Internet of Things Data within the Context of the Data Act: Between Opportunities and Obstacles

Prisca von Hagen

Abstract

Chapter 2 of the Data Act regulates access to data generated during the use of Internet of Things products. It is the first major legislative push to regulate broad data access rights. This article provides an overview of the regulatory structure of data access under the Data Act, as well as an analysis of some of the essential issues. The Data Act establishes a three-party constellation between the "user", the "data holder", and third parties as "data recipients". The article describes the relationship between them and explains the rights and obligations of each party. The Data Act also interacts with other data regulation, such as the GDPR, which is discussed below. The European Commission aims to enable users to make a self-determined decision about access to the data they generate. This decision should lead to more data being made accessible. However, there are difficulties that need to be taken into account. These include, for instance, informing users about the modalities of their data access. Past discussions about the possible need for data ownership had been halted prior to the Data Act. With the new legislation, questions about its role in creating ownership-like position through the back door picked up this topic again. Therefore, this article outlines the discussion on whether the provisions in the Data Act possibly enable such a position and how the control over the data is actually distributed.

1. Introduction

The Data Act (DA, Regulation 2023/2854) came into force in January 2024 after a 2-year legislative process. Following a transition period, it will take effect in September 2025. Among other regulatory areas, it details data access rights that are aimed at enabling users of Internet of Things (IoT) products (i.e. products that are connected to the internet and work together as a network) to access the data they generate more easily. This marks the

first introduction of such broad data access rights. The access is intended to enable more extensive data usage. However, the DA's regulations also create obstacles that may undermine its goals. The purpose of this chapter is to present the regulatory content of the final draft and to summarise the most important points of discussion, which could also hinder the effectiveness of the DA.

2. The concept of the DA

European legislators are confronted with the issue of data not being fully used within the European internal market. According to the European Commission (2022a), 80% of industrial data remain unexploited. The lack of data use is a complex problem for many reasons and one that has multi-dimensional effects. Therefore, it requires a range of solutions to tackle the problem, of which the DA is one part.

2.1 Reasons for the lack of data sharing

Thus far, individual large companies have generally had de facto control over data. Manufacturers of IoT products, for instance, can design them so that only they can access the data (Kerber, 2022, p. 4; Eckard and Kerber, 2024, p. 120). There has also been a lack of relevant regulation that would incentivise or oblige companies to share data. Although there are, at least, regulations governing the requirements for processing personal data, this has not thus far been the case for non-personal data (Eckard and Kerber, 2024, p. 115).

The European Commission (2020) has also identified various reasons for the lack of data sharing. Competitive pressure between companies incentivises competitors not to cede any economic advantages (European Commission, 2020, p. 8). In addition, there is uncertainty as to whether the contractual partner who gets access to the data will use it in accordance with the contract (European Commission, 2020, pp. 8–9).

2.2 Effects of the lack of data sharing

The problems caused by the lack of sharing of IoT data can be divided into two categories (Kerber, 2022, p. 4). First, the users of IoT products cannot,

themselves, utilize the data, which raises a question of fairness. Although the users generate the data by using their IoT products (recital 6 DA), the manufacturers benefit from the users' data through data-driven business models (Podszun and Pfeifer, 2022, p. 953). However, the user may have an economic interest in offering the data on the data market themselves, or at least in participating in the profits generated by their data (Podszun and Pfeifer, 2022, p. 953).

Second, the lack of data sharing prevents third parties from using the data. This hinders the emergence of secondary markets, such as repair services (Kerber, 2022, p. 5; Podszun and Pfeifer, 2022, p. 953). Meanwhile, being the sole party that holds the data, puts individual market participants in a much better position (European Commission, 2020, p. 9): They can unilaterally determine the conditions of data transfer, and have an innovation advantage (European Commission, 2020, p. 8). Overall, this means that potential value-creation opportunities are missed (Kerber, 2022, p. 5).

2.3 Approaches of the European legislator

The European Commission (2020) has recognised these issues and tackled them with the development of the European Data Strategy. The European Data Strategy is intended to supplement measures such as the introduction of the General Data Protection Regulation (GDPR, Regulation 2016/679)[1] to establish a trusting and functioning European data space. Building on the Data Strategy, the European legislator first introduced the Data Governance Act (DGA, Regulation 2022/868)[2], which regulates the infrastructure required to share data. The introduction of the DGA was subsequently followed by the DA.

2.3.1 The European Data Strategy

The European Data Strategy aims to make personal and non-personal data more usable (European Commission, 2020, pp. 4–5). The strategy is intended to secure economic and social welfare within the European Union

1 For more information on the GDPR, see Chapter 14 'EU data protection law in action: introducing the GDPR' by Julia Krämer.

2 For more information on the DGA, see Chapter 11 'The Data Governance Act – Is "trust" the key for incentivising data sharing?' by Lucie Antoine.

(European Commission, 2020, p. 4). In addition to economic considerations, the European Commission (2020, p. 3) has also focused on using the data for general welfare purposes, such as tackling climate change.

According to the European Commission (2020, p. 4), standardised data regulations are important to the creation of a single market for data.

The European Data Strategy contains four pillars outlining specific measures (European Commission, 2020, p. 11). The first and the third pillars of the strategy form the basis for the regulation of IoT data. In the first pillar, the European Commission (2020) has stated that they would like to develop a horizontal legal framework, covering all sectors, for the use of and access to data. They also announced that they want to regulate data governance (European Commission, 2020, pp. 8–9), which was implemented shortly afterwards through the DGA and the regulations on data intermediation services introduced therein. Data intermediation services can be helpful in ensuring the use of data, for example by establishing contact between parties and helping to anonymize the data (cf. recital 26 DA). In this pillar, the European Commission (2020, pp. 7–8) has also anchored the idea of adopting a Data Act that promotes the sharing of data in business-to-government (B2G) and business-to-business (B2B) relationships. The measures of the third pillar furthermore aim to strengthen individuals' control over their data in the future (European Commission, 2020, pp. 20 ff.). The European Commission (2020, p. 20) notes in the first pillar that increased control can be achieved through the DA.

In addition to the horizontal regulations that apply across all sectors, within the fourth pillar, vertical regulations that focus on access to data directly in relation to nine sectors already identified (e.g. the health data space or the mobility data space) are also considered (European Commission, 2020, pp. 21 ff.).

2.3.2 Basic idea of the DA with regard to IoT data

The second chapter of the DA aims to ensure that more data generated by IoT products are made accessible. The users of IoT products, who can be both natural persons and legal entities such as companies, are granted sovereignty over the data generated by their use (recital 15, 18 DA; Kerber, 2022, p. 5). The DA enables users to access the data, use it for lawful purposes (recital 30 DA) and permits third parties to use it at the user's request. The DA is the first legislation to regulate non-personal data (Eckard and Kerber, 2024, p. 114). The European Commission (cf. 2017, p. 13) has

already considered the question of whether those involved in the generation of the data should also decide what happens to it. It is based on the idea that it is only fair if those who are actively involved in the production have access to and can use the data (recital 6 DA; Kerber, 2022, p. 5).

This general allocation of access rights to IoT data is intended to make more data available and stimulate the data economy (recital 6 DA). It is assumed that users have "data literacy", which enables them to assess the value of their data and thus motivates them to make it available to third parties as well (recital 19 DA; Kerber, 2022, p. 5). The DA aims to further promote this data expertise (recital 19 DA). The granting of usage options to third parties includes support for secondary services (e.g. repairs and maintenance) and the development of innovative business models (cf. recital 19 DA).

It is noteworthy that the European legislator is not merely aiming to compensate for a market failure but to completely restructure the data market (Metzger and Schweizer, 2023, pp. 49 ff.; Hennemann and Steinrötter, 2024, p. 6). The regulation intends to break up larger companies' "gatekeeper" position (cf. recital 40 DA; Metzger and Schweizer, 2023, pp. 47, 49) and plans to redesign the market by offering incentives to users (Hennemann and Steinrötter, 2024, p. 6).

The regulations regarding IoT data will be added by an unfairness test for data usage agreements and other contracts related to data between two enterprises in Article 13 DA.

In addition to chapter 2, the DA includes other areas, such as data access in the G2B relationship in chapter 5, and requirements for the interoperability of data processing services, such as cloud providers in chapter 8.

3. The design of the IoT data access

3.1 Scope of application: what data are covered?

The right of access relates to personal and non-personal data from IoT products, which include smart household appliances (e.g. a networked refrigerator) as well as "smart agricultural and industrial machinery" (cf. recital 14 DA).

According to Articles 3 (1) and 4 (1) DA, the right to access includes the product data, the associated service data and the metadata required for its use. The term product data refers to information generated by using the IoT

product (recital 15, Art. 2 No. 16 DA). Data generation during use means that data are generated directly while the product is being actively used. Data access includes data generated indirectly through use (e.g. data related to the environment; recital 15 DA). Data that are merely a consequence of use are also expressly included (recital 15 DA). For example, the access claim also relates to data automatically generated by sensors and recorded in the background (recital 15 DA). In this respect, it is irrelevant if the data are generated when the product is inactive, for instance, while in stand-by mode (recital 15 DA).

The access rights also relate to connected service data (Art. 2 No. 6 DA). Connected service data are generated during the provision of a digital service, such as software (cf. Art. 2 No. 6 DA) necessary for the operation of the product connected to the IoT product (recital 15 DA). Furthermore, the data do not necessarily have to be modified to be covered by the scope of the DA, meaning that raw data are also included (recital 15 DA).

Metadata as additional data is important for understanding and using the generated data. Examples of metadata include timestamps, which are required to place the data in correct relation to one another (recital 15 DA).

However, if the data holder makes significant investments in analysing the data to gain further insights, this derived information is no longer part of the scope of application (recital 15 DA).

3.2 Relevant actors

The DA constructs a three-party constellation between the "user", the "data holder", and third parties as "data recipients".

As noted above, the user can be a natural person or a legal entity, such as a company (Art. 2 No. 12 DA). The decisive factor is the user's ownership of the corresponding product or at least the right for temporary use (Art. 2 No. 12 DA). Included are, for example, farmers who lease smart tractors that they need for work (Specht-Riemenschneider, 2022b, p. 813).

Data holders, who most often are the manufacturers of smart products (Specht-Riemenschneider, 2022b, p. 813), are obliged to share the data (cf. recital 5 DA). The key factor is their de facto control over the data generated (Specht-Riemenschneider, 2022b, p. 813). Data holders are obliged to retain the data for a reasonable period (recital 24, DA), and as soon as they delete the data, they lose their status as data holders. (Bomhard and Merkle, 2022, pp. 173–174).

Finally, data recipients are companies or natural persons to whom the data are made available by the data holders, despite the fact that they are not product users (Art. 2 No. 14 DA). For example, companies needing the data to repair a product are considered to be data recipients (cf. recital 32 DA).

3.3 Data access of the various actors

Whereas in the past only the data holders had de facto control over (non-personal) data, a concept has now been introduced that gives the user access to the data. However, through contractual agreements with the user, the data holders can also continue to use the data (Art. 4 (13), (14) DA). The data holder is obliged to make the data available to third parties at the request of the user (Art. 5 (1) DA).

3.3.1 Data access of the user

Users should be given the power to make decisions regarding their data (cf. Podszun and Pfeifer, 2022, p. 956). Without a contractual agreement between the two parties, access to the data, in the past, depended on who had de facto access to it prior to the DA (Etzkorn, 2024, p. 118).

According to the DA (Art. 2 (2), (3) DA), the data holder must provide the user with the information necessary to gain access to their data before concluding the purchase, rental or lease agreement for the IoT product. For example, information should be provided regarding what data are generated through use, in what format they can be retrieved and how the user can gain access. It is also important that the information can be recalled not only prior to the conclusion of the contract but also later (recital 24 DA).

Data holders should consider the direct accessibility of the data already during the design process (Art. 3 (1) DA). Accessibility can be ensured, for example, via a user interface (Specht-Riemenschneider, 2022b, p. 815). If this "accessibility by design" is not possible, the user has the right under Article 4 (1) DA to have the data made accessible to them in another. It is unclear whether a so-called in situ right, which would permit the user to view the data only on the data holders' server, is sufficient (cf. Specht-Riemenschneider, 2022b, p. 816; Kerber, 2022, p. 9; Hennemann and Steinrötter, 2024, p. 3). Regardless of the form of provision, the data holder must grant access to the data free of charge (Art. 3 (1), 4 (1) DA).

Only microenterprises or small enterprises are exempt from this obligation (Art. 7 (1) DA), as the effort involved would be unreasonably high (cf. recital 41). However, the data may contain trade secrets. In this case, the user must take appropriate measures to ensure their protection (Art. 4 (6) DA).

Subsequently, the user can "use the data for any lawful purpose" (recital 30 DA), which includes commercial use (Efroni et al., 2022, p. 10; Etzkorn, 2024, pp. 120–121). However, the user is prohibited from using the data to develop a competing product (Art. 4 (10) DA).

If the product is used by multiple users (e.g. in the case of several owners) all must be given access to the generated data (recital 21 DA). In practice, this can be realised by providing the option of setting up several user accounts through which each user can access the data (recital 21 DA). If the product is resold, the data holder must provide an option for each user to delete the previously generated data (recital 21 DA).

3.3.2 Data access for data recipients

The user can decide whether the data should be shared with third parties. According to Article 5 (1) DA, the data holder must provide the data to the data recipient at the user's request in the "same quality as it is available to" them. Microenterprises or small enterprises are also excluded from this obligation under Article 7 (1) DA. The data recipient may only use the data for the purposes to which it has contractually agreed with the user. Moreover, they must adhere to further conditions, such as the protection of the data holder's trade secrets (Art. 6 (1), (2) DA). These additional conditions are intended to take into account the conflicting interests of data holders and data recipients (Etzkorn, 2024, p. 121).

Data intermediation services that can support the appropriate fulfilment of data access requests are also explicitly envisaged as potential data recipients (recital 26 DA). The consideration of intermediaries creates a close link with the DGA, which is intended to establish the appropriate infrastructure.

In contrast to the user's free access, the data recipient has a duty to compensate the data holder for the use of the data (Art. 9 (1) DA). The compensation must be "reasonable" and should ensure that data holders are incentivised to generate data (Podszun and Pfeifer, 2022, p. 957). However, it is difficult to determine when a compensation payment is reasonable (Podszun and Pfeifer, 2022, p. 957). It must be determined in each individual case whether the conditions fulfil these requirements. If the

data recipient is a small or medium enterprise or a not-for-profit research organisation, the compensation under Article 9 (4), (2) (a) DA is limited to the costs of provision.

Moreover, gatekeepers within the meaning of Article 5 (3) DA are expressly excluded from data access, as the power of gatekeepers is explicitly intended to be undermined and not manifested through further data access (cf. recital 40 DA).

3.3.3 Restrictions for the use by the data holder

Although data holders maintain de facto access to the data, they are only permitted to use it under Article 4 (13) DA if they have contractually agreed to this with the user. In practice, however, an agreement on the use of the data by the data holder will be made a condition for the purchase, rental or lease agreement (Bomhard and Merkle, 2022, p. 174; Kerber, 2022, pp. 22–23).

It is unclear whether this contract between the data holder and the user can also include a general agreement on the commercial use on the part of the data holder by passing it on to third parties (Hennemann and Steinrötter, 2024, p. 7). In any case, it is only possible within the meaning of Article 4 (14) DA if the commercial disclosure of non-personal data is for "the fulfilment of their contract with the user" (cf. Hennemann and Steinrötter, 2024, p. 7). This stipulation indicates that disclosure to third parties is subject to the narrow limits of the contract signed with the user (Hennemann and Steinrötter, 2024, p. 7). Meanwhile, the processing of personal data continues to be subject to the requirements of the GDPR. According to this, the explicit purpose of the data processing must be clear (Art. 5 (1) (b) GDPR).

4. Problematic aspects

The DA has generated significant interest both in legal studies and practice. It has raised many open questions as well as points of friction, of which the following are among the most important. This presentation, however, is not exhaustive.

4.1 Relationship of the DA to other legal regulations

A central topic of contention throughout the legislative process was the relationship with other legal regimes. For example, as the DA also regulates personal data already governed by data protection law, there are questions of demarcation with the GDPR. As manufacturers, in particular, are obliged to provide access, and the data may allow conclusions to be drawn about the functionality of products (Macher and Graf Ballestrem, 2023, p. 661), the protection of trade secrets plays a significant role. Not least, the DA complements existing digital legislation, such as the GDPR and the DGA.

4.1.1 Relationship to data protection law

The DA refers to personal and non-personal data generated during the use of IoT products. The term personal data refers to data that relate to a natural person and make it possible to identify that person (Art. 4 No. 1 GDPR). The use of IoT products easily leads to the generation of personal data, for example, when using a connected car (Steinrötter, 2023, p. 219). Data holders have an obligation to verify whether the data are personal before granting an access request (Heinzke, 2023, p. 205). In general, it is difficult for controllers to determine when the data can be used to establish a link to an individual from which their identity can be inferred. Data holders will also have problems, especially with large data sets, in drawing the line between personal and non-personal data (recital 34 DA; Bomhard and Merkle, 2022, pp. 172, 174–175; Heinzke, 2023, p. 205).

If the datasets contain personal data, the DA and GDPR apply in parallel in accordance with Article 1 (5) DA (cf. Specht-Riemenschneider, 2022b, p. 810). In case of conflicts between the legal provisions, the GDPR takes precedence pursuant to Article 1 (5) DA. According to Schmidt-Kessel (2024a), collisions should only occur rarely, as the two legal norms have different subject matters. Whereas the GDPR deals, in particular, with the right to use data, the DA contains contract law provisions (Schmidt-Kessel, 2024a, p. 127).

Nonetheless, in certain situations, the access claim causes problems that particularly concern the relationship between the GDPR and the DA (cf. Specht-Riemenschneider, 2023, pp. 664 ff.; Steinrötter, 2023, pp. 220 ff.). In addition, implementing the data access request might create data protection conflicts in some cases.

Legal Basis for Data Processing

According to the GDPR, the processing of personal data requires a legal basis, such as the data subject's consent. If the data are processed without such a legal basis, the data controller faces fines.

If the user requesting the data is the data subject within the meaning of the GDPR, the request for access to the data constitutes implied consent to data processing (Bomhard and Merkle, 2022, pp. 174–175; Specht-Riemenschneider, 2022b, p. 810).

A problem arises when the user and the data subject are not identical and the user requests access to the data for themselves or a third party (Steinrötter, 2023, p. 223; Specht-Riemenschneider, 2023, p. 665). This problem can occur, for example, if a farmer's tractor is operated by a subcontractor (cf. Zech, 2015a, p. 137). Concerning the first version of the DA, it has been discussed whether legal bases for data processing could arise from the DA itself in these cases (Specht-Riemenschneider, 2023, pp. 664 ff.; Steinrötter, 2023, p. 223). This would indicate that the data subject's consent is not required. This would benefit data holders, in particular, who would thereby make the personal data accessible on a legal basis and avoid claims for fines (Steinrötter, 2023, p. 223). However, this is rejected in the final version of the DA in recital 7 DA, which states, "[W]here the user is not the data subject, this Regulation does not create a legal basis for providing access to personal data or for making personal data available to a third party […]".

Relationship between the right to data portability and Article 4 (1) and Article 5 (1) DA

Since the introduction of the GDPR, data subjects have the right to receive their personal data in accordance with Article 20 (1) GDPR or to have them transmitted to others under Article 20 (2) GDPR. They also have the right to obtain a copy of the data processed by the controller in accordance with Article 15 (3) GDPR. Therefore, these provisions are similar to Article 4 (1) and Article 5 (1) DA, which provide the user and third parties with access to IoT data. The claims under the DA indeed have narrower provisions, such as that access must be "without undue delay" and "free of charge". In contrast, under the GDPR, the controller is given an extendable 1-month period within the meaning of Article 12 (2) GDPR and can demand a fee if the data subject exercises their right in an unreasonably excessive manner

(cf. Richter, 2022, p. 307; Steinrötter, 2023, p. 221). However, Article 1 (5) DA expressly stipulates that Articles 4, 5 DA "complement" Articles 15 and 20 GDPR. Therefore, it is positive that Article 4 (1) and Article 5 (1) DA include not only personal data but also non-personal data (cf. Steinrötter, 2023, p. 221).

Criticism of the creation of user accounts

There are data protection concerns, in particular, related to accessing data via user accounts. As described above, this procedure is intended to enable users to assert claims to data access (cf. recital 21 DA). This is important for verifying status as a user (Steinrötter, 2023, p. 222). The problem here, however, is that this creates a link between data and users, which can create a personal reference, even with data that were initially non-personal (Specht-Riemenschneider, 2023, pp. 663–664; Steinrötter, 2023, p. 222). Anonymous data access would probably have been possible, but this approach was not pursued further (Podszun and Pfeifer, 2022, p. 952).

4.1.2 Relationship to trade secret protection

The relationship between the DA and the protection of trade secrets was discussed extensively during the legislative period (cf. Hennemann and Steinrötter, 2024, pp. 3–4). The German Trade Secrets Protection Act (GeschGehG, 2019) protects trade secrets from unauthorised use, acquisition or disclosure in accordance with § 1 (1) GeschGehG. It is based on the Trade Secrets Directive. According to § 2 (1) GeschGehG, a trade secret is information that is not in public domain and that has economic value. In addition, the GeschGehG indicates that the person who knows the information must take steps to maintain secrecy.

Companies are concerned that their trade secrets will be jeopardised by the DA's access to data (Macher and Graf Ballestrem, 2023, p. 661). If information is made public, it is no longer secret, and it therefore loses its trade-secret characteristic (cf. Metzger and Schweizer, 2023, pp. 74–75). However, the data holders could use the trade secret protection argument to (unjustifiably) deny access to the data. (Macher and Graf Ballestrem, 2023, p. 661).

Data as trade secret

However, it is difficult to determine whether data are trade secrets at all (Heinzke, 2023, pp. 205–206; Grapentin, 2023, p. 174). Data must have semantic information value to be categorised as information within the meaning of the GeschGehG (cf. Zech, 2015b, p. 1156; Wiebe, 2023, p. 232; Heinzke, 2023, pp. 205–206). Therefore, there are discussions regarding the trade-secret characteristic of raw data, in particular. In part, raw data do not qualify as a trade secret because they contain no substantive information (European Commission, 2022b, p. 89). This view disregards the fact that raw data, in connection with other data, can have substantive value and can thus be protected as a trade secret (Grapentin, 2023, p. 174; Lorenzen, 2022, p. 253; Wiebe, 2023, p. 232). If, for example, raw data from CT or MRI devices (e.g. temperature and coil rotations of the machine) are linked, significant insights into the functioning of the machine can be derived (Grapentin, 2023, pp. 174–175). In addition, the commercial value, which may be very low for the individual raw data points, increases when linking these with other data (Zech, 2015b, p. 1156; Lorenzen, 2022, p. 253).

Ultimately, courts must decide whether raw data constitutes a trade secret (Metzger and Schweizer, 2023, p. 75). In the event that court proceedings are protracted, data holders could withhold the data for the duration of the proceedings (cf. Kerber, 2022, p. 12).

Approaches of the DA with regard to trade secrets

The protection of trade secrets was extensively revised between the first draft and final version of the DA (cf. Hennemann and Steinrötter 2024, pp. 3–4). Whereas trade secrets were initially only disclosed via data access in accordance with Article 4 (1) DA if the necessary measures were taken to ensure confidentiality, the hurdles for refusal are higher in the final version. Article 4 (8) DA now requires that the data holder prove that they would suffer serious economic damage if the data were to be disclosed. Accordingly, the data holder can only refuse access in individual cases. They must inform the user, in writing, of the refusal and the reasoning for it, and they must notify the competent authority. Even if the conditions for refusing access to data are now stricter, the data holder is still able to use trade secret protection against the user's claim (cf. Hennemann and Steinrötter, 2024, p. 4).

4.1.3 Relationship to database protection

Finally, the relationship between the existing database protection and the provisions of the DA is unclear. Under the Database Directive (Directive 96/9/EC), the extraction or re-utilisation of databases can be prohibited in accordance with Article 7 (1). Database protection is intended to guard the essential investments necessary to create the database (recital 40 Database Directive).

However, Article 7 of the Database Directive does not apply to the data access claims of Articles 4 (1) and 5 (1) DA, according to Article 43 DA. This indicates that the data holder is not entitled to refuse access to the data on the grounds of database rights (cf. Kim, 2024, pp. 87–88; Hennemann and Steinrötter, 2024, p. 6). Nevertheless, there is a controversy regarding the scope of application of the two legal regimes (cf. Kim, 2024, pp. 89–90). According to the DA, data should be prepared in a usable manner (recital 15 DA). If the data are the "outcome of additional investments", they are excluded from the scope of the DA (recital 15 DA). However, creating a database requires a substantial investment in accordance with Article 7 of the Database Directive. The standard is therefore in need of clarification (Kim, 2024).

4.1.4 Relationship to other existing legal instruments

The Digital Markets Act (DMA, Regulation 2022/1925) and the DGA are supplemented by the DA (cf. Specht-Riemenschneider, 2022b, p. 811). The DMA and DA, in particular, jointly pursue the goal of breaking up the accumulation of power by gatekeepers (recital 40 DA).

As noted above, the DGA establishes an infrastructure that intends to realise fairer data distribution, for example through registered or certified data intermediaries. Although the original draft focussed primarily on the promotion of secondary services (e.g. maintenance and repairs; cf. Efroni et al., 2022, p. 14), data intermediation services were included in the final version at various points and recognised as a central element in the distribution of data (cf. Art. 2 No. 10; recital 30 DA).

The European Health Data Space is currently in the legislative process and represents the first vertical regulation on access to data from the healthcare sector.

4.2 Independent decision by the user?

Another point of discussion is the extent to which the user can make independent decisions and whether the possibility of requesting access results in better data distribution. Alongside the data holder, the user is at the centre of the regulations on IoT products (Podszun and Pfeifer, 2022, p. 960). The users' decision to release the data for themselves or third parties should lead to a fairer distribution and thus to more innovation (Krämer, 2022, p. 5). This decision requires the user to be informed (Podszun and Pfeifer, 2022, pp. 960–961), as otherwise, the allocation of data value may be asymmetrical (Eckard and Kerber, 2024, pp. 128–129). However, there is a lack of information among users, particularly in B2C relationships (Kerber, 2022, p. 22). Consumers are, for instance, unaware of the value their data might generate (cf. Krämer, 2022, p. 20).

The DA introduces obligations to inform users that are intended to counteract the information asymmetry between users and data holders (cf. recital 24 DA). In addition, the contract with the data holder pursuant to Article 4 (13) DA, which is necessary for the data holder to be able to use the data, may provide users with further information such as the "envisaged uses by the IoT provider" (Leistner and Antoine, 2022, p. 92).

However, in the case of personal data, experience has already shown that data protection declarations are not read and understood in the majority of cases (Specht-Riemenschneider, 2022a, p. 139; Kerber, 2022, p. 22; Krämer, 2022, p. 9), due to the length and complexity of these texts, among other reasons (cf. Rakoff, 1983, p. 1226; Ben-Shahar, 2009, pp. 13–14). This is in keeping with observations made regarding contractual clauses (cf. Ben-Shahar, 2009, p. 1; Bakos, Marotta-Wurgler and Trossen, 2014, p. 1). For various reasons (e.g. rationality considerations), it may make sense not to read the conditions (Ben-Shahar, 2009, p. 14), when, for example, the cost of reading exceeds the expected benefits (Hillman and Rachlinski, 2002, p. 446).

The information problem is exacerbated by the fact that personal and non-personal data in datasets generated by IoT products are, as noted above, difficult to distinguish from one another (cf. Richter, 2022, p. 304; Bomhard and Merkle, 2022, p. 172). Therefore, it is to be expected that data holders will apply information requirements cumulatively to avoid legal consequences (Steinrötter, 2023, p. 219). In addition, the data holder may be required to comply with further information requirements, for example, under consumer contract law (Rammos and Wilken, 2022, p. 1243).

Therefore, the effectiveness of the information obligation is highly questionable, especially with regard to the B2C sector (cf. Heinzke, 2023, p. 208). In any case, it is closer to the assumption that the user does not perceive the information in this case, either, and that they conclude contracts with the data holders without dealing with the content (Hennemann and Steinrötter, 2022, p. 1483; Podszun and Pfeifer, 2022, pp. 960–961).

4.3 "Property right" of the user versus technical–factual control of the data holder

A much-discussed question throughout the legislative process was to whom the DA assigns rights and what the effects are on the power relations.

The extent to which "ownership" of data, in the form of a transferable exclusive right that protects the data in particular from unauthorised use, makes sense and can promote the data economy has already been discussed (cf. Dorner, 2014; Zech, 2015a; Drexl, 2017). The exclusive right of ownership means that the right holder has a legal defence against anyone (cf. Zech, 2015a, p. 140) – that is to say they also have the right to determine who uses the data, and they can assert claims in the event of unauthorised use. However, to whom this transferable, exclusive right should be assigned, given the multitude of parties involved, (e.g. manufacturers or users), is challenging (cf. Wiebe, 2016, p. 883; Drexl, 2017, p. 277). Data can contain information at the semantic level. An exclusive right of use can therefore prevent access to information and even lead to a monopolisation of information (Wiebe, 2016, pp. 881–882). Due to existing problems, the discussion was settled, and the focus has now shifted to data access rights (cf. Wiebe, 2023, p. 1569; Specht-Riemenschneider, 2022b, p. 810; Hennemann and Steinrötter, 2022, p. 148).

The implementation of exclusive rights to data was explicitly avoided when the DA was introduced (cf. recital 6 DA). However, whether the design of the DA results either in exclusive rights for the user (cf. Bomhard and Merkle, 2022, p. 175; Hennemann and Steinrötter, 2022, p. 148) or, conversely, establishes an exclusive position for data holders by strengthening their de facto control (cf. Kerber, 2022, pp. 15 ff.; Specht-Riemenschneider, 2022b, p. 818) is now being discussed.

4.3.1 "Ownership-like" position of the user?

According to the first approach, Article 4 (13) DA in particular, according to which the data holder may only use non-personal data on the basis of a contract concluded with the user, establishes an ownership-like position (cf. Bomhard and Merkle, 2022, p. 175). According to this argument, excluding the data holder if the user does not agree to a contract with them creates an exclusive position of the user that is akin to an absolute right (Bomhard and Merkle, 2022, p. 175; Hennemann and Steinrötter, 2022, p. 1483).

This is countered by the argument that the DA is only a reaction to the de facto control of data holders and does not aim to introduce a right similar to ownership, but merely to distribute data more fairly (cf. Metzger and Schweitzer, 2023, p. 50). The data are not directly assigned to the user. Rather, the user only has access to the data if they actively make use of their access rights (Specht-Riemenschneider, 2022b, p. 815).

The DA expressly prefers simple access rights to the granting of exclusive access and usage rights (recital 6 DA). In addition, the trilogue procedure of the European legislator included Article 4 (14) DA, which stipulates that third parties who obtain data from the data holders must be contractually obliged not to share it. However, this would not be necessary if an exclusive right of use had been established as a right similar to ownership (Schmidt-Kessel, 2024b, p. 78).

4.3.2 (Exclusive) de facto position of the data holder?

The previous argument against the establishment of users' ownership-like rights is also the argument for the contrary approach, which posits that the DA would result in (exclusive) de facto rule by the data holders (cf. Kerber, 2022, pp. 15 ff.; Specht-Riemenschneider, 2022b, p. 818). Whereas de facto control over the data was previously purely factual, the DA regards this as a given (Martens, 2023, p. 19). According to some scholars, this is even seen as a legal position equivalent to the holder of an IP right (cf. Eckard and Kerber, 2024, pp. 123–124; Kerber, 2022, p. 17). As explained above, de facto control over the data remains with the data holder (cf. Podszun and Pfeifer, 2022, p. 956).

The data holder is thus authorised to decide which data are collected (Specht-Riemenschneider, 2022a, p. 139). They can also delete the data at their discretion, provided they have complied with a reasonable storage period (cf. recital 24 DA). In addition, Article 11 (2) DA introduces safeguards

allowing data holders to require users and recipients to take various actions in case of unlawful use, such as deletion of the data provided (cf. Kerber, 2022, p. 16; Specht-Riemenschneider, 2022a, p. 137). The data holder can also comply with the user's request for access if the user can access the data on the data holder's server. In this case, the data would remain under the control of the data holder (Specht-Riemenschneider, 2022a, p. 139).

The use of non-personal data by the data holder pursuant to Article 4 (13) DA is only possible if the data holder and the user have concluded a corresponding contract. Such a contract would give the user some control. However, these contracts can be made a condition for the IoT product contract without restrictions (Specht-Riemenschneider, 2022a, p. 139).

5. Conclusion

With the intention of making more data usable and disrupting the gatekeeper position held by large companies, the European legislator is pursuing an important goal. However, the specific form of the legislation raises doubts about its effectiveness (cf. Kerber, 2022, p. 3; Specht-Riemenschneider, 2022b, p. 810; Wiebe, 2023, p. 1569; Heinzke, 2023, p. 208). Although positive changes have already been made in the course of the legislative process, both the structure of the parties involved, as established by the DA, and the individual provisions are subject to criticism.

Structurally, it is questionable whether the de facto position of the data holder is strengthened without strengthening the user. For example, tighter requirements for the contract in accordance with Article 4 (13) DA (Specht-Riemenschneider, 2022b, pp. 818–819), would accomplish the latter. The fact that the user's ability to make decisions is limited due to a lack of information, especially in a B2C relationship, will also reduce the benefits of the DA (cf. Eckard and Kerber, 2024, p. 128; Metzger and Schweizer, 2023, pp. 56–57).

Furthermore, legal uncertainty regarding individual provisions of the DA is challenging. If, for example, compensation is demanded for making data accessible to a data recipient in accordance with Article 9 (1) DA and the parties cannot reach an agreement, a lengthy process that delays data access might be initiated (cf. Podszun and Pfeifer, 2022, p. 957). Even in cases where it is necessary to determine whether the necessary measures have been taken to protect a trade secret, a court will have to decide (Metzger and Schweitzer, 2023, p. 75). Delay will be a particular concern if the data

must be made accessible to a third party who is a competitor of the data holder (Podszun and Pfeifer, 2022, p. 959).

Although the DA has been in force since the beginning of 2024, what is certain is that the practical benefits of this legislation – in particular its potential to stimulate the data market – will become apparent in September 2025, when it takes effect.

References

Bakos, Y., Marotta-Wurgler, F. and Trossen, D. R. (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *Journal of Legal Studies,* 43(1), pp. 1–35.

Ben-Shahar, O. (2009) 'The Myth of the 'Opportunity to Read' in Contract Law', *European Review of Contact Law*, 5(1), pp. 1–28.

Bomhard, D. and Merkle, M. (2022) 'Der Entwurf eines EU Data Acts', *Recht Digital*, 2(4), pp. 168–176.

'Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases' (1996) *Official Journal* L77, 27 March, pp. 20–28 [Online] Available at: http://data.europa.eu/eli/dir/1996/9/oj (Accessed: 30 January 2025).

Dorner, M. (2014) 'Big Data und „Dateneigentum"', *Computer und Recht*, 30(9), pp. 617–628.

Drexl, J. (2017) 'Designing Competitive Markets for Industrial Data', *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, 8(4), pp. 257–292.

Eckard, M. and Kerber, W. (2024) 'Property rights theory, bundles of rights on IoT data, and the EU Data Act', *European Journal of Law and Economics*, 57(1–2), pp. 113–143.

Efroni, Z., von Hagen, P., Völzmann, L., Peter, R. and Sattorov, M. (2022) *Position Paper of the Weizenbaum Institute – Regarding Data Act* [Online]. Available at: https://www.weizenbaum-library.de/handle/id/125 (Accessed: 30 January 2025).

European Commission (2017) *Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Building a European data economy'* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0009 (Accessed: 30 January 2025).

European Commission (2020) *Communication from the Commission to the European Economic and Social Committee and the Committee of the Regions: A European strategy for data* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 (Accessed: 30 January 2025).

European Commission (2022a) *Press release regarding the Data Act, 23.02.2022* [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 (Accessed: 30 January 2025).

European Commission (2022b) *Study on the legal protection of trade secrets in the context of the data economy (2022)* [Online]. Available at: https://beck-link.de/an8vn (Accessed: 30 January 2025).

Etzkorn, P. (2024) 'Datenzugangsansprüche nach dem Data Act', *Recht Digital*, 4(3), pp. 116–123.

'Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (GeschGehG)' (2019) *Bundesgesetzblatt I 2019*, pp. 466-472.

Grapentin, S. (2023) 'Datenzugangsansprüche und Geschäftsgeheimnisse der Hersteller im Lichte des Data Act', *Recht Digital*, 3(4), pp. 173–182.

Heinzke, P. (2023) 'Data Act: Auf dem Weg zur europäischen Datenwirtschaft', *Betriebs Berater*, 2023(5), pp. 201–209.

Hennemann, M. and Steinrötter, B. (2022) 'Data Act – Fundament des neuen EU-Datenwirtschaftsrechts', *Neue Juristische Wochenschrift*, 75(21), pp. 1481–1485.

Hennemann, M. and Steinrötter, B. (2024) 'Der Data Act', *Neue Juristische Wochenschrift,* 77(1), pp. 1–8.

Hillmann, R. and Rachlinski, J. (2002) 'Standard-Form Contract in the Electronic Age', *N.Y.U. Law Review*, 77(2), pp. 429–495.

Kerber, W. (2022) 'Governance of IoT Data: Why the EU Data Act will not Fulfil its Objectives', *GRUR International Journal of European and International IP Law*, 72(2), pp. 120–135.

Kim, D. (2024) 'Der Datenbankschutz sui generis nach dem Data Act', *Multimedia und Recht*, 27(MMR-Beilage), pp. 87–91.

Krämer, J. (2022) *Improving the economic effectiveness of the B2B and B2C data sharing obligations in the proposed Data Act* [Online]. Available at: https://cerre.eu/wp-content/uploads/2022/11/ImproveEffectiveness_DataAct_Final.pdf (Accessed: 30 January 2025).

Leistner, M. and Antoine, L. (2022) *IPR and the use of open data and data sharing initiatives by public and private actors* [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf (Accessed: 30 January 2025).

Lorenzen, B. (2022) 'Geschäftsgeheimnisschutz und Data Act', *Zeitschrift für geistiges Eigentum*, 14(3), pp. 250–267.

Macher, E. and Graf Ballestrem, J. (2023) 'Der neue EU Data Act: Zugang zu Daten – und Geschäftsgeheimnissen?', *Gewerblicher Rechtsschutz und Urheberrecht in der Praxis*, 125(9), pp. 661–664.

Martens, B. (2023) *Pro- and anti-competitive provisions in the proposed European Union Data Act (2023)* [Online]. Available at: https://www.bruegel.org/sites/default/files/2023-01/WP%2001.pdf (Accessed: 30 January 2025).

Metzger, A. and Schweitzer, H. (2023) 'Shaping Markets: A Critical Evaluation of the Draft Data Act', *Zeitschrift für Europäisches Privatrecht*, 31(1), pp. 42–80.

Podszun, R. and Pfeifer, C. (2022) 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission', *Gewerblicher Rechtsschutz und Urheberrecht*, 124(13), pp. 953–961.

Rakoff, T. D. (1983) 'Contracts of Adhesion: An Essay in Reconstruction', *Harvard Law Review*, 96(4), pp. 1173–1284.

Rammos, T. and Wilken, T. (2022) 'Der Data Act – Chancen und Risiken für Unternehmen durch das geplante europäische Datengesetz', *Der Betrieb*, 20, pp. 1241–1249.

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (2016) *Official Journal* L119, 4 May, pp. 1–88 [Online]. Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 30 January 2025).

'Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)' (2022) *Official Journal* L152, 3 June, pp. 1–44. [Online]. Available at: http://data.europa.eu/eli/reg/2022/868/oj (Accessed: 30 January 2025).

'Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)' (2022) *Official Journal* L265, 12 October, pp. 1–66. [Online]. Available at: http://data.europa.eu/eli/reg/2022/1925/oj (Accessed: 30 January 2025).

'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 (Data Act)' (2023) *Official Journal* L, 22 December, pp. 1–71. [Online]. Available at: http://data.europa.eu/eli/reg/2023/2854/oj (Accessed: 30 January 2025).

Richter, S. (2022) 'Der schmale Grad zwischen Schutz personenbezogener Daten und Datenkommerzialisierung – Eine Analyse des Zusammenspiels des Entwurfs zum Data Act und der GDPR' in Heinze, C. (ed.) *Tagungsband Herbstakademie 2022 – Daten, Plattformen und KI als Dreiklang unserer Zeit*. Oldenburg, Germany: Oldenburger Verlag für Wirtschaft, Informatik und Recht, pp. 299–311.

Schmidt-Kessel, M. (2024a) 'Einordnung des Data Act in das Mehrebenensystem des Unionsprivatrechts', *Multimedia und Recht*, 27(MMR-Beilage), pp. 122–128.

Schmidt-Kessel, M. (2024b) 'Heraus- und Weitergabe von IoT-Gerätedaten', *Multimedia und Recht*, 27(MMR-Beilage), pp. 75–82.

Specht-Riemenschneider, L. (2022a). 'Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation?' *Zeitschrift für Rechtspolitik*, 55(5), pp. 137–140.

Specht-Riemenschneider, L. (2022b) 'Der Entwurf des Data Act', *Multimedia und Recht-Beilage*, 25(MMR-Beilage), pp. 809–826.

Specht-Riemenschneider, L. (2023) 'Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und GDPR', *Zeitschrift für Europäisches Privatrecht*, 31(3), pp. 638–669.

Steinrötter, B. (2023) 'Verhältnis Data Act und DS-GVO: Zugleich ein Beitrag zur Konkurrenzlehre im Rahmen der EU-Digitalgesetzgebung', *Gewerblicher Rechtsschutz und Urheberrecht*, 125(4), pp. 216–226.

Wiebe, A. (2016) 'Protection of industrial data – a new property right for the digital economy?', *GRUR International Journal of European and International IP Law*, 65(10), pp. 877–884.

Wiebe, A. (2023) 'The Data Act Proposal – Access rights at the intersection with Database Rights and Trade Secret Protection', *Gewerblicher Rechtsschutz und Urheberrecht*, 125(4), pp. 227–238.

Zech, H. (2015a) 'Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers"', *Computer und Recht*, 31(3), pp. 137–146.

Zech, H. (2015b) '"Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnemarkt', *Gewerblicher Rechtsschutz und Urheberrecht*, 117(2), pp. 1151–1160.