gaia-x
Hub Germany

The EU Data Act and its impact on data spaces

Marco Mitrovic, Dr. Abel Reiberg, Dr. Karl Wienand – Gaia-X Hub Germany

Table of Contents

Authors

Dr. Abel Reiberg, acatech – national academy of science and engineering, project lead & coordinator Gaia-X-Hub Germany

Marco Mitrovic, acatech – national academy of science and engineering, scientific advisor Gaia-X funding project & Gaia-X-Hub Germany

Dr. Karl Wienand, acatech – national academy of science and engineering, scientific advisor Gaia-X funding project & Gaia-X-Hub Germany

About this Paper

This paper is based on a four-part blog series published by Gaia-X Hub Germany in response to numerous questions and uncertainties from our community regarding the EU Data Act. The blog series addresses the regulation from different perspectives: (1) an introductory overview of the EU Data Act, (2) the provisions for B2C and B2B data sharing, (3) a use case on B2G data access in the context of disaster management, and (4) the rules on switching between data processing service providers. This document brings together the contents of these blog articles, expands selected sections, and provides an English translation to make the information accessible to a broader audience. It is intended as a practical guide for understanding the structure, obligations, and opportunities of the Data Act.

1. Introduction: What is the EU Data Act

The Regulation 2022/868 of the European Union, also known as EU Data Act (or DA for short) has been in force since 11 January 2024 and, after a transitional period, all of the regulations it contains will become mandatory by September 2025. Once again, the EU is using the legal possibilities to regulate and thus promote the European data economy in a standardised manner. With the Artificial Intelligence Act, the Data Governance Act and now the Data Act, the European Union is taking on a global pioneering role. The DA, in particular, will oblige companies to provide data on a large scale from September 2025. This means that numerous producers and service providers will face new obligations – but also the opportunity to turn to new technological possibilities and take further steps into the data economy. In this paper, the Gaia-X Hub Germany provides an overview of the far-reaching regulations of the DA and shows how current data space initiatives make it easier to comply with the new requirements and utilise the opportunities of data exchange.

1.1. The core of the Data Act: data availability

The aim of the EU Data Act (DA) is to increase the availability of data. European companies are already collecting data on a large scale. This data could be used to improve existing processes and develop new products and services. However, this potential often remains unutilised at present because the data is frequently siloed, lacks interoperability, or is inaccessible due to legal uncertainties or missing incentives for sharing. Companies themselves are often not in a position to fully process the data for every benefit. At the same time, the exchange and trade of data has not yet taken place to the extent that would be possible. For example, 80 per cent of European industrial data remains unused.

The EU now wants to change this through incentives and obligations. To this end, the DA obliges companies to share data. To this end, the law contains far-reaching obligations for companies to provide data – both to users and to authorities and third parties. For example, data generated by users must generally be made available to the users themselves. Data that is required for official tasks must also be made available in emergencies, for example.

The DA will therefore impose new obligations on many companies. The following is a brief overview of what the new regulations provide for and how they can be complied with.

The provisions of the Data Act can be categorised into three simplified areas, which the next sections will expand upon.

Obligation to provide user data (B2C)

The first area concerns the provision of user data. Many products already collect data today: Cars, voice assistants and thermostats, for example, collect data on their surroundings, their users or the way they are used. From September 2025, manufacturers or data holders will have to make such usage data available to users of the products. Manufacturers are the producers of the products or services in question, while data holders are those who have actual control over the data generated, regardless of

whether they manufactured the product themselves. The obligated parties may not hide behind technical difficulties and cumbersome procedures when making data available. In future, they will have to design their products and services in such a way that the data generated is directly accessible to users. Experts refer to this as "data accessibility by design". If direct access cannot be set up, users still have a right to the data. A data holder must provide them immediately upon request, free of charge and in a standard and machine-readable format, ideally in real time.

Obligation to provide data to the authorities (B2G)

The Data Act also places data holders under an obligation towards state actors: authorities can request the provision of data if there is an "exceptional need" for this. This is the case if the authority requires data to fulfil its statutory duties in the public interest but is unable to obtain it by other means. For example, in the event of a disaster, such as major flooding as in recent years, authorities such as the Federal Office of Civil Protection and Disaster Assistance could request data from private organisations on rainfall and water levels. The authority must submit a request for this. The requested organisation must comply with this request immediately or justify why it cannot comply.

Regulations on interoperability and switching between data processing services

The DA creates new obligations for private organisations to share data. This could make significantly more data available for digital business models and smart applications in the future. At the same time, the legislator wants to prevent new digital monopolies and ensure that there is no strong concentration of data and data-based value creation among individual players. Instead, users should not be dependent on the services of individual providers of data processing services. On the contrary, they should be able to switch easily between data processing services. To this end, the DA obliges providers of data processing services to remove any barriers to switching. For example, fees for switching providers may at most cover costs. From 2027, these fees must even be completely eliminated.

Furthermore, the DA obliges interoperability: providers of data processing services must use open or common standards and formats - these can also be defined by the European Commission in the future. This means that principles that are already being implemented in practice through data space initiatives such as Gaia-X are being enshrined in law. Data spaces are also directly addressed by the DA: Transparency and interoperability goals that are already being pursued or realised by initiatives such as Gaia-X will be addressed by the DA.

1.2 Who enforces the DA?

In Germany, the Federal Network Agency (BNetzA) will be primarily responsible for the application and enforcement of the EU Data Act (DA). Although the federal government is yet to finalise the details, the most important aspects are already included in the DA. For example, users can contact the Federal Network Agency if their right to access usage data is violated. Third parties who should be granted access can also turn to the Agency, for example if they feel they are being discriminated against when accessing usage data. In turn, data holders must inform the BNetzA if they justifiably refuse to disclose data in certain cases.

In order to enforce compliance with the regulations, the BNetzA may impose sanctions that are "effective, proportionate and dissuasive" (Article 40(1) DA). For example, these can include fines of up to 20 million euros or up to 4 per cent of a company's annual turnover.

In addition to the possibility of submitting legal remedies and contacting the BNetzA with a complaint, authorised users and third parties can also contact a dispute resolution body together with the data holders concerned. These are independent, competent organisations that can be accredited as mediators and make binding decisions in the event of a dispute based on established procedures and fee schedules.

1.3. Data spaces as solution

Decentralised data ecosystems offer practicable solutions to meet the aforementioned obligations and objectives of the EU Data Act (DA). Instead of developing their own proprietary interfaces, data holders can join existing data space initiatives and make data available via data spaces. In this way, existing technologies can be adopted, e.g. for identifying users, for secure data transfer or for documenting data transfer. Costs for development and testing as well as the legal assessment of own solutions are thus largely avoided.

This is relevant, for example, with regard to the obligation to provide user data. By using data spaces, users can access the required data without encountering technical hurdles. An important aspect of data spaces is, for example, the cataloguing of data sets. Data space catalogues provide a clear overview of available data sets and their possible uses, which is of great interest to both users and third parties. Cataloguing structures the data and makes it more easily accessible, which meets the requirements of the Data Act, which calls for transparency and easy access to data. In this way, data spaces facilitate access to data and significantly reduce the effort involved in data management and provision.

Data spaces also offer considerable advantages when providing data to authorities by enabling transparent and legally compliant data exchange. The requested data can be provided immediately upon request without violating security standards or data protection regulations.

Data spaces can also make a significant contribution to fulfilling the requirements of the Data Act in the area of interoperability. This requires providers of data processing services to use open and common standards and formats to ensure that data can be easily exchanged between different services and platforms. This is where data spaces can act as a solution, as they are designed for interoperability from the ground up. This is particularly relevant when it comes to switching between data processing services, as the flexible structure of data spaces removes barriers such as proprietary interfaces or incompatible data formats.

Data spaces therefore make it easier to comply with the regulations contained in the Data Act. They also open up new opportunities for companies to drive forward data-driven business models and innovations. Open data spaces can be used to establish new exchange relationships, offer or demand data and data-based services and thus continue on the path to the data economy.

The following sections illustrate more in detail each of the aspects mentioned above, while focusing on data sharing in B2C and B2B contexts.

2. Data sharing mandates in B2C and B2B contexts

The EU Data Act (DA) represents one of the most important regulatory measures to promote the European data economy. It is intended to significantly increase the availability and utilisation of data in the internal market. To this end, the law obliges companies to provide data. This section elucidates the obligations contained in the Data Act to provide data to users and third parties. These are intended to facilitate the development of new products and services.

2.1. Who must provide what data?

Cars, fitness trackers, smart home devices – a wide range of products generate and store data when they are used. Due to the EU Data Act (DA), such usage data must be made accessible from September 2025. So-called "connected products" are particularly affected. These are products that generate or collect data when they are used and can transmit this data. Possible transmission paths are, for example, an internet connection or a cable that can be connected if required. This therefore refers in particular to devices that can be categorised as part of the Internet of Things. However, the law does not cover devices that are specifically intended for the storage, processing or transmission of another party (other than the user): for example, the servers on which connected services are hosted.

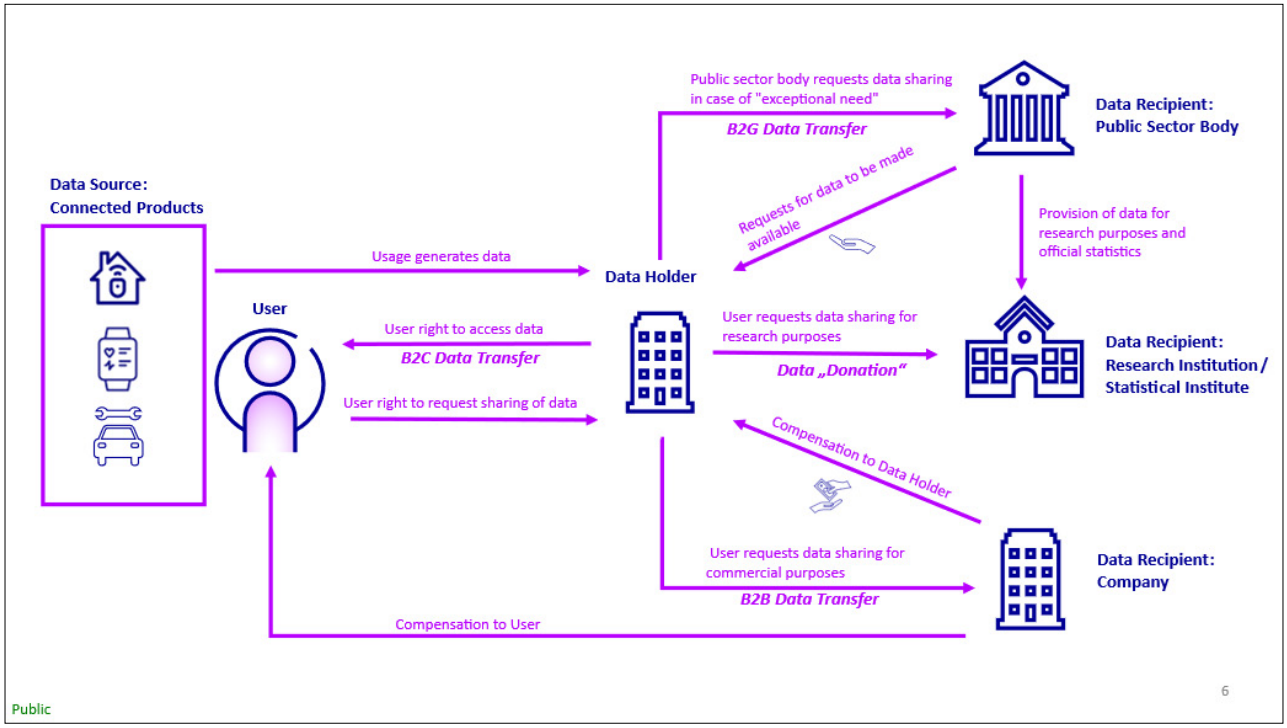
If, for example, headphones, air filters or refrigerators collect data, this must be made available. Firstly, the manufacturers of such products have a duty to provide access to usage data. For example, the manufacturer of a fitness tracker must make all tracked information fully accessible if this is not already the case. Secondly, the providers of digital services linked to the product must also provide data. In the case of the fitness tracker, for example, this could be an external service that uses the tracking data to create and offer analyses and recommendations, for example on the user's sleeping behaviour.

The new obligations to share data initially appear to be a hurdle for companies. Even traditional products such as washing machines and loudspeakers now process data. Manufacturers now have to provide this data and accept the costs involved. However, the obligations do not affect every company: Small and medium-sized enterprises are generally exempt. The regulation also offers new opportunities. Access to data allows new functions and services to be developed. For example, apps can be developed that combine usage data from household appliances from different manufacturers in order to create analyses and recommendations on usage habits or the energy consumption of the appliances.

The Data Act can therefore open new markets, whereby the openness of these markets should be guaranteed.

2.2. Who gets access to data?

When data is made accessible, one of the most important questions is: for whom? The EU Data Act (DA) answers this question by putting users at the centre. They can request the data themselves or arrange for data to be made accessible to third parties. These can be private companies or data altruistic organisations that develop new products, services or information from usage data, for example. However, large platform companies, which are considered gatekeepers under the Digital Markets Act, are not authorised.



2.3. In what form must access be granted?

According to the EU Data Act (DA), access to data for users must be "simple, secure, free of charge, in a comprehensive, commonly used and machine-readable format" (Article 3(1) and Article 4(1) DA) and "direct" (Article 3(1) DA) or "continuous and in real time" (Article 4(1) DA). Access must also be implemented in such a way that users are not unduly influenced in their decision. For example, it should not be permissible for user interfaces to make the selection of a certain option more likely than another (as is often the case today with queries about cookie use on websites).

In addition, data must be disclosed to third parties if this is requested by users. Access for third parties must be provided on "fair, reasonable and non-discriminatory terms and in a transparent manner" (Article 8(1) DA). For example, the manufacturer of a connected product may not exclude certain data recipients or demand particularly high consideration or particularly demanding technical measures from them. In principle, a consideration may be demanded for the provision of data, whereby the basis for the calculation must be specified. If the data recipients are micro-enterprises or non-profit research organisations, the consideration may only correspond to the costs of provision.

With all requirements for the provision of data, it must of course be assumed that these are only to be fulfilled to the extent that the technical effort is actually reasonable. However, it is clear that a simple reference to technical challenges will not be enough to deny access.

2.4. Implementation through data spaces

Nowadays, there are a variety of options for the provision of usage data. The EU Data Act (DA) does not specify which of these options are to be used.

However, in order to maximise economic and social added value, it would be desirable for data sharing to be as transparent, secure and sovereign as possible. Initiatives to establish data spaces in particular have the potential to fulfil these requirements. They serve the goal of disseminating largely open-source and therefore freely available solutions in order to exchange data in open, i.e. non-discriminatory spaces or marketplaces.

The first data spaces are already being implemented by companies and research institutions. For example, the Health-X dataLoft (https://www.health-x.org/home) project is working on a data space for health data and the Marispace-X (https://de.marispacex.com/) project is working on a data space for maritime data. The EU and its member states are also intensively promoting the development of data spaces in general. For example, with funding programmes such as the funding competition "Innovative and Practical Applications and Data Spaces in the Gaia-X Digital Ecosystem" and with specific passages in new laws such as the Data Act.

It can therefore be assumed that data spaces offer particular efficiency and legal certainty for the providers of usage data and realise economic and social potential.

2.5. The Data Act in practice: an example from the Gaia-X funding competition

The provisions of the EU Data Act (DA) can be illustrated by the Health-X dataLOFT project: The aim of the project is to establish a health data space for patients, doctors, research institutions and companies. In line with the objectives of Gaia-X, data is managed decentrally and only used with the consent of those affected. Wearables, among other things, are considered potential data sources. One example is fitness wristbands that collect data on the user's heart rate and sporting activities and transmit it to the device manufacturer. Such devices are "connected products" within the meaning of the DA. Users are entitled to request access to data relating to their heart rate or sporting activity, for example. The manufacturers of the trackers are obliged to provide access. This must be provided to the users themselves or to third parties in accordance with their requirements.

The Health-X data space should make such processes easy to realise. Users should be able to determine data recipients, purposes of use, etc. in an uncomplicated and granular manner. Appropriately authorised data recipients would then be granted access via the Health-X data space. For example, users could specify that data on their heartbeat is available as a data donation to public institutions for heart research. Users could also transfer data on their sporting activities to service providers in order to receive personalised training recommendations. The data space would ensure that the data is only accessible for the time periods, purposes and recipients etc. specified by the user and is otherwise protected from access.

The realisation of such a data space would offer considerable advantages for the enforcement of the DA: Shared use by all relevant stakeholders would avoid development costs for isolated solutions and interoperability problems. In addition, a comprehensive data ecosystem would be created in which – based on the will of the users – data would be accessible and usable. This would guarantee the sovereignty of users (in line with the purpose of the DA) and at the same time enable new forms of data utilisation.

3. B2G data sharing: the case of disaster management

Disaster scenarios highlight the need for rapid, reliable and secure data sharing between public authorities and private companies. Whether it's flooding, wildfires or pandemics—timely access to relevant data can save lives, allocate resources more effectively and helps strengthening civil protection . However, in many cases, data needed by public authorities is held by private actors, who must weigh operational, legal and ethical considerations before sharing it. With the EU Data Act, the regulatory framework for such business-to-government (B2G) data sharing has been significantly strengthened. The following section explores how data can support civil protection, how the Data Act enables access in emergencies, and how data spaces and trustees can support secure, efficient data exchange in practice.

3.1. How data strengthen civil protection

Data is crucial in modern disaster management: river levels, infection figures and aerial images of forest fire areas, combined with operational data, allow precise forecasts, simulations of disaster scenarios and the development of response strategies. Some data, such as precipitation levels, is publicly available. In other cases, confidential data is required, for example from private companies.

Until now, companies and authorities have had few established processes for data exchange. The authorities first have to justify which data they need, why and in what form. However, these clarifications cost time, which is particularly scarce in times of crisis.

The EU Data Act (DA) now sets out clear rules for the exchange of data between public authorities and companies in cases of exceptional necessity. The core principle: public authorities may request the necessary data from companies to deal with public emergencies – and the companies must provide this data or justify their refusal.

To illustrate this, let's look at the fictitious town of "Steinbach" and its collaboration with two companies. The electricity provider "Enervolt" has data on energy consumption. The mobile phone provider "SmartFunk" collects various location data from its users. This personal data requires special protection. However, the DA affects companies in all sectors.

3.2. Authorities can request the necessary data

If the city of Steinbach can obtain the necessary data on the market or through other agreements, it must do so in accordance with the EU Data Act (DA). If Enervolt and SmartFunk have not yet provided the data, the DA allows the city to request it.

In the event of a severe storm, for example, the data from Enervolt would be particularly useful. It helps to recognise power outages and dynamically organise the supply. This makes it possible to identify the most affected areas, increase efficiency and limit further outages. Furthermore, as the data is not personal, there are few obstacles to the application.

SmartFunk, on the other hand, collects personal data. According to the DA, Steinbach must justify why other data is not sufficient for the purpose. In a pandemic, SmartFunk data could indeed be indispensable. During the COVID-19 crisis, aggregated, anonymised location data from mobile phone providers showed how the mobility of the population affects the spread of the virus. This enabled authorities to issue early warnings of potential waves of infection.

As soon as the need for data has been established, the City of Steinbach submits a request for data in accordance with Article 14 of the Data Act. This request must be made in writing and is usually published. Among other things, the city must specify the purpose of data use, the deadline for data delivery, the duration of access and the time of data deletion as well as the third parties (public and private) with whom it will share the data.

In order to minimise the burden on companies, the same data may not be requested several times by different authorities (according to the "once only" principle). Steinbach can have this data processed by third parties, provided they are specified in the request. This allows it to use smart services or analyses from third-party providers without having to develop its own tools.

When the request arrives, companies must check that it is appropriate and compliant: Has only relevant data been requested? Does the requested granularity correspond to the stated purpose? The burden of proof therefore shifts from the requesting authority to the company that wishes to refuse.

In the example of the storm in Steinbach, SmartFunk could see the request for personal data as inappropriate. SmartFunk then has five working days to request amendments or refuse the request. Enervolt, on the other hand, considers the request to be reasonable and must "comply promptly" under the Data Act. However, the city of Steinbach and all third parties with whom it shares data are obliged to ensure the integrity and security of all data received.

In the pandemic example, SmartFunk approves the request and provides the requested location data of its users. However, the Data Act requires this data to be aggregated, anonymised or pseudonymised before it is made available. The city of Steinbach must protect this sensitive data in particular.

The companies provide the data free of charge, but can demand public recognition for their contribution. Only small and micro-enterprises may demand consideration for organisational and technical costs, plus a "reasonable margin".

3.3. Data spaces reduce compliance burdens on administration and companies

To comply with these regulations, a secure, transparent and legally compliant technical solution is required. Developing or procuring your own solutions costs time and money and does not guarantee interoperability. It is therefore not a given that the software of the city of Steinbach, its municipal utilities, neighbouring cities, Enervolt and SmartFunk (and possibly third parties) will all be compatible with each other. Bridging the gap between solutions is inefficient and extremely time-consuming. Sharing data within a data space solves many of these problems and preserves the autonomy and rights of the parties.

Data spaces ensure legal compliance if the data usage rules are legally compliant. At data space level, it is possible to define which actors are authorised to access data and under what conditions, for example following a Data Act request. In the event of new regulations, data exchange remains compliant if the rules are updated. Pre-agreed guidelines speed up the creation, review and approval of requests. This significantly reduces the burden on administration and companies.

3.4. Data spaces and data trustees: trust for authorities and companies

Additional data sources can be connected as required, even if they do not participate in the data space. For example, through data trustees who manage and protect data or rights to data on behalf of others. Data trustees such as those involved in the EuroDaT (https://www.eurodat.org/) funding project offer several useful functions for disaster prevention: they aggregate data (e.g. from different companies), anonymise and pseudonymise personal data, issue protected billing environments and enable "compute to data". Sensitive data is transferred to a protected environment where it is processed. Only the results are passed on.

In disaster situations, transparency and trust are essential, as every verification or authentication step costs time and effort that would be better spent on crisis management. Authorities must be able to trust the data sources. Similarly, data holders, especially private companies, need to ensure who is actually accessing the data. Data spaces, following Gaia-X concepts, offer a robust solution here with an integrated trust framework and verified, sovereign identities that automatically ensure the integrity and trustworthiness of data and actors.

4. How the Data Act makes it easier to switch providers

With the Data Act, the EU wants to strengthen the exchange and use of data. This section examines the regulations on interoperability and provider changes. The aim of these regulations is in particular to make it easier for customers to switch providers and use several services at the same time. This can make a significant contribution to greater control and flexibility for users and to strengthening competition and innovation in the European data economy.

4.1. The goal: removing barriers to switching

In the current data economy, dependencies on large platform operators have arisen in many places, as switching providers is often associated with high costs and complex migration processes. Challenges such as a lack of standards and restrictive contractual clauses often make switching even more difficult. The resulting "vendor lock-in" sometimes leads to negative consequences for customers. These can include excessive prices and inadequate services, for example services that fall short of the desired level of data protection. In order to reduce such dependencies, the Data Act provides for new regulations to reduce barriers to switching and thus make it much easier to change providers. Technical and contractual requirements are intended to give customers more freedom to choose the best provider for them.

4.2. The subject matter: “Data processing services”

The regulations are aimed at providers of data processing services, which are a "considerable number of services with a very wide range of different purposes" (recital 81 DA). Almost any service that involves the handling of data (including "the collection, organisation, structuring, storage, adaptation or alteration" of data (Article 2(7) DA) can be considered a data processing service. Clear examples include services that can be categorised as "Infrastructure-as-a-Service" (IaaS), "Platform-as-a-Service" (PaaS) and "Software-as-a-Service" (SaaS) (recital 81 DA). However, numerous other categories of services are also affected by the regulations. All input and output data generated through the use of these services, as well as metadata, are covered. The only exception is data that falls under the intellectual property or business secrets of the provider. Test versions or customised products are again largely exempt from the new regulations. However, some requirements, such as the provision of open interfaces and the exportability of data in machine-readable formats, remain.

4.3. One solution: predefined contractual clauses for easy switching

The Data Act obliges most providers of data processing services to contractually regulate the switch to other service providers with their customers. Many contract contents are specified. For example, it is stipulated that in the event of a switch at the customer's request, "all exportable data and digital assets" (Article 25(2) letter a DA) must be transferred to a service provider named by the customer or to an "ICT infrastructure on the customer's own premises" (Article 25(2) letter a DA). As a rule, exportable data must be provided in a common machine-readable format (Article 30(5) DA). There is a maximum period of 30 days for the transfer after the expiry of a maximum notice period of 2 months (Article 25(2) letter a DA). In addition, care and security requirements must be met when switching (Article 25(2) letter a. no. ii -iv

DA). Fees for the bill of exchange may not exceed the costs of the bill of exchange until 12 January 2027 (Article 29(3) DA). Thereafter, they must be completely cancelled (Article 29(1) DA). Only if data is not used for switching but for parallel use of data processing services may charges be levied in the amount of the provider's own costs (Article 34(2) DA). In the long term, this means that providers of data processing services must create cost-efficient switching options. The Data Act also protects companies from unfair contractual conditions. Providers with excessive market power may no longer impose one-sided "take-it-or-leave-it" conditions. Contractual clauses that unreasonably penalise companies can be declared null and void in future (Article 13 DA).

4.4. Another means: information and transparency obligations

To make it easier to switch providers, providers must also fulfil information and transparency obligations. For example, an "online register" must be maintained, which also contains information "on all data structures and data formats" (Article 26 letter b. DA) that are necessary for switching. Furthermore, information must also be provided on "available switching and transmission methods and formats as well as restrictions and technical limitations" (Article 26 letter a. DA).

4.5. Reducing technical hurdles and interoperability

The Data Act specifically addresses technical hurdles that stand in the way of switching providers. For example, providers of data processing services must generally provide their customers with open interfaces for switching providers (Article 30(2) DA). In addition, providers of data processing services must generally fulfil certain interoperability obligations. A central aspect here is "functional equivalence" (Article 2(37) DA): After switching to a service of the same type, customers should receive the same results with the same input. Functional equivalence therefore means that an application or service continues to have the same functional characteristics after a change and that users can maintain the same workflows, regardless of which provider provides the technical infrastructure. The relevant specifications and standards are listed by the EU in a specially created central database (Article 30(3) DA). The specification can be formulated by European standardisation bodies on behalf of the EU Commission (Article 33(4) DA). In certain cases, the formulation can also be carried out by the EU Commission itself within the framework of corresponding legal acts (Article 33(5) DA). The European Digital Innovation Board, in which acatech is represented alongside other stakeholders, must also be involved in these legal acts.

5. Conclusions

The EU Data Act introduces ambitious regulatory requirements that aim to reshape the way data is accessed, shared and reused across sectors. While these obligations pose significant technical, legal and organisational challenges, they also open the door to entirely new data-driven business models, services and forms of cooperation. This final section summarises the main implications of the Data Act for different data sharing contexts and points to concrete opportunities that can arise if companies and institutions actively engage with the new rules.

B2C, B2B data sharing

The Data Act sets out far-reaching obligations for the provision of usage data. These are a challenge for manufacturers of networked products and connected services – for example, products in the Internet of Things. However, the new obligations are also an opportunity for the aforementioned manufacturers and providers, as well as for users and organisations that can process usage data.

Manufacturers of connected products can demand a margin if they pass on usage data to third parties. In addition, their products can be upgraded through new downstream data utilisation. Users, in turn, can sell their data and make it available for useful services. Third parties that process data can use data for their business or public benefit purposes, provided this is desired by the users.

The Data Act can therefore provide an impetus to strengthen data exchange for the economy and the common good. In order to make use of this impetus, interested organisations need to look at the technologies for data exchange in particular. Particularly relevant in this context are the data spaces that are currently being developed, which provide the basis for transparent, secure and sovereign data exchange.

B2G data sharing

The Data Act formalises a right of access for public authorities to privately held data in cases of exceptional need. This marks a significant shift towards institutionalising public-private data collaboration for the common good. For companies, this creates a duty to be prepared for such requests—with clear internal processes, documentation and legal evaluation. At the same time, this provision can help governments respond more effectively to crises and better fulfil their public tasks, as shown in case of disaster management. Data spaces, in combination with trustworthy intermediaries like data trustees, can play a key role in reducing friction in B2G data exchange and enabling secure, scalable and compliant cooperation models.

Provider switching

The Data Act creates comprehensive obligations to provide user-generated data – both to authorities (see Section 0) and to users and third parties (see Section 2). The Data Act also aims to remove barriers to switching data processing services. In future, numerous companies will have to ensure easy switching

through appropriate contractual provisions, information offerings and the interoperability of their services. This can make a significant contribution to giving customers of data processing services a new level of self-determination. Dependencies, such as those that exist in many places, particularly in relation to large providers, could thus be reduced and a more favourable environment for competition created. This should ultimately have a positive impact on the innovative strength and prosperity of the European data economy.

It is evident that the Data Act is a regulatory initiative of considerable ambition, introducing novel obligations and privileges for all relevant parties and thereby redefining the management of data. It is imperative to acknowledge the ensuing technical challenges that must be addressed to ensure the effective functioning of a modern data ecosystem. As discussed in this article, the concept of Data Spaces is a satisfactory solution to fulfil the requirements of the Data Act.

Authors:

Dr. Abel Reiberg

Acatech – national academy of science and engineering, project lead & coordinator Gaia-X-Hub Germany

Marco Mitrovic

Acatech – national academy of science and engineering, scientific advisor Gaia-X funding project & Gaia-X-Hub Germany

Dr. Karl Wienand,

Acatech – national academy of science and engineering, scientific advisor Gaia-X funding project & Gaia-X-Hub Germany