Fraunhofer CINES

Implications of European Data Strategy and Data Regulation for the Energy Sector

White paper

Table of contents

List of Abbreviations

Abbreviation	Explanation
API	Application Programming Interface
BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)
DA	Data Act
DAO	Data altruism organization
DGA	Data Governance Act
DIS	Data intermediation service
DT	Data trustee
GDPR	General Data Protection Regulation

Management Summary

Two important regulations, the Data Act (DA) and Data Governance Act (DGA), have been adopted as part of the European Commission's Digital Strategy and Digital Decade. This white paper discusses their implications for the energy sector and explores them based on three use cases.

With the number of decentralized power generation and consumption systems growing sharply and interconnections between energy and the other major sectors of heating and mobility also on the rise, the energy sector faces particular challenges when it comes to the digital transformation and use of data. This makes the opportunities and risks associated with future data regulations of particular interest.

The most striking change has come through the Data Act (DA), in the form of the right of equipment operators to receive their data generated during operation from the manufacturer and use it themselves or through third-party service providers. This expands data availability for operators of wind turbines, for example, and permits the use of data with service partners to optimize operation and maintenance. This utilization route can also be translated to operation of other kinds of equipment.

The Data Governance Act (DGA) creates a legal framework for data donation and trusteeship models. These models may be of interest from the standpoint of the energy industry in terms of obtaining rights to use measurement data pertaining to consumers, which can be used anonymously and for a specific purpose such as creating better and more individual household load profiles.

In the field of electric mobility as well, a data trusteeship model may be a way to resolve the pronounced conflicts of interest between automotive manufacturers and energy sector users when it comes to the use of electric vehicle (EV) battery data. Data access that is accepted by both sides creates tremendous potential for both availability and flexibility of data from EV fleets.

These and other applications unlock new opportunities, but the regulations also come with great complexity. The DGA in particular imposes extensive obligations on data trustees. In addition, it is often difficult to develop business models for data trustees in practice in the absence of public start-up funding.

For the business sector, one of the main impacts of the coming regulations is that they create a need for organizations to revise their own digital and data strategies or craft new ones altogether. Especially in plant and systems engineering, there are also costs and effort involved for developing and providing additional interfaces for customers. At the industry level, associations can take on new roles as neutral data trustees. To this end, the associations should hold internal discussions, define goals and work toward those goals in funded projects. At the same time, there is a need for revision and simplification of the DGA from the policy side to create greater scope for implementation of data trustee and intermediation services.

1. Introduction

The Data Act and Data Governance Act, both part of the European Commission's Digital Strategy and Digital Decade, are important regulations that are now in place to simplify access to and use of data. The objective of both regulations is to support data-driven innovation and streamline existing processes in various industrial sectors in order to bolster competitiveness. The Data Act is intended to make more data available from internet-connected products. The aim is to enable transparent and fair access, including for small and medium-sized enterprises (SMEs). The Data Act and Data Governance Act represent the overall framework for improved exchanges of data, but they do not supply concrete implementation. With this in mind, this white paper takes a deeper dive into how both pieces of legislation affect data-driven innovation in the energy sector and identifies potential actions that energy sector stakeholders can take.

With the number of connected products such as decentralized power generation and consumption systems growing sharply, the energy sector faces particular challenges when it comes to the digital transformation and use of data. Furthermore, increasing sector coupling also means that there are large volumes of data to coordinate between the electricity, heating and transport sectors. These two regulations are thus especially relevant to the energy sector, as it is home to a large number of connected devices that generate data.

The new regulations offer numerous opportunities for operators of connected products by giving them simple access from the manufacturer to the data their equipment generates during operation, along with the chance to use these data themselves or through third-party service providers. Leveraging data in this way can help with aspects such as optimizing operational workflows, thereby cutting costs. Improved access to data can also give rise to new business models in that the data can be used as a basis for targeting product improvements or developing enhanced services, for example to maintain systems or equipment.

At the same time, the new regulations also involve additional requirements, and with them, risks. Increased availability and use of data require more robust data protection and security measures to guard sensitive information against misuse. Companies need to ensure that they are able to meet the new legal requirements and zero in on where they need to invest in IT infrastructure and expertise. For manufacturers of internet-connected equipment, it is necessary to review which data their systems and equipment collect and in what form they can continue to use these data, including in the future, if their customers' rights as operators are reinforced by the Data Act. The requirements that apply to easy access to equipment data may open up new opportunities for exchanging data between companies and bolster collaboration and interoperability among stakeholders in the energy sector.

Against this background, the Data Act and Data Governance Act offer significant opportunities to advance the digital transformation and data use in the energy sector. The implications of these regulations are multifaceted, opening up opportunities for energy sector stakeholders to enhance their competitiveness while also creating certain risks related to meeting requirements. Therefore, the goal of this white paper is to develop an improved understanding of the ramifications of the new data regulations and highlight ways the energy sector can successfully navigate these changes.

2. Fundamentals of Data Exchanges

2.1. Parties to data exchanges

The key parties to data exchanges are the **users** and **providers** of data. As the term suggests, the providers make their data available to the data users. For users, the focus is generally on the availability of suitable data and on verifying the quality of the data so they can use the information in their own use cases. For data providers, the typical top priorities are ease of sharing data (interoperability) and preventing risks (such as leaks of trade secrets), along with assuring data quality.

Data trustees are intermediaries who bring the two parties together and both make the data exchange possible and simplify it. In particular, their role involves helping to foster trust between the parties. Experiments involving various data trusteeship models are currently under way across a variety of industries, from automotive and mobility to crop production and forestry. However, there is not yet a general model that has emerged as optimum at this point. Even without a single model, there are a number of aspects that data trustees commonly handle or support:

- Secure technical infrastructure for data exchange
- Trustworthy authentication of data users and data providers
- Data catalogs or portals to help find available data
- Sample agreements and standard clauses for data exchange
- Payment settlement and similar processes

Ambitious data trustees can also offer other functions, such as active matchmaking between providers and users, development and certification of software tools and solutions and even orchestration of comprehensive data and developer ecosystems.

Two important subcategories of data trustees are **data intermediation services** (DISs) and **data altruism organizations** (DAOs), which are defined in the Data Governance Act and are subject to certain obligations, some of them extensive, under the DGA (see Sec. 2.5 below). However, not all data trustees and data donor organizations necessarily fall within the scope of the DGA. Some are even explicitly exempt; this includes data brokers and data trustees that serve only a closed (limited) group of providers and users.

2.2. Data categories and data sources

Depending on the scale and type of protection required, data falls under two different categories: **open data** and **protected data**. These categories can also be further subdivided into subcategories in some cases. Which category data belongs to has implications for exchanges of data. The less protected data is, the simpler it is to share. Another category that is growing increasingly important is **synthetic data**.

- **Open data:** Data that can be used, distributed and reused without restrictions.[1] Data that was originally personally identifiable and has been anonymized — i.e., the connection to a specific individual has been **irreversibly** broken, so it is impossible that this person will be reidentified — is also considered non-personal data and can be used as open data.
- **Protected data:** All other data that is not publicly accessible and is protected. Depending on the reason for the protection and the scope of protection afforded, this category can be further broken down as follows:
- **Personally identifiable data:** Data that relates to an identified or identifiable natural person and thus falls within the scope of the data protection and privacy laws (GDPR, BDSG, etc.).
  - **"Special categories" of personal data:** Article 9 GDPR creates a subcategory of data that requires special protection (because it is presumably especially sensitive). This includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, along with genetic, biometric and health-related data and data concerning a person's sex life and sexual orientation. Processing of these types of data is subject to especially stringent conditions. These kinds of data are likely to be seldom relevant to the energy sector, however.
  - **Data containing trade secrets:** Data concerning certain technical systems or processes often includes critical business information, such as battery characteristics in the energy storage industry. Each company has to define for itself which of its data can be shared without restrictions, which can be shared only subject to certain conditions or with specific users and which is so sensitive that it cannot be made available to external parties.
  - **Synthetic data:** Data generated artificially. Synthetic data is generated based on a "real" data set. The artificial (synthetic) new data set replicates the structures of the original set on which it is based, but without individual "artificial" values being associated with the underlying "real" values and without any possibility of inferring information that would identify those underlying real values from the artificial data set. Synthetic data plays a growing role in AI development.

There are many different **data sources**. Sources that are especially important to the energy sector are:

- Industrial production, plant and equipment data
- Time series of measurement data concerning power use by households and companies
- Public data from public bodies
- Research data and association data

2.3. The data life cycle

Exchanges of data take place within the data life cycle, which can be visualized as having five stages (see Fig. 1).

The first stage of the data life cycle is **(1) collection**. The data provider typically handles this part, which generally involves the use of sensors and occasionally (in the case of households, for example) manual entry as well. Software applications can also generate data relevant to the energy sector, such as price predictions and energy market transaction data.

The next part of the data life cycle is **(2) preparation or enhancement** of the raw data that has been collected to make it usable for further analyses and processing. This step includes, in particular, **cleaning the data** to eliminate measurement, unit, format and other errors, along with **formatting**and possibly **annotating** or **compiling** the data according to a set formula or pattern. In the case of personal data, the preparation process can also include **anonymization** or **pseudonymization** to ensure that data protection and data security are observed. This is especially important if there are plans to share the data. For the same reason, critical information can be deleted from data that is not personally identifiable but still requires protection (such as trade secrets)[2]

1 https://data.europa.eu/elearning/en/module1/#/id/co-01

2 Anonymization or deletion of business data and similar data is by definition associated with a loss of information. How much information is lost and how problematic the loss is depend on the specific issue at hand and the details of the data set. There are statistical techniques that can be used to calculate the expected loss of information.

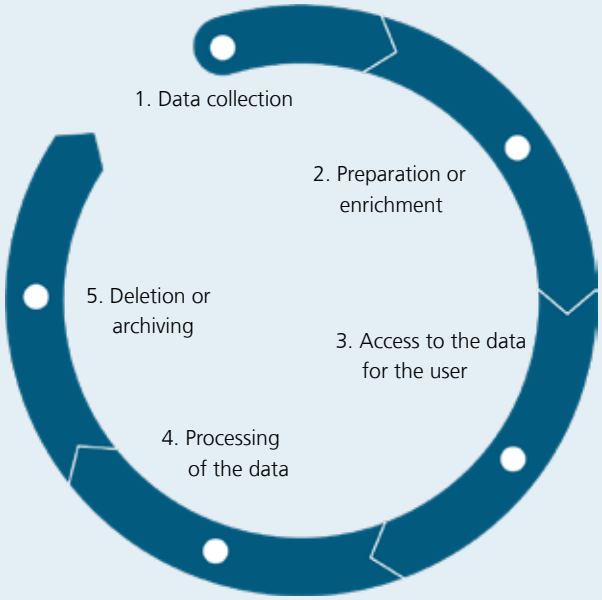


Fig. 1: The data life cycle: collection, preparation, access, processing and deletion

One very important aspect if the data will be shared or even merely used broadly within the organization that has collected it is the generation of **meaningful metadata**. Good metadata allows users to find relevant data sets and quickly understand which data the set contains; how the data is structured, formatted, annotated and/or coded; by whom and when it was collected; the quality and reliability of the information; which units are used and how the raw data was processed and prepared. Metadata should be generated according to defined standards and specified vocabularies. There are numerous metadata standards these days[3]

If the data is shared, the provider now grants the user **(3) access** to the data. Concretely, this can take place by way of machine-to-machine communication, for example via an API, or through human-to-machine communication in the form of provision in a web portal or transmission by email. The disadvantage of this route for the data provider is that the provider gives up all practical control over the data.

Alternatively, the data can also be uploaded to a secure data space that is under the control of the data provider or a third party (such as a data trustee). Users then process the data inside this space so that the provider or trustworthy third party retain the ability to monitor and control the data. Finally, the data provider can refrain from giving the user any direct access to the data at all, instead merely allowing the user to send their own algorithms to the data provider (or the trustworthy third party). In this case, the provider or third party implements the algorithms on the data and all the user receives back is the results of the calculations. In any event, the data provider, user and any third parties (trustees, other service providers) need to reach organizational and technical agreements so the data are available and can be processed securely and in high quality.

Once the shared data have been provided for the data user, the **(4) processing** can take place to generate value from the data. The final step is **(5) the deletion or archiving of the data**, depending on the agreement between the data provider, users and any third parties that may be involved.

At each of these steps, the data providers and users face various challenges when it comes to enabling the seamless exchange of data in the energy sector.

2.4. Challenges in exchanging data

2.4.1. Economic challenges and risks

Increased sharing and joint use of data between companies, government entities and even households are key drivers of economic growth, new business opportunities and achievement of transformative goals such as the energy transition. The EU's data strategy and digital transformation strategy, along with multiple new EU regulations, create a legal and political framework for this.

In spite of its potential, however, data sharing is not necessarily an immediate success. The reason for this is that data providers and users often face a fundamental **trilemma involving benefits, costs and risks or uncertainties**. Sharing data is worthwhile for both providers and users if the value created in the process (the benefit) outweighs the costs and risks. However, it can be difficult to gauge ahead of time whether this is the case. This means that advances in data sharing will require lower costs and risks, greater benefit and reduced uncertainty.

The **value** (benefit) for data users typically lies in additional sales, cost reductions or innovations made possible by the shared data. Possible benefits to data providers include fees or other monetary compensation that they can charge for the data, reciprocal access to data or products or services that users develop with the data and provide to the providers at a lower cost. Providers can also grant access to data as a contribution

3 For example, see https://rdamsc.bath.ac.uk/ and https://www.dcc.ac.uk/guidance/standards/metadata/list.

to the wider community even without a direct economic benefit, for instance as a data donation or for PR reasons.

The main **cost** on both sides is generally the personnel expenses involved in sharing and preparing the data, verifying quality and analyzing the information. Other costs arise from the time and effort involved in identifying and pursuing valuable use cases for the data, entering into agreements with the data provider or user, ensuring compliance, any necessary investments in IT infrastructure and potential fees for data access.

Key **risks** arise from deficiencies in data protection, privacy, data security and legal certainty. For data providers, there is a risk that their data will be analyzed for illegitimate purposes or by unauthorized parties or that trade secrets will leak out. Data users run the risk that errors in the data or metadata will go undetected, leading to costly further errors down the line, or that the added value they hope to achieve by using the data will not be realized. As one typical example, uneven data quality can significantly impair the accuracy and reliability of AI applications. And finally, each side faces the risk that compliance violations by the other party may rebound onto it, resulting in legal damages or reputational harm.

Another area of **uncertainty** regards which valuable use cases there are, what data is needed for those use cases, how much added value there is to be achieved and what levels of time, effort and expense will be needed to get there. This is of special concern where plans call for developing cross-industry or cross-domain use cases. These hold out the greatest potential for innovation but are often the least defined. Amid this situation, identifying and developing use cases frequently requires extensive communication and collaboration between potential partners. Trustworthy third parties can play an important role as matchmakers, bringing data providers and users together and helping them to identify use cases.

Intermediaries like **data trustees** help to reduce the risks and costs for data providers and users alike. They lower the costs of searching through matchmaking and by providing maintained data catalogs and portals, help to guarantee the trustworthiness of the parties and the security of transactions and support the handling of transactions from a technical, legal and business perspective.

2.4.2. Data standardization

The data user needs to be able to interpret and further process the data that is provided. This makes the use of standards crucial. Data that is collected and provided according to standards reaches a larger market and is more versatile, which makes it of higher value.

This unlocks particular opportunities for the energy sector, as many processes and data formats are already regulated in this industry and are in place at businesses. The unregulated parts of the industry hold significant potential as well, for example in the provision of operating data on equipment or communication of data for emerging processes such as provision of flexibility.

2.4.3. Challenges in exchanging data

Before any data is processed (collection, cleaning, analysis, deletion, etc.) or exchanged, it is necessary to ensure legal compliance. This is especially the case for personally identifiable data (see Article 6 in conjunction with Article 5 GDPR), but it is also true of data that is not personally identifiable where specified by other provisions, such as those of copyright or competition law or contracts. Fundamental issues, which are generally covered by a contract or data protection policy, include the purposes for which the data is processed, the extent to which the data or the results of processing are permitted to be shared with third parties, time limits for erasure, security measures and what compensation, if any, data providers are to receive.

One challenge is that compliance failures by one party can give rise to legal risks for the other. If, for example, one of the purposes for which the data user intends to process the data or even the sharing of the data itself is not covered by the data protection policy or other contractual documents on the data provider's side, this can result in a compliance violation by both the user and the provider. In principle, this challenge can be addressed through solid contract drafting and advance legal review of the plans for data access and processing. Trustworthy third parties like data trustees can also provide suitable frameworks for data providers and data users alike to address this challenge.

Data security:
Ensuring data security is crucial in the case of **industrial production, plant and equipment data**. In one survey conducted by Bitkom, 47 percent of businesses that do not share data expressed concern about possible misuse of their data (Bitkom 2023b). This is why authentication and authorization are crucial, as they are instrumental in controlling data access and preventing abuse and the disclosure of trade secrets.

With this in mind, companies and other institutions have already incorporated protective measures into their general data security strategies, so they can be used for exchanges of data. Depending on the details of the data sharing, protective measures can be adopted by data trustees or other trustworthy third parties.

Interoperability:
Interoperability is a key requirement, and often also a challenge, when it comes to simplifying the exchange of data. In the Bitkom survey mentioned above, 26 percent of respondents gave up on plans to exchange data because the data was

not directly compatible (Bitkom 2023b). There is a wide variety of different data formats even within the same industries, a situation the Data Act intends to simplify considerably. The data must be available in a "comprehensive, structured, commonly used and machine-readable format" (EU Com 2024).[4] Meeting these requirements is a challenge for many companies. This applies to both preparing the data according to suitable standards, including industry standards, and potential updates when standards are adjusted.

Data requiring protection:
Implementing protective measures for protected data (such as industrial production, plant and equipment data or personally identifiable data) is a challenge. Companies need to ensure that no information is disclosed that could violate the rights of equipment manufacturers or users, thereby leading to financial losses or compensation. Data providers are therefore obligated to take technical measures to protect sensitive information while guaranteeing the usability of data at the same time. If there are plans to share aggregated data, it is necessary to ensure that no personally identifiable information can be derived from it. In the case of smart meter data, personally identifiable information can be protected through geographic or temporal aggregation, for example (Wagh, Mishra 2023). There are technical solutions available to protect sensitive data, meeting the requirements of data providers and users alike.

Right to withdraw in the case of data donations:
In the case of personal data, data donations play an important role, as they can lower the costs to data users. But because these kinds of data often contain sensitive information about individuals, data users have to ensure that the data in question is properly erased if a data donor exercises their right to withdraw consent or the donation agreement expires. If the data has been anonymized, it is no longer considered to constitute personal data and thus no longer falls within the scope of the GDPR, so the rights to withdraw consent (and all other GDPR provisions) cease to apply.

Trilemma — challenges
The biggest challenge when it comes to exchanging data is the **trilemma involving benefits, costs and risks or uncertainties**. Both data providers and data users have a number of questions to answer:

1. What is the benefit or value of the data?
2. How much time, effort and expense will go into sharing the data (including the necessary data preparation)?
3. How great is the potential risk involved in the data exchange, and what uncertainties are there?

While data providers are concerned mainly with the dilemma of benefit versus cost, data users face the added challenges of ensuring data quality and interoperability and honoring the right to withdraw consent.

Models and concepts for data spaces as platforms have been developed and already put into live operation across various sectors as infrastructure to resolve some of the challenges in exchanging data as noted above. Data spaces represent decentralized data ecosystems that are aimed at shared benefit and based on jointly agreed technologies and standards to ensure the interoperability of the data and the security of the exchange.

When it comes to resolving the challenges involved in sharing and exchanging data, data trustees are one option, acting as neutral service providers between data providers and data users. In addition to secure data exchange, including via their own data spaces, data trustees can also help resolve other challenges (including meeting compliance requirements, preparing data for anonymization and other procedures, acting in the role of broker/matchmaker between data providers and users or providing advising services).

2.5. Solutions for data sharing through EU regulation

2.5.1 Data Governance Act (DGA)

What are the goals of the DGA, and what are the plans for achieving them?
The DGA entered into force in June 2022 and has applied since September 24, 2023. It has two main goals. First, it is intended to support the sharing and donation of data among private entities and the use of shared or donated data. The DGA attributes a lack of trust to the low willingness that has been seen so far among companies, private individuals and other stakeholders in the data economy to share or donate data or use shared or donated data. With this in mind, the DGA has developed a legal framework for *data intermediation services providers* (DISPs), which are intended to enable commercial sharing of data, and for *data altruism organizations* (DAOs), which aim to help advance the donation of data. Both types of organization can be viewed as subtypes of data trustees. The legal framework defined in the DGA is intended to promote the emergence of trustworthy DISPs and DAOs, thus easing the situation (European Commission 2024, Kerber 2021).

4 See the first paragraph of Article 5 of the Data Act, available online at http://data.europa.eu/eli/reg/2023/2854/oj (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828).

The second goal of the DGA is to enable public bodies that possess protected data to release the information for further use. The Open Data Directive (Directive EU 2019/1024) already urged public sector bodies to release data in their possession for use by private entities. However, protected data — personally identifiable data, trade secrets, intellectual property and data subject to confidentiality obligations — was exempt. The DGA stipulates conditions under which these kinds of data can be disclosed. However, it does not define any new legal obligations to actually release the data. That is up to the Member States. Another important point is that data in the possession of public enterprises and cultural and educational institutions (such as universities) is explicitly exempt from these provisions of the DGA. The rules that apply to DISPs and DAOs are therefore likely to be the most relevant to the energy sector rather than those concerning the release of public data. In light of this, the remainder of the discussion focuses on DISPs and DAOs.

What are data intermediation services, what are they allowed to do, and what are their obligations?

Article 2 DGA defines a data intermediation service as a service which aims to establish *commercial relationships for the purposes of data sharing* between an *undetermined number* of data holders (companies, natural persons etc.) on the one hand and data users on the other. The following are explicitly *not* considered DISPs:

i. Services such as data brokers that collect data from data holders, enrich or transform the data (for example through aggregation) for the purpose of adding substantial value to it and license the use of the resulting data to data users *without establishing a commercial relationship between data holders and data users*
ii. Services that are exclusively used by one data holder (such as a major corporate group) in order to enable the use of the data held by that data holder (an internal data platform used by the group, for example)
iii. Services used by multiple *legal* persons in a *closed group* (for example, within a supply chain)
iv. Providers of technical tools such as clouds or software that enable the exchange of data but where the provider does not act as an intermediary or broker. A cloud provider is thus not a DISP, but a data marketplace operator is.

Data intermediary organizations can be for profit or not for profit. Articles 11 and 12 DGA set out the provisions that apply to DISPs, which are relatively extensive. The key points are as follows:

- DISPs have to observe all of the existing legal provisions, such as those on data protection and privacy, competition, protection of trade secrets and so on. In particular, the DGA does not take precedence over the GDPR.
- DISPs are not permitted to use the data that data providers share through them for any purposes other than (i) to provide it to the data users, (ii) to further develop the intermediation service itself and/or (iii) for security purposes. This means the data intermediation organization is not permitted to use the data for its own commercial or other purposes that go beyond acting as an intermediary.
- The legislature seems to provide that DISPs share the data exchanged through them, as a general rule, in the format in which they have received it from the data providers. In principle, format conversion is permitted only to improve interoperability, at the user's request, for legal reasons or to satisfy international data standards. Other forms of data enrichment seem to be permissible only if they serve the exchange of data — the law mentions "curation," conversion, anonymization and pseudonymization — and require the express consent of the data providers in any case. Any enrichment of the data with additional information or aggregation into a larger data product that goes beyond this could therefore be unlawful and should undergo legal review as a first step.
- The same applies to additional services and tools. The DGA mentions that a data intermediation services provider could offer these kinds of options but seems to be primarily referring to services/tools that directly facilitate sharing of data (such as intermediate storage or anonymization). Whether farther-reaching services such as analytics would be permissible is still unclear. All applications of services/tools require the data provider's consent.
- DISPs must be separate legal entities. A DISP cannot be a business unit within a company, for example; it would need to be organized as a separate subsidiary or similar. DISPs are not permitted to grant special conditions (such as discounts) to data providers and/or users if they also use other services offered by the DISP or its affiliates.
- DISPs must register with a competent authority, which each EU Member State designates. In Germany, this falls within the purview of the Federal Network Agency (Bundesnetzagentur). This authority passes the registration along directly to the European Commission, which maintains a public list[5] of recognized DISPs.
- Other provisions concern fair, transparent and non-discriminatory access, security, breaches, notification obligations, insolvency, interoperability, logging and cross-border transfers of data.

DISPs that already offered their services on June 23, 2022, are required to fulfill the DGA starting on September 24, 2025. DISPs that began operating after June 23, 2022, would already be obligated to fulfill the DGA now as a general rule.

5 This list can be viewed at https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services.

In practice, however, this is already not possible in full, as Germany did not designate the competent authority until just recently. Across the EU, not many DISPs have been registered with the Commission yet (those that have been registered are from countries including Finland, France and Hungary). Recognized DISPs are allowed to use the shared "EU Recognised Data Intermediary" logo.[6]

What are data altruism organizations, what are they allowed to do, and what are their obligations?

Data altruism organizations (DAOs) are legal entities that collect data made available on the basis of data altruism ("data donations") and provide it to users for objectives of general interest (Article 15 DGA). Article 2, point (16), DGA defines "data altruism" as the voluntary sharing of data, on the basis of consent, by data holders or natural persons without any reward that goes beyond compensation related to the costs that these providers of data incur where they make their data available, for objectives of general interest such as combating climate change, improving mobility, or research. The DGA is silent on the issue of whether for-profit enterprises are permitted to use these kinds of donated data, and if so whether they can do so for purposes with an at least indirect profit motive (such as product R&D). The DGA does not rule this out, anyway. At any rate, donors of data must not be rewarded for their altruism (regardless of the form of the reward, such as compensation, discounts, access to special services, etc.).

Article 19 DGA allows a DAO to register as *"EU recognised"* with an authority of a Member State (in Germany, this is also the Federal Network Agency). *Recognized* DAOs are allowed to use the "EU Recognised Data Altruism Organisation" logo and are listed in a common European register. However, registration as a "recognized" DAO is *explicitly not required*; even "unrecognized" organizations are permitted to continue their data altruism activities (Recital 46 DGA).

The conditions that apply to recognition are relatively extensive (Articles 18 through 21 DGA). Recognized DAOs are not permitted to pursue any for-profit aims and must be legally independent from any organization that operates on a for-profit basis. Their documentation and reporting obligations include but are not limited to the names and contact details of all data providers and data users, the time or duration, purposes and technical means of the processing undertaken by the users and the technical data protection measures utilized, along with any results. A DAO is required to notify data providers, before any processing their data, of the objectives, purpose and, where applicable, location of processing and make tools for simple granting and withdrawal of consent available to them. There are also security requirements and compliance with a "rulebook" that has yet to be defined by the Commission, which is to set down information and security technology requirements in further detail (Article 22 DGA). A draft version is to be available in early 2025. The EU also plans to publish a *common consent form* for DAOs so consent can be obtained in a standardized form EU-wide. However, as of the time of writing, only a single DAO (from Spain) has been listed in the European register of recognized DAOs.

What are critical discussion points?

There is broad-based support for the DGA's goal of promoting greater sharing, donation and use of data. The development of an EU-wide legal framework and shared European logos and branding for DISPs and DAOs is also fundamentally reasonable. At the same time, there is criticism (see, for example, Veil 2021a, 2021b, 2021c) that the DGA primarily creates new and labor-intensive obligations for both DISPs and DAOs without offering any substantial relief from existing regulatory burdens (such as GDPR exemptions) or advantages to counterbalance them. The view that *lack of trust in the security and neutrality* of DISPs and DAOs is the main reason impeding their development, which underpins the DGA, also seems open to debate. However, as noted above, trust/neutrality do not by themselves create a positive incentive for sharing data. The expectation that the benefit will outweigh the cost is what creates this kind of incentive. The time and effort (which equate to higher costs) that the DGA compels DISPs and DAOs to expend and the restrictions it imposes on their own use of data, special conditions, organizational form and potentially additional services and value-adding data enrichment (in the case of DISPs) and for-profit objectives (in the case of DAOs) certainly do not make it any easier to build DISPs or DAOs or to create offerings that actively induce the sharing and donation of data. Nevertheless, the fundamental logic of advancing the sharing of data to a greater degree still holds. With this in mind, data economy stakeholders should both examine the extent to which DISPs and recognized DAOs as defined by the DGA are nonetheless a feasible route for them and actively investigate whether other constructs that do not fall under the DGA are legally possible for them and could be a good idea from an economic and/or technical standpoint. This could involve measures like establishing a nonprofit sectoral data broker that does not establish any direct commercial relationships between data providers and users — making it not a DISP as defined by the DGA, so it is exempt from the provisions of the DGA — but is still designed to enjoy as much trust as possible (for example, no profit motive of its own, operation by an industry association, or similar).

6 Logos are available at https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union.

2.5.2. Data Act (DA)

What are the objectives of the Data Act?
The primary objective of the Data Act is to more fairly distribute the value created from data among the stakeholders in the digital environment. Data silos are to be broken down and the data released in the process made more accessible to all those involved in this space, creating a data market geared toward competition and unlocking new possibilities for data-driven innovation. At the same time, the legislation aims to strengthen the rights of those whose products and services generate commercializable data in the first place.

How are these aims to be achieved?
The goals of the Data Act are to be achieved first and foremost in that users of digital products and services based on them are given more control over the data generated by their products and the services they use. Users can be private individuals or enterprises (Article 2, point (12)) such as plant and equipment operators. For example, users can demand that the data holder provide data — wherever possible, in real time — for themselves or data recipients (Articles 4 and 5). "Data holder" means a natural or legal person that has control over a product and an associated service and is thus in a position to provide data (Article 2, point (13)). "Data recipient," in turn, is defined as a natural or legal person to which or whom the data holder makes data available for business purposes at a user's request (Article 2, point (14)).

Furthermore, pursuant to Article 4, point (13), data holders are not permitted to use non-personal data generated by the user for their own purposes unless an agreement has been reached with the user regarding this beforehand. Article 3(2) and (3) obligate the data holder, in this context, to provide far-reaching information to the user prior to entering into a contract. This is intended to promote the monetization of data use. Users are to be given the choice of providing their data to either data holders or data recipients, depending on who offers them better service or more compensation for the use of their data.

Which data is covered by the Data Act?
The specifications of the DA pertain mainly to two types of data: product data (Article 2, point (15)), which is generated through the use of a product, and related service data (Article 2, point (16)), which represents the digitalized form of the user's interactions, intentional or not, with the product. However, user access is restricted exclusively to "readily available data" (Article 2, point (17)), which the data holder can obtain without disproportionate effort going beyond a simple operation. This means the law applies to both raw and "pre-processed" data (physical parameters such as temperature, pressure, flow rate, position, acceleration, speed etc.) as well as to the metadata (which includes the basic context and timestamp for the data) needed to make the provided raw and pre-processed data usable (Recital 15). Enriched data, meaning in particular analyses or interpretations of raw or pre-processed data, is not covered by the user's claim to access and sharing. Beyond that, the provisions of the DA extend to both non-personal data and personal data. However, the provisions of the GDPR are not affected, which means that data holders and recipients are still required to observe the currently applicable data protection regulations.

Fig. 2: Data Act timeline
The Data Act entered into force on January 11, 2024, but most of its provisions take effect 20 months later, on September 12, 2025. Exceptions include the obligations arising from Article 3 (1) to design products in such a way that data is accessible to users by default, which take effect one year later, on September 12, 2026, and the extension of the specifications to existing contracts, which does not take effect until September 12, 2027.

Provisions concerning data transfers from the data holder to the data recipient

Further provisions govern the conditions under which data is transferred from the data holder to the data recipient. For example, to ensure interoperability, the data must be provided in a structured, commonly used and machine-readable format (Article 5(1)). Beyond that, Article 9 permits data holders to demand that the data recipient provide reasonable consideration for the provision of data, but they must take various factors into account when doing so (particularly if the recipients of the data are SMEs) to demonstrate that it is reasonable.

Data recipients are also particularly prohibited pursuant to Article 6(2), point (e), from using the data they receive to develop a product that competes with the product from which the data originates and from disclosing the data on their end to another third party for this purpose. The law also addresses issues of protecting trade secrets (e.g., Article 4(6)[7]).

Other relevant provisions concern access to data by public bodies under exceptional circumstances.

What are critical discussion points?

Critical discussion points relate in particular to drawing the line between the raw and pre-processed data to be provided and enriched data, which falls outside the scope of the law. There are fears across European industry that lack of legal clarity could lead to the disclosure of trade secrets to non-European competitors. Within the European energy sector, there is also concern that the DA could bring even greater legal uncertainty to a regulatory landscape that is already viewed as being unclear and complicated. The stakeholders designated as "gatekeepers" by the European Commission pursuant to the Digital Markets Act (currently seven companies: Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta (Facebook, Instagram, WhatsApp), Microsoft and Samsung) are exempt from the provisions of the Data Act due to their dominant position. The goal of this carve-out is to prevent data from leaking to the biggest digital players, at least.

There are also questions regarding how the extensive rules established by the Data Act are to be enforced in practice. For example, using provided data to develop a competing project is prohibited, but whether recipients of data will abide by this prohibition and how to monitor this in case of doubt is as yet unresolved.

2.6. Side note: potential business models for data trustees

Numerous attempts to establish sound **business models** for data trustees are currently under way. However, a definitive model has not yet taken shape. Owing to the wide variety of industries and fields of application involved, it is likely that different industry-specific models will emerge. Even so, any solid business model will have to answer three key questions:

- What is the data trustee's value proposition to data users and data providers?
- How is the data trustee funded?
- Does it pursue for-profit aims?

In principle, data trustees can pursue **for-profit aims**. However, there are two reasons that can argue in favor of non-profit orientation. First, it can be easier for a non-profit data trustee to build trust, especially when the operator is also a neutral instance known to the industry stakeholders (such as an association or consortium). Second, it tends to be easier for a data trustee that operates purely on the basis of covering its own costs to keep the costs (such as fees) to data providers and users low, which in turn lowers barriers to participation.

Existing data trustees often seem to obtain at least a portion of their **funding** from government or private sources (such as associations, foundations, corporate consortia). Furthermore, fees are often charged to data users (less often to data providers) or there are at least plans to do so. There are many possibilities in this regard: For example, fees can be structured as a subscription model (time period, data volume) or by access, or they can include a freemium component (free up to a certain threshold, then paid) or be charged on a sliding scale according to the users, with cheaper access for SMEs or universities (Kreutzer 2023). Depending on the industry context, more individual models can be a good idea. In the field of medicine, for example, it is common for pharmaceutical companies to bear the costs of biobanks' expansion of their data stocks — which not infrequently run to eight figures, — and in return be granted temporary exclusive use of the data before it is released to everyone.[8]

The **value proposition** determines which services the data trustee offers. The core service will typically be enabling the **exchange of data**. Two fundamental legal and organizational structures are possible for this. The first one involves the data trustee enabling *direct* data exchanges between providers and recipients that are structured as *direct business relationships*

7 Regulation (EU) 2023/2854 (Data Act) available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854

8 For further discussion of this point, see Kreutzer, S. et al. (2023): Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. Bericht zu Arbeitspaket 1.2: Anforderungen und Umsetzungshemmnisse für Datentreuhandmodelle. Technopolis Group.

between these two parties. In this case, the data trustee falls within the scope of the DGA. This has the added advantage that the data trustee can register as a "recognized DISP," which can foster trust. It also makes it possible to structure the data exchanges from a technical perspective as direct data flows between providers and recipients — that is, without the data passing through the data trustee itself. This is likely to reduce the security- and compliance-related requirements and costs to the data trustee. At the same time, the data trustee is then subject to all of the requirements and restrictions of the DGA.

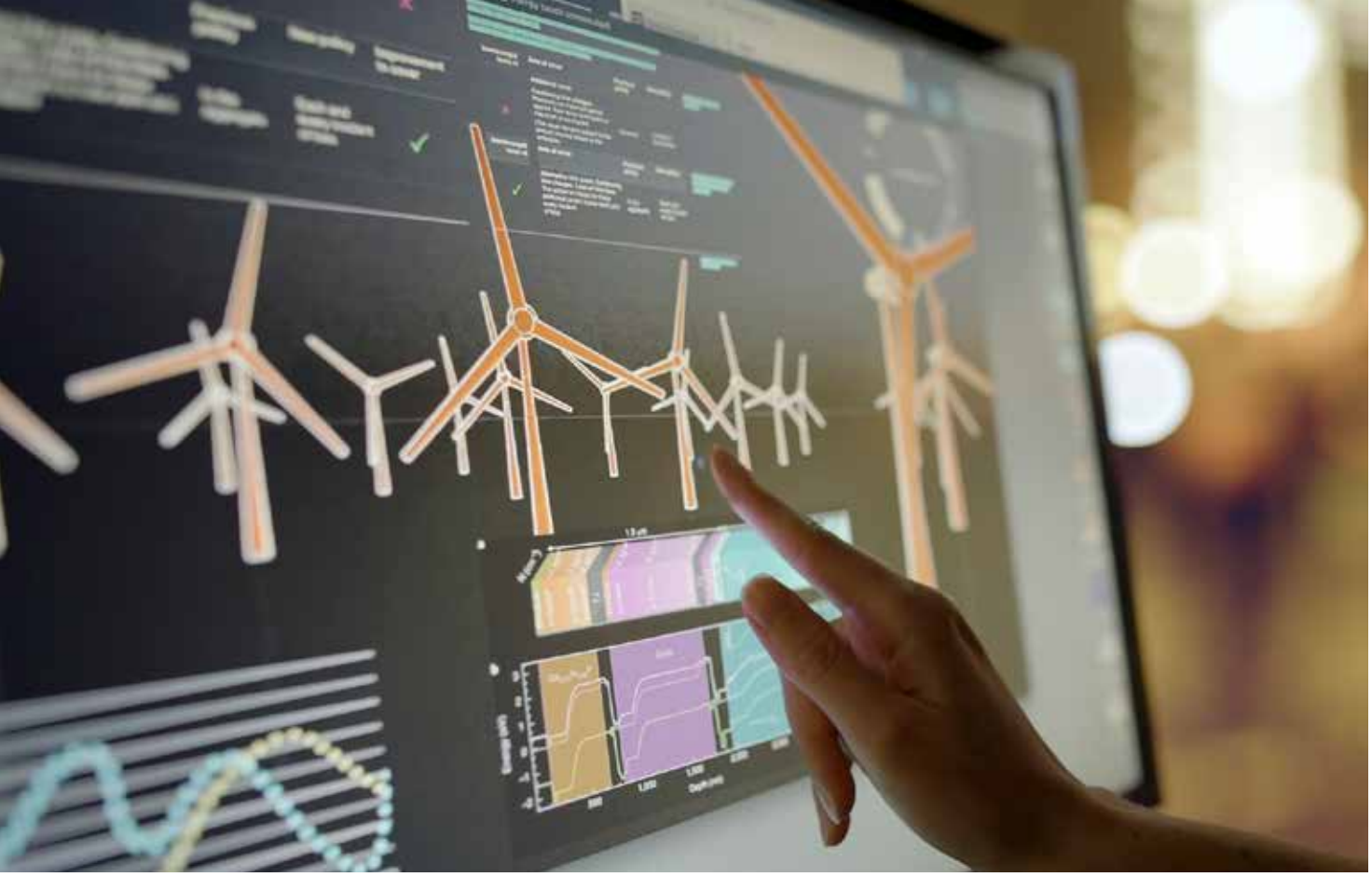
Alternatively, the **data exchange** can also be structured as *business relationships between the data trustee and the data provider or users alone in each case*, *without* direct relationships between providers and users. This would remove the data trustee from the scope of the DGA, creating greater leeway from a regulatory perspective. However, in that case it seems likely that the flow of data would run through the data trustee at any rate, and the data would be in its direct custody and control, possibly for a longer period — with all the additional security and legal requirements that go along with that, but potentially also the possibility of developing additional offerings and value propositions for providers and users alike. Depending on the industry and application context, combination forms of data trustee that bring together different elements of these two basic legal and organizational forms could also be an option.

However it is structured, the core service of data exchange is likely to have the following key parts:

- Providing the necessary technical infrastructure for the data exchange, including a technical and organizational architecture that makes it easy for data providers to see how their data is being used (purposes, methods, possibly results) and to exercise data sovereignty (i.e., being able to prohibit certain uses and erase data)
- Ensuring data security and data protection, adherence to usage and exchange agreements and other forms of compliance on the part of providers/users; where applicable, supporting the parties in this
- Assuring the quality of data and metadata
- Further forms of data processing or preparation, particularly those aimed at enabling or facilitating data exchange: anonymization or pseudonymization, formatting, possible cleaning

Additional services can be designed around this "core." One potentially very important service involves acting as a **matchmaker** and even **use case orchestrator** for data providers and users. As discussed above, identifying and developing new use cases often requires extensive communication between providers and users, along with an in-depth understanding of their respective domains and even business models, as well as technical and business capabilities. Without all this, it can be difficult to even see which data, partners and potential new applications could be of interest in the first place. If data trustees build deeper knowledge about their participants and the participants' data and domains, they can bring potential providers and users together on a specific basis and orchestrate these discussions and processes of identification and development.

There should be no legal problem with this kind of matchmaking or even company / use case builder services, including under the DGA, as the data trustee (DISP) is not itself using the provider's data in the process (at least not for purposes that go beyond enabling the exchange of data). However, **additional services** based on processing of provided data are also conceivable. These could also be highly interesting to both providers and users, but they might be more difficult from a legal perspective for a data trustee that falls under the DGA. Nonetheless, the legal interpretations are still on the fluid side at present. A legal review would definitely be advisable. Services like these could include, for example, enriching data with additional information and/or aggregating it into larger data products, offering analytics tools and/or services and other self-produced analyses and interpretations of the data.



3. Sample Use Cases for Exchanging Data in the Energy Sector

3.1. Data donation and trustee for HEMS data

Power suppliers' schedules are based to a large extent on standard load profiles for household consumption. However, the actual load profiles increasingly deviate from these standard profiles. This pushes up costs in the power supply sector, as the discrepancy between the predictions and actual demand must be made up in the short term with costly balancing energy. To be able to plan for future realities in households that consume electricity, extensive and detailed information is needed from households, supplemented where applicable by information on whether they have solar panels, home energy storage systems, heat pumps, wall boxes or home energy management systems.

The Data Governance Act now gives private and commercial consumers the option to share their consumption data in high time resolution with data trustees (data intermediation services) and data altruism organizations. These entities in turn offer ways to provide the data on an earmarked basis for additional uses and applications by electricity suppliers, grid operators and other stakeholders in the energy system, such as research institutes. In this arrangement, the data trustee or DAO acts as an intermediary between the households that are providing data and the electricity suppliers and others who are using it, handling data access and potentially other aspects of data governance. There are various possible configurations for this:

- Data trustee/DAO as entity processing and storing data: Data can be collected by the trustee or DAO, stored there and then provided to data users.
- Data trustee/DAO without own direct access to data: Alternatively, a data trustee or DAO can control and monitor the exchange of data between the households and data users without having its own direct access to the data.

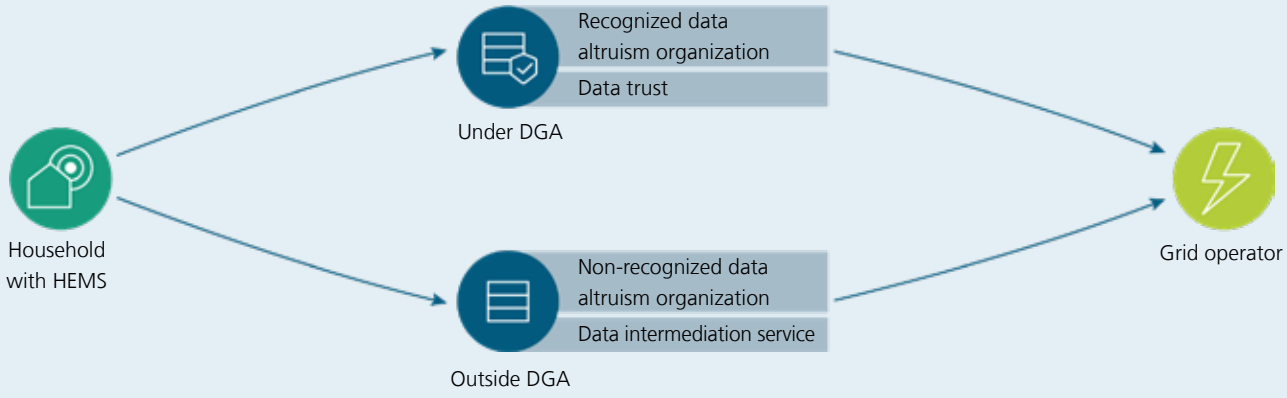


Fig. 3: Data donation regarding power consumption from HEMS to determine load profiles within and outside the Data Governance Act (DGA)

There are also various possible configurations for the specific form in which a data trustee or DAO is organized:

- Data trustee as data intermediation service (DISP) as referred to in the DGA
- Data trustee that chooses an organizational form that does not fall under the provisions of the DGA

These options — data trustee outside the DGA, DISP under the DGA, "recognized" DAO under the DGA, unrecognized outside it — all have different pros and cons depending on the use case. A DAO could be the form that garners the most trust for households in particular, but because a "DGA-recognized" DAO, at any rate, is not allowed to offer data donors any direct monetary advantages, it could be difficult for it to create sufficient incentives for donors. The benefit to donors would be very indirect, manifesting itself in lower grid fees for all electricity customers.

As discussed, a data trustee that does not fall under the DGA enjoys greater freedoms with regard to business models and data use than a DISP as referred to in the DGA, which could make it easier to create value for users and providers of data. However, "getting around" the DGA could require organizational structures that themselves give rise to new costs, while any trust advantages stemming from branding as a "recognized DISP" would be lost. In short, the specific pros and cons need to be analyzed and weighed in detail, but it is clear that there is a potential benefit to be derived from the data.

3.2. Exchanges of data in operation of wind turbines

Modern wind turbines are complex machines equipped with hundreds of sensors that control and monitor their functioning. The data generated by these sensors is key not only to the turbines' operation but also to predictive and reactive maintenance and repair. Access to and use of this data is typically governed by the purchase agreement between the manufacturer and the operator. The buyer generally acquires a portion of the available data. The manufacturer collects the full data volume in systems of its own.

At the same time, the initial purchase often also involves entering into years-long full maintenance agreements, which assign responsibility for service to the manufacturer or its service partners and guarantee a minimum level of availability for the operator. The exclusive data availability gives the manufacturer's service arm a competitive advantage over independent service providers. The Data Act will expand operators' access to data and give them clear rights to use the data generated by their equipment. This means data can be used jointly with third parties that do not compete with the manufacturer. It is conceivable that external software services could be involved here for tasks like early detection of errors. Cooperation with suppliers on aspects such as condition monitoring or other services relating to individual components also becomes possible. Uses of the data are also potentially relevant in the non-technical sector, such as when assessing the risk of failure or damage for funding entities and insurers.

3.3. Exchanging data to use information from EV batteries

The charging behavior of the surging number of electric vehicles is becoming an increasingly important factor for the electricity system. For example, it is necessary to predict and plan for the power needed to charge these vehicles with the greatest possible accuracy. Simultaneous charging peaks can also cause bottlenecks in the distribution network. And that means local temporal forecasts are also useful. Aside from that, the existing vehicle fleet represents a large pool of geographically available battery storage overall, and bidirectional charging in particular will make this an important source of flexibility in the power grid going forward.

All of these functions require access to vehicle battery data. The information needed includes the battery's rated output and capacity, current charge status, technical condition and possible operating points. This data is part of the battery management system and is present both in the vehicle and at the manufacturer's end. The battery is the highest-value component in any electric vehicle. Both battery properties and battery management are thus viewed as key areas of expertise for manufacturers in the electric mobility space. As a result, manufacturers are very reluctant to release this data, since they are trying to avoid detrimental impacts from competitors combining and reverse engineering control expertise from the data.

The Data Act gives automotive customers the right to access their battery data and permits them to share it with third parties as well. The EU's Renewable Energy Directive (RED III) also provides pathways for battery data from home storage systems and EVs to be shared for applications in the energy system.

The conflict of interest between use in the energy sector and protecting manufacturers' sensitive IP can be resolved by involving a data trustee, whether organized as a DISP as envisioned in the DGA or in a different structure. A DAO could also be an option, although the economic interests of those involved and the issue of incentivizing vehicle owners could argue against it. The trustee would govern the exchange of data between stakeholders and guarantee that the data is used for the earmarked purpose of energy sector applications. The data would flow in this case either through the data trustee ("man in the middle") or directly between providers and users. In any event, the data trustee would monitor access to the data and compliance with the terms of use, pseudonymize and possibly aggregate the data and securely encrypt it. Finally, the trustee would likely handle aspects of compliance and administration for the interested parties and might also act as a matchmaker.

Trust in and acceptance of the data trustee's organization is a crucial factor in light of the size of the stakeholders involved and the intensity of the divergent interests, especially as there is also no clear industry association in this field of energy systems integration that would be an obvious choice for this role. Alternatively, a solution can be discussed and created at the regulatory level.

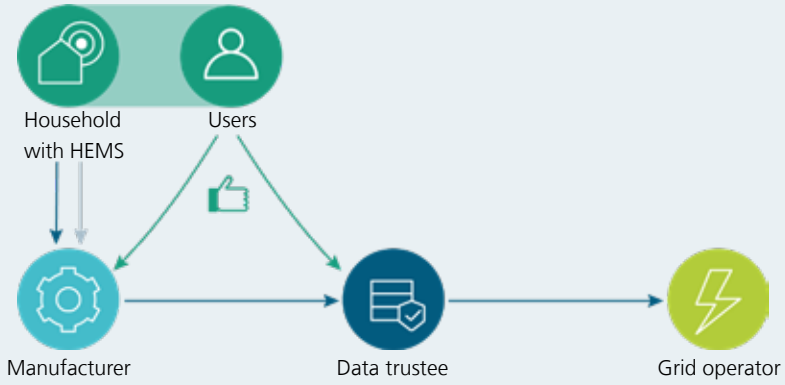


Fig. 4: Current and future flow of HEMS data via a data trustee to grid operator
Source: authors' own illustration

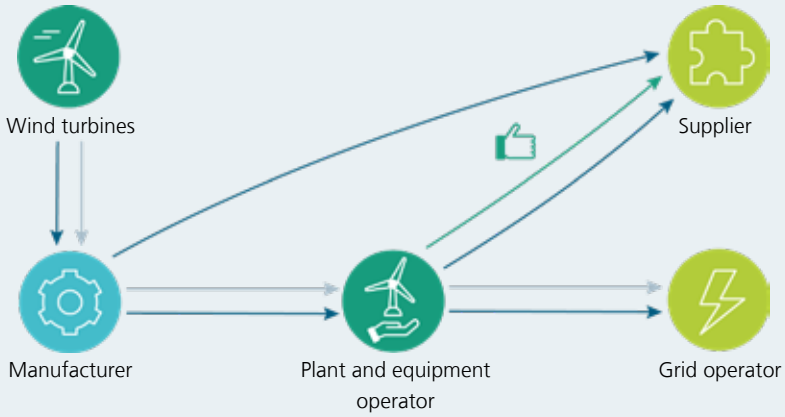


Fig. 5: Current and future flow of wind turbine data via a data trustee to third-party service providers. Source: authors' own illustration

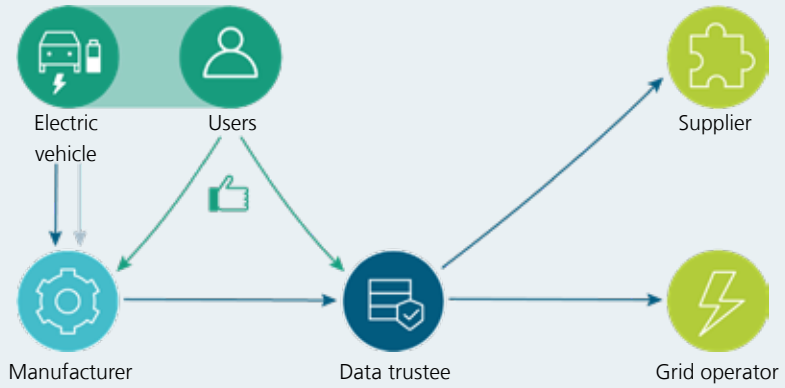
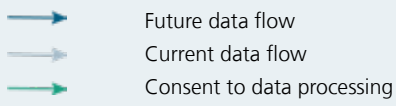


Fig. 6: Current and future flow of data from electric vehicle batteries via a data trustee to grid operator and third-party service providers
Source: authors' own illustration



4. Opportunities and Avenues of Action

4.1. Opportunities for data exchange through the Data Act and Data Governance Act

Areas of application
The sample use cases show that the new rules on data use established by the Data Act and Data Governance Act unlock opportunities for improved use of data and may simplify technical solutions and implementation for industry players. To that end, it is necessary to create sufficient incentives for potential participants.

Data Act
The future rights to use the data generated from a person or entity's own systems and equipment established by the Data Act open up a wide range of possibilities. From an energy sector perspective, there is particular interest in HEMSs. Data from these systems can be mined by entities such as grid operators and electricity suppliers for insights to optimize their processes. This can take place through more efficient, more individual load profiles and forecasts or by providing flexibility to the electricity market or in bottleneck management. This area holds huge potential to be tapped into for flexibility that can be addressed and marketed digitally (European Commission 2022).

In addition, all operators of the systems and equipment in the energy system benefit from their operating data being usable. As a result, the widely discussed advantages for optimization of operation and maintenance can also be utilized for the energy sector. This represents an important economic improvement in light of the high capital intensity of renewable energy facilities.

One important aspect in mobilizing this potential will be the usability of the data in a clearly understandable format, if at all

possible using relevant technical standards. Another criterion for success is the provision of well-documented interfaces (such as REST API) so the data can be readily incorporated into additional systems in ways that lend themselves to automation. Access to these interfaces requires authorization concepts and authentication methods to ensure that authorized access to the data is secure. Data space concepts can yield approaches for controlling access on the basis of shared identity concepts in this regard.

Data Governance Act

The data donation and data intermediation service (data trusteeship) models set down in legal terms by the Data Governance Act can help to resolve conflicts of interest or break down motivational barriers when it comes to the use of data. At the same time, there is a need for incentives for potential participants to get involved with these models. Data trustees can also specialize in entering into data use agreements with data providers and users, thereby streamlining processes. This holds out the prospect of making agreements and negotiations simpler and laying clearer legal bases for the use of data. Reducing legal risks can also make access easier for smaller stakeholders.

One key question in all this is who can be the operator of a data trustee, data donation company or data space as a data intermediation service. The organizations that take on this role should enhance trust in the data use process on the part of organizations that do not wish to agree on data usage with each other directly. This means it is crucial to identify the issues in the industry that can be solved through data trustees or data donation models. In this regard, these organizations are required to meet stringent requirements for technical and organizational integrity and ideally to have already won the trust of business partners in the market. Amid this situation, it is important to clarify whether associations can play a role in the data economy, and if so how, for instance by offering data trustee arrangements.

As designing business models for these roles has proven to be difficult thus far, one possible outcome is that a small number of domain-specific data specialists will emerge to satisfy the sometimes quite complex requirements that apply in the areas of technology and compliance, provide services and offer advice on the use of data infrastructure.

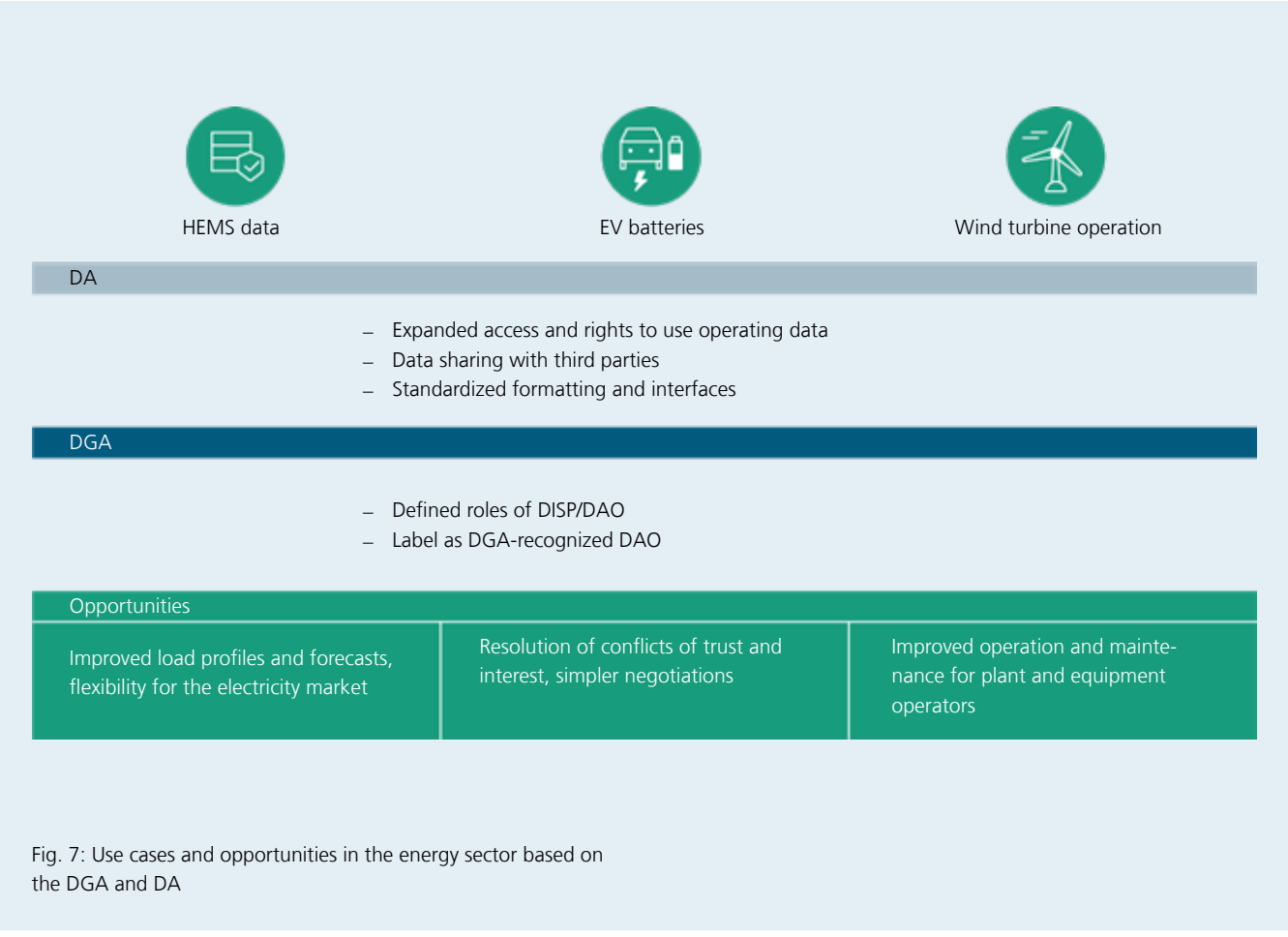


Fig. 7: Use cases and opportunities in the energy sector based on the DGA and DA

Challenges and implications

Data Act
While plant and equipment operators gain new rights under the Data Act, the same legislation requires companies in the mechanical engineering industry in particular to be aware of their upcoming obligations and meet them by developing digital products and services. This should go hand in hand with the development of a strategy for how the new customer relationships can be utilized for the future business. This gives rise to both time, effort and cost associated with execution and risks to the future data-based business in this sector.

Data Governance Act
A sound medium-term perspective is necessary to entrepreneurial decisions for or against participation in data trusteeship models or data intermediation services. The benefits of participating are particularly uncertain when a model is still in its inception. They are based in part on network effects and thus in many cases do not fully emerge until a critical mass of other stakeholders gets involved. This level of uncertainty can contribute to lack of motivation at the individual organizational level.

Another exacerbating factor is that the extensive requirements involved come at a heavy cost for both data trustees and data intermediation services, and these costs need to be passed through to participants via the business model. There is also a legal risk, which can likewise impact the costs and the number of providers.

In this situation, companies and associations should review whether a data trustee or DISP could be a way to realize valuable use cases or resolve legal obligations collaboratively. The next step in execution should be to develop financially sound models while also considering the opportunities afforded by a broker role. The concept selected must include incentives for all of the stakeholders involved. Public funding can be used to finance flagship projects, covering a key part of the development costs at the start of the process. In the medium term, projects like this should forge connections with other domains. In this regard, applying standards for data, processes and ecosystems is especially important.

Government
The path to realizing the functions and services envisaged in the DGA is marked by a trilemma due to high uncertainty, low motivation on the part of stakeholders and the high costs of execution. These challenges impede development in an area that is actually intended to reduce friction in the system.

The explicit restrictions the DGA imposes on the services that a data intermediation service is allowed to offer, in that it cannot make commercial use of the data itself, also make it more difficult to develop solid business models. Within a customer relationship, this can lead to situations in which stakeholders request additional services from a data trustee but the trustee is not allowed to provide them. There is also uncertainty surrounding the scope of the benefits the intended labels will actually provide.

From a policy standpoint, it is especially important now to create legal certainty surrounding the new rules established by the DGA, some of which are not yet fully concrete. At the same time, this process should leave considerable scope for various interpretations so different approaches can be tried out within the relevant framework.

To achieve this, continued support and funding for experiments involving the stakeholders most relevant to the use cases at hand will be a good idea during the ramp-up phase. This should encompass both the for-profit and nonprofit sectors. Initiatives aimed at data standardization and at maintaining data models and transferring them to application should also receive funding and support due to their central role.

Industry
Realizing the sample use cases described in this white paper and other applications will require balancing the individual motivations of participating stakeholders, the technology involved and the overall legal conditions.

Clear motivation on the part of participants is key here. The subjective benefit of participating in a model must outweigh the costs within a reasonable period extending from the time when the decision is made. Beyond that, it must be clear — and be clearly communicated — what constitutes an incentive for data holders to share their data. This involves both an intermediation issue and a conflict of interest for stakeholders whose business model is based on having an edge in terms of data.

As another basis, the subject of trust in the organizations and technologies involved needs to be more fully understood, with a greater grasp of the various complexities. The regulatory approach, especially as reflected in the Data Governance Act, of fostering trust through stakeholder certification addresses a key point in building a fair data economy. However, certification alone will not be sufficient to create trust for increased sharing of data between stakeholders. From the stakeholder perspective, the benefit to be derived from greater data exchange and a fair balance among the interests of the stakeholders involved are crucial, and this issue is not resolved by certification alone. Another essential condition for creating trust is secure technology for controlling access to the data provided. This allows the data holders to know which stakeholders are using and commercializing data.

Companies in the industry will particularly need to familiarize themselves with the obligations and opportunities the situation creates and to develop data and digital strategies of their own. Organizations that have the role of data holder need to lay the technological foundations for data access and prepare the required pre-contractual information from a legal standpoint. At the industry level, this topic should be addressed and followed up by associations and standardization bodies.

The EU's expectations have so far gone unfulfilled at the government and policy level. Unresolved legal questions impede development, and complex requirements make it more difficult to implement business models for data trustees. The DGA has thus overshot the mark in part. Improvement is needed at the policy and regulatory levels to help with this.

In spite of these deficiencies, the new rules hold out tremendous opportunities for the data economy in the energy sector. These should be explored in greater detail, supported and funded and ultimately tapped into at the industry level in collaboration with associations and other industry initiatives.

5. List of figures

6. Bibliography

Bitkom (2023): Press Release: Data Act: Bitkom-Präsident Wintergerst zum Abschluss der Trilog-Verhandlungen.
Available online at https://www.bitkom.org/Presse/Presseinformation/Data-Act-Bitkom-zum-Abschluss-Trilog-Verhandlungen, last retrieved on July 12, 2024.

Bitkom (2023b): Bitkom survey https://www.bitkom.org/Presse/Presseinformation/Datenoekonomie-Unternehmen-nutzen-Daten#

Digitaleurope (2023): Joint Statement: The Data Act is a leap into the unknown. Available online at https://www.digitaleurope.org/news/joint-statement-the-data-act-is-a-leap-into-the-unknown/, last retrieved on July 12, 2024.

Eurelectric (2022): Commission proposal for a Data Act — A Eurelectric position paper. Available online at https://cdn.eurelectric.org/media/5911/eurelectric-data-act-position-paper_final-h-E8583728.pdf, last retrieved on July 12, 2024.

European Commission (2022); Directorate-General for Energy; Klobasa, M.; Kühnbach, M.; Singh, M.; Knorr, K.; Schütt, J.; Boer, J.; Rolser, O.; Hernandez Diaz, D.; Fitzschen, F.; Garcerán, A.; Reina, R.; Stemmer, S.; Steinbach, J.; Popovski, E.; Antretter, M.: Digitalisation of energy flexibility. https://doi.org/10.2833/113770.

European Commission (2024): Data Governance Act explained. Available online at https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained, last retrieved on July 12, 2024.

Kerber, W. (2021): DGA — einige Bemerkungen aus ökonomischer Sicht, https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/pdf-dateien/kerber_dga_einige-bemerkungen_21012021.pdf Kreutzer, S.; Heimer, T.; Nachtigall, H.; Pschorn, L.; Bauer, F.; Blind, K.; Martin, N.; Grafenstein, M. von; Streblow, R.; Du, J.; Schölzel, J. D. (2024): Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft: Bericht zu Arbeitspaket 1.2: Anforderungen und Umsetzungshemmnisse für Datentreuhandmodelle; this study is being performed on behalf of the German Federal Ministry of Education and Research (BMBF) (co-financed by the European Union's NextGenerationEU program). https://doi.org/10.18154/RWTH-2024-04375.

Kreutzer, S. et al. (2023): Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. Bericht zu Arbeitspaket 1.2: Anforderungen und Umsetzungshemmnisse für Datentreuhandmodelle. Technopolis Group.

Veil, W. (2021a): Data Governance Act II: Datenmittler. Available online at https://www.cr-online.de/blog/2021/10/11/in-der-datenschutzrechtlichen-todeszone-der-data-governance-act-teil-ii/, last retrieved on July 12, 2024.

Veil, W. (2021b): Data Governance Act III: Datenaltruismus. Available online at https://www.cr-online.de/blog/2021/10/28/data-governance-act-iii-datenaltruismus/, last retrieved on July 12, 2024.

Veil, W. (2021c): Data Governance Act IV: Dataismus. Available online at https://www.cr-online.de/blog/2021/12/07/data-governance-act-iv-dataismus/, last retrieved on July 12, 2024.

Wagh and Mishra, 2023: A distributed approach to privacy preservation and integrity.

WindEurope (2023): Joint Industrial Statement on the Data Act. Available online at https://windeurope.org/policy/joint-statements/joint-industrial-statement-on-the-data-act/, last retrieved on July 12, 2024.

Publishing notes

Published by
Fraunhofer Cluster of Excellence »Integrated Energy Systems« (CINES),
EUREF Campus 23—24, 10829 Berlin, Germany

Responsible for text content
Volker Berkhout, volker.berkhout@iee.fraunhofer.de; Marian Klobasa, marian.klobasa@isi.fraunhofer.de; Nicholas Martin, nicholas.martin@isi.fraunhofer.de; Murat Karaboga, murat.karaboga@isi.fraunhofer.de; Jonathan Bergsträsser, jonathan.bergsträsser@iee.fraunhofer.de; Manuel Wickert, manuel.wickert@iee.fraunhofer.de; Junsong Du, junsong.du@eonerc.rwth-aachen.de; Rita Streblow, rstreblow@eonerc.rwth-aachen.de; Lukas von der Heide, lukas.von.der.heide@iee.fraunhofer.de; Marijke Welisch, marijke.welisch@zv.fraunhofer.de

Institutes involved
Fraunhofer Institute for Energy Economics and Energy System Technology IEE
Fraunhofer Institute for Systems and Innovation Research ISI
RWTH Aachen University

Image credits
Cover: iStock/peshkov; S.6: iStock/imaginima; S.16: iStock/Laurence Dutton, S.20: iStock/gorodenkoff

Recommended citation format
Berkhout, Volker; Klobasa, Marian; Martin, Nicholas; Karaboga, Murat; Bergsträßer, Jonathan; Wickert, Manuel; Du, Jungsong; Streblow, Rita; von der Heide, Lukas; Welisch, Marijke (2025): Implications of European Data Strategy and Data Regulation for the Energy Sector. Whitepaper. Karlsruhe, Kassel. Fraunhofer CINES.

Published
January 15, 2025, Version 1.0