GEODE FACT SHEET

Data Management

Introduction

In the energy market, several parties (grid operators, suppliers, aggregators, service providers, etc.) have to be able to exchange/access large amounts of information (metering and energy consumption data, data required for customer switching, demand response and other services) in an efficient, secure and reliable way.

Article 23 of the Electricity Directive (EU) 2019/944 obliges Member States to put effective data management structures in place in order to ensure efficient and secure data access and exchange, as well as data protection and data security.

A number of countries are in the process of defining their national model for data management. Existing national data management models vary considerably between different Member State, both regarding where data is stored and how data is exchanged, and what type of retail market model is being implemented. The data management model in each Member State should be designed to optimally support the requirements of the national electricity market. The chosen market model plays a key role in the provision of electricity-related services to customers and it should support any changes.

POLICY & REGULATORY REQUIREMENTS

GEODE identifies the following recommendations for future legislation and for decision makers when deciding on data management models.

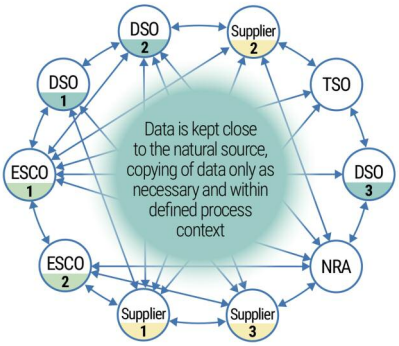
- Customer and business value must be put the first priority.
- European legislation must be neutral on which data management model (centralised, de-centralised or hybrid) is implemented in a Member State.
- To avoid unnecessary costs and risks, existing well-functioning data management solutions must remain in place. This is in line with Recommendation 3 and 9 of EU Smart Grids Task Force EG1 – *Towards Interoperability within the EU for Electricity & Gas Data Access and Exchange*[1].
- Data management infrastructure and its regulation and governance should be independent, open, transparent and technology neutral.
- All relevant stakeholders and market actors must be involved in the process of developing any data management infrastructure. This also applies to future updates and improvement processes.
- Focus should be on interoperability and communication. The high level goal of data management initiatives is to make systems work together to add value and new capabilities.

[1] EU Smart Grids Task Force Expert Group 1 – *Towards Interoperability within the EU for Electricity & Gas Data Access and Exchange:* https://ec.europa.eu/energy/sites/ener/files/documents/eg1_main_report_interop_data_access.pdf

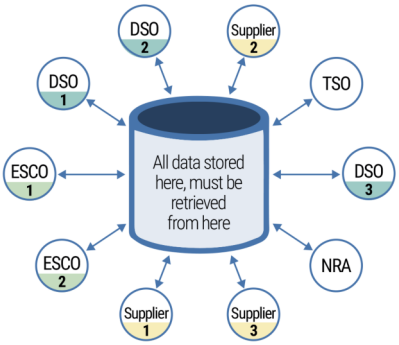
- Data exchange should be based upon Open Standards. These standards should be defined or adopted explicitly by the appropriate European organisations.
- Consider possible secondary effects. Establishing centralised hubs will lead to accumulation effects and create Single Points of Attack or Failure. In turn, de-centralised models might lead to increased complexity. Fallback scenarios must be put in place.[2]
- All cost and risk factors should be considered and analysed critically. It is difficult to estimate the costs of reaching the necessary service and performance level with different data management solutions. Thus, it is important to critically analyse cost drivers, ownership structures and already existing data management solutions. It is clear that a system change introduces additional costs. Only if the benefits outweigh the costs is a change advisable.
- Keep entrance barriers for all market participants low and allocation of costs fair.
- Consider the six Principles of the General Data Protection Regulation, GDPR[3], when deciding on a data management model: *Lawfulness, Fairness and Transparency, Purpose Limitation, Data Minimisation, Accuracy, Storage Limitation, Integrity and Confidentiality.*
- Use English for documentation of procedures, among actors and for data exchanges.

Data Management Models

Data management models are typically classified based on the architecture of data storage and exchange. The most widely known models are the **de-centralised model,** the **centralised model** and the **hybrid model**. The three models are described in more detail and illustrated below.



The De-centralised Model is an architecture in which data is stored at the source (e.g. metering information at DSO, contract information at supplier, capability data at DER, etc.) and systems are communicating directly with each other. Market actors are working together to develop standardized market communication. An example is *Energy Data exchange* in Austria *(EDA)*.

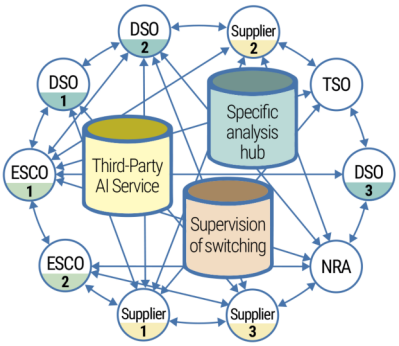


The Centralised Model includes a data hub to which data is sent and stored. All business processes run on that hub and results are sent back to its clients. It is operated and developed by a specific party or service provider. Market participants use its functionalities. An example is *Datahub* in Finland.[4]

[2] See more in the section *Secondary effects to be considered about Data Management Models* in this paper.

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural person-swith regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[4] To be introduced in 2022.



The Hybrid Model is a combination of the two previous models. All market participants can communicate in a de-centralised manner, but in some use cases (e.g. compliance monitoring for services like supplier switching, supervision of trading activities or integration functionality for e.g. smaller parties), there are task-specific central structures. Data is copied sparingly and only within a specific use case context. For instance, the Netherlands is aiming for such an environment without a data hub in between.

SECONDARY EFFECTS TO BE CONSIDERED ABOUT DATA MANAGEMENT MODELS

The decision on a data management model could have unintended consequences and risks that need to be assessed, and might require structured risk management methodologies to be applied.

The following list shows a non-exhaustive number of aspects to be considered. Some of the aspects that are mentioned in the section *Policy & Regulatory Requirements* above, also appear in the list below, further elaborated.

- **There is a risk of snowball effects.** Once an infrastructure is in place for one use case (e.g. supplier switching), it may be cheaper to make additional use of it (e.g. billing or data sharing), because many cross-functional items can be re-used.
- **Data management infrastructure has to be technology neutral in terms of which data management model (Centralised, De-centralised or Hybrid) is implemented in a Member State.** This is in line with Recommendation 2 of the joint TSO-DSO Data Management Report[5] and Recommendation 4 of EU Smart Grids Task Force EG1 Towards Interoperability within the EU for Electricity and Gas Data Access & Exchange.[6]
- **Data exchange should be based upon Open Standards**. These standards should be defined or adopted explicitly by the appropriate European organisations. It must be kept in mind that the concept of Open Standards should be differentiated from Open Source. The first allows for a competition of implementations on the market and avoids unnecessary dependencies on the vendors, whilst still enabling diversity. Being based simply on Open Source software or hardware is probably too vague and insufficiently transparent, so this is not a reliable basis for regulation or for legislation. It would be acceptable to use Open Source components that implement any Open Standards in use.
- **Future needs will imply different system requirements.** Hence, when new use cases are implemented, it must be analysed whether a given approach still meets dependability requirements.
- **When establishing centralised data hubs, from an information security/safety point of view, they act as a Single Point of Reference/Single Point of Attack.** This means, that if all data is copied and consumed from a central point, all services based on that central point will not be able to function if that single point is attacked or malfunctioning.

[5] TSO-DSO Data Management Report.
https://www.geode-eu.org/uploads/GEODE%20Germany/DOCUMENTS%202016/TSO-DSO_Data%20Management%20Report.pdf

[6] EU Smart Grids Task Force Expert Group 1 – *Towards Interoperability within the EU for Electricity & Gas Data Access and Exchange:*
https://ec.europa.eu/energy/sites/ener/files/documents/eg1_main_report_interop_data_access.pdf

- **The party running a centralised data hub can prioritise developments and resources according to its own agenda, unless it is sufficiently regulated.** It must be ensured that operators of data management platforms cannot exert inappropriate influence on its activities. Please see Recommendations 0 and 10 of EU Smart Grids Task Force EG1 Towards Interoperability within the EU for Electricity and Gas Data Access & Exchange.[7]
- **If a de-centralised model is not defined in a way that is consistent and standardised, there is a risk of more complexity (and hence cost) associated with the number of different actors, interfaces, formats and exchange protocols and diversity in general.** Switching between these different areas creates costs and complexity and potentially a barrier to entry.
- **In a de-centralised model unless Open Standards are used, there is a risk of creating dependencies to the providers of integration infrastructure.**
- **Use English for documentation of procedures, among actors and for data exchange. Procedures are often detailed in a national language.** Therefore, keeping at least the documentation in English, with improved syntax, helps to keep systems and relevant markets open and leads to increased competition amongst service providers, as there are no language barriers.

Conclusion

Currently many decisions, that will have an effect on energy data management, are underway. The outcome of these processes – even though they might seem very technical in nature at a first glance – will have significant impact on European retail energy markets. These decisions must be seen as strategic, safety-relevant and critical for the Energy Transition, security of supply and the allocation of responsibilities in the future. To respect this, available CBAs and studies must be challenged critically, and secondary effects and risks must be considered. According to Art. 23 of the Electricity Directive (EU) 2019/944[8], the decision on a data management model remains a national decision for each Member State. The high-level goal of all data management initiatives should be to make systems work together to add value for the customers in the context of the whole system approach.

[7] EU Smart Grids Task Force Expert Group 1 – *Towards Interoperability within the EU for Electricity & Gas Data Access and Exchange:* https://ec.europa.eu/energy/sites/ener/files/documents/eg1_main_report_interop_data_access.pdf

[8] Art. 23.2 RED *"Member States shall organise the management of data in order to ensure efficient and secure data access and exchange, as well as data protection and data security. Independently of the data management model applied in each Member State, the parties responsible for data management shall provide access to the data of the final customer to any eligible party".*