.

On question 34: Regarding the sharing of data of smart connected objects by the manufacturer with explicit permission of the user

Individual owners of smart connected objects should be able to permit whomever they choose to easily use the data generated by their use of that object. This procedure can be supported as long as objects do not gather any personal data from individuals and the owner of the object is also the user of it. If the owner of the object is also its user and it is their own personal data, consent within the scope of the GDPR is required.

On question 35: Regarding the sharing of data of smart connected objects by the manufacturer without the agreement of the user

Device manufacturers should not be allowed to permit whomever they choose to easily use the data generated by the use of that object without agreement of the user. The agreement of the end user should be obligatory. Such agreements can, for example, already be included in the scope of contracts clarifying the use-terms for smart objects and need to comply with the requirements of the GDPR in the case of personal data.

On part VIII: Safeguards for non-personal data in international contexts

Non-personal data generated by EU companies may be subject to access requests pursuant to provisions of laws of third (non-EU/EEA) countries. This would be specifically relevant when processing of such data occurs in a cloud computing service, the provider of which is subject to the laws of third countries.

We welcome that the European Union seeks to establish safeguards for the protection of non-personal data processed in the described context.

On question 62: Regarding solutions at an EU regulatory level to mitigate the risk for European companies stemming from the request for access by foreign jurisdiction authorities to their data

In general, projects seeking to increase the level of data sovereignty within the European Union, for example the GAIA-X initiative, can contribute to the reduction of the risk of European companies' data to be accessed by authorities from foreign jurisdictions. Nevertheless, the use of cloud-services offered within the GAIA-X initiative is voluntary and not existing yet. Many companies rely on cloud-services hosted by non-EU parties now and will do so in the future. Therefore, it is of utmost importance to establish agreements between EU-countries and third-party countries which guarantee compliance with European data hosting, processing and usage standards that guarantee the availability and legally compliant usability of state of the art (cloud-) technology.

Contact

Sandra Struve
Representation to the EU
Phone: +32 2 774 5119
sandra.struve@bdew.de

Johannes Imminger
Representation to the EU
Phone: +32 2 774 5114
johannes.imminger@bdew.de

Lisia Mix
Headquarters Berlin
Phone: +49 30 300199-1064
lisia.mix@bdew.de

Dr. Jörg Rehberg
Headquarters Berlin
Phone: +49 30 300199-1211
joerg.rehberg@bdew.de