Journal of Universal Computer Science, vol. 30, no. 9 (2024), 1205-1223
submitted: 27/9/2023, accepted: 30/5/2024, appeared: 14/9/2024 CC BY-ND 4.0

„Stop it, Fridge!“ – Legally Secure and Interest-Based Data Sharing in the Age of Modern (Cyber) Technology

Dagmar Gesmann-Nuissl
(Professorship for Private Law and Intellectual Property Rights,
Chemnitz University of Technology, Chemnitz, Germany,
https://orcid.org/0000-0003-0092-7845, dagmar.gesmann@wiwi.tu-chemnitz.de)

Ines Maria Tacke
(Professorship for Private Law and Intellectual Property Rights,
Chemnitz University of Technology, Chemnitz, Germany,
https://orcid.org/0009-0006-0023-4992, ines-maria.tacke@wiwi.tu-chemnitz.de)

Stefanie Meyer
(Professorship for Private Law and Intellectual Property Rights,
Chemnitz University of Technology, Chemnitz, Germany,
https://orcid.org/0000-0001-9988-9564, stefanie.meyer@wiwi.tu-chemnitz.de)

Abstract: As part of the modern Internet, Internet of Things (IoT) devices are particularly indispensable. The reason these devices fit so seamlessly into our everyday lives is that they constantly generate, process and evaluate data (using the Internet) and can react smoothly to circumstances – such as the refrigerator that automatically reorders missing food or a maintenance monitory system in smart homes that assigns digital maintenance orders to the responsible tradesmen. These data flows and underlying information are the subject of a wide variety of legal projects: Europe aims to become a pioneer of the data economy by providing access to available data accessible for further value and business models. Subject matter includes both personal data and non-personal data, such as IoT machine data. To achieve these political-economic goals, but also to ensure the interests of users and especially manufacturers in confidentiality and fair competition, we introduce the person of the neutral data intermediary: the data innovator.

Keywords: IoT devices; data economy; data act; data intermediary; data innovator
Categories: A.0, A.m, E.m
DOI: 10.3897/jucs.132132

“Cyber-Security is much more than a matter of IT.”
— Stephane Nappo

1 Introduction

The concept of the Internet of Things (IoT) has become an integral part of today's parlance - whether from the perspective of users who want to effectively integrate smart IoT devices into their everyday lives or from the perspective of entrepreneurs who develop such devices. The idea as such now dates back more than 30 years: Mark Weiser first discussed the vision of "ubiquitous computing" in 1991, in which objects

equipped with sensors are integrated into their environment in such a way that they are perceived as ubiquitous [Weiser, 1999]. This vision has remained essentially the same despite the change in terminology. IoT is also generally understood as the possibility of interconnecting objects with each other (using the Internet) [Bräutigam, 2017]. In an industrial context, this is specified as "Industry 4.0", while in a private context it is referred to as "smart products" [Bräutigam and Klindt, 2015]. The ubiquity or interoperability of objects is primarily ensured by the exchange of data due to progressive digitization and networking. This exchange of data using the Internet causes social and political debates in two respects: On the one hand, with regard to cyber security and the privacy of the individual user; on the other hand, there is a discussion of data as the "raw material of the future" and the innovative power of data exchange is recognized [BMBF - German Federal Ministry of Education and Research, 2021].

Consequently, IoT devices in particular and the use of the data generated there are also becoming the subject of legal efforts and developments initiated by the European Commission in recent years. With a remarkable rapidity, a comprehensive re-regulation of modern information technology is being advanced - starting with the Digital Services Act [European Union, 2022b] and the AI Act [European Union, 2021] up to the more recent legal acts that relate in particular to data and the data economy (e.g., Data Governance Act [European Union, 2022c] or Data Act-Draft [European Union, 2022a]). The objective is obvious: the EU aims to become a role model for a data-using society. To this end, the European Commission has defined essential steps with the European Data Strategy [European Commission, 2020b]. The declared aim is to create an ecosystem based on data sharing. European companies, public authorities and scientists are to be given access to large quantities of high-quality data for research and value-adding innovations [Hennemann and Steinrötter, 2022].

The following paper is dedicated to the legal prerequisites of this data transfer, starting from IoT devices that are particularly encountered in the private sector ("smart products"). The problem of data exchange based on such products is evident: First, the personal character of the data concerned is also relevant due to private use; and second, it is precisely non-personal data that provides relevant information that an entrepreneur may not be interested in disclosing from the point of view of competitive and business secrecy protection. Therefore, our paper follows the consistent jurisprudential method of outlining the relevant problem, describing the legal requirements (the status quo) and examining the solution strategy by reviewing the legal fundamentals and methods of interpretation (wording, legal history, legal purpose and teleological considerations) from the perspective of the IoT entrepreneurs concerned. We explain how the European legislator intends to ensure data exchange and what further steps need to be taken to specifically balance the conflicting interests and to bring the idea of data sharing to a higher level.

2 Internet of Things Devices as Basis of Data Economy

Walking through cities, it is easy to find a variety of "smart products" in a wide range of applications, such as lighting in cities, fitness trackers on the arms of passers-by, or other technologies that occasionally enable city centers to be more energy-efficient. When smart products are established in households, such as heaters controllable by app,

smart vacuum cleaner or lawn mowing robots, refrigerators, etc., they are referred to as "smart home" devices or "eHome" or "smart living" [Ametsbichler, 2019]. The market share of smart home-devices is considerable: According to a forecast, a market volume of 11.43 billion euros will be reached in 2027, which corresponds to an expected annual sales growth of 11.48% [Statista, 2023].

2.1 "Smart Home" IoT-Devices

In recent years, the number of networked smart home devices available on the market has grown at an accelerating pace. In a modern household, virtually any device can be smart and networked with other devices.

The "Family Hub Refrigerator", which is connected to a smart doorbell with a camera capability, indicates who is ringing the doorbell and offers the option of letting guests in directly [Samsung, 2023]. The smart TV is connected to the Internet and interconnected with other home devices such as voice assistants, and a complex networked alarm system consisting of motion detectors, door and window contacts, smoke detectors and cameras provides security. A smart dishwasher detects when dishwasher tabs are running low and notifies users by sending a push message. If necessary, it can also reorder the tabs directly and transfer all relevant information into the house´s energy-management-system. Especially smart home services can also be implemented securely using the smart-meter-gateway as a standardized interface [KIASH, 2024]. The implication of "smart home" is an exponentially growing amount of personal and non-personal machine-generated data (Big Data) [Garcia et al., 2020]. Naturally, the types of data collected vary depending on the smart home device or service. In some cases, data is collected about the user and their home, in other cases, machine data is collected about the device and its operation. Personal data can be collected as information entered directly by the user or as user behavior information collected by operating the device or accessing the service. In either case, the volume of data produced in the world is growing rapidly, from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025 [Garcia et al., 2020].

Especially in the smart home environment, the distinction between personal and non-personal data is a considerable issue. With the development of technical possibilities regarding data processing, the risk of personalization increases even for raw data that appears to be non-personal [Greveler et al., 2012]. This previously personal data can be used in aggregated, processed and anonymized form. This serves both to improve future services and to participate in the data economy. In this context, it should be noted that not only personal data is collected in the intimate environment of a smart home, but also machine data. Machine-generated data can be generated independently of the user's direct involvement by computer processes or sensors that collect information from devices. This data can be personal or non-personal. In our context, the focus is on non-personal machine data that does not include information about a specific or identifiable individual. Typical examples of such non-personal machine data include information about the device as such and its operation, such as maintenance intervals.

2.2 Economic Relevance of Smart Home Data

Together, anonymized data and non-personal machine data constitute the basis of the data economy. Although the legal literature focuses particularly on the value of personal data, non-personal data also have a high economic value [Bisges, 2017; Wandtke, 2017; Fries and Scheufe, 2019]. This intrinsic value of data enables direct monetization of data by licensing [Czychowski and Winzek, 2022]. Besides the direct economic value of data, data also drives economic development in the Digital Single Market [Roßnagel, 2017; European Commission, 2020b].

Data is the basis for improving products and services by analyzing user data and then identifying weaknesses and optimizing functions afterwards. Apart from improving the original products and services, data can also provide new business opportunities by enabling additional data-driven services such as energy optimization, security monitoring, or predictive maintenance, thus enhancing productivity in all economic sectors. Data is a key driver of technological innovation, notably in the areas of artificial intelligence, machine learning and data analytics. Aggregated data on maintenance frequencies, for example, enables manufacturers to improve their products and craftspeople to offer their services in a targeted manner, which can significantly increase the success of marketing measures. Data concerning the total energy consumption of an apartment building can be used to install measures to improve energy management.

Overall, smart home data is gaining particular economic relevance, especially in the context of the data economy. On the one hand as a valuable resource, on the other as a driver in the development of new technologies, products and services. For companies that occupy a dominant position in a particular market sector, the current dynamics of European law (see 3.) will even force them to make certain data available in the conceivable future.

3 Legal Fundamentals

As described at the beginning, it is a declared ambition of the European Commission to establish the EU as a role model and pioneer of a data-using society. Companies, public authorities and scientists are to benefit from freely exchangeable data, development and research incentives are to be promoted and the profit potential to be achieved is to be increased. Data is at the core of the digital economy, and its sharing offers significant potential for value creation. According to the European Commission, the potential that Union-wide exchange of data can offer has so far remained largely untapped, as access to data is concentrated in a few, rather larger companies [Bomhard and Merkle, 2022]. The legislative projects initiated in recent years, some of which have already been enacted, are now intended to create new rights of access to data with involvement of data intermediaries - with significant obligations for the providers and manufacturers of smart products.

3.1 General Data Protection Regulation (GDPR)

Since 2018 and with the enactment of the General Data Protection Regulation (GDPR) on May 25, many questions regarding the data protection of the individual user or the data subject have been condensing. The scope of the GDPR is not restricted even by

the more recent legal acts that progressively open up access to data. On the contrary, like the e-Privacy Directive [European Union, 2002], it applies without restriction alongside the new regulations. The GDPR also contains provisions concerning the transfer of data.

The right to informational self-determination enshrined in the GDPR is the key principle guiding the provisions. The right to data portability standardized in Article 20 (1) GDPR should also be seen in this respect. According to this, "the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided [...]". The GDPR defines the term "data" in Art. 4 No. 1 as "any information"; in the scope of the GDPR, it is only about personal data, i.e. data relating to identified or identifiable individuals, see Art. 4 No. 1 GDPR.

Nevertheless, with the right to data portability or transferability, a completely new data protection law instrument has been created [Paal and Götz, 2023]. According to Recital 68, its main purpose is to allow the user or data subject better control of their data [Jülicher et al., 2016], while facilitating the transfer from one data controller to another [Paal, 2021]. In short, in addition to the original objectives of data protection (data sovereignty), Art. 20 GDPR already addresses data economy and also pursues competition law objectives - just as the European Commission does with its other legal efforts.

3.2 Draft Data Act (DA-D)

The core of the European data sharing is the draft Data Act (DA-D). After the European Commission presented an initial draft for the Data Act in February 2022, the member states agreed on a draft with the European Parliament in the night of June 26, 2023. This means that only confirmation by the EU Parliament and the Council of the European Union is required for entry into force. The DA-D is intended to promote the fungibility of data. This continues the path already taken by the Free-Flow-of-Data Regulation [European Union, 2018], the Open Data Directive [European Union, 2019a] and the Data Governance Act (see 3.3).

3.2.1 Scope of Application

Unlike the GDPR, this draft departs from a focus on personal data and pursues a purely economic approach [Richter, 2023]. Overall, the DA-D has five goals: (1) Facilitate data access and use for consumers and businesses while maintaining incentives to invest in value creation using data; (2) Introduce the use of data held by businesses by public entities such as Union institutions, bodies, or agencies in certain situations where exceptionally necessary; (3) Facilitate switching between cloud and edge services; (4) Introduce safeguards to prevent unlawful disclosure of data without prior notice by cloud service providers; (5) Plan to develop interoperability standards for data to be reused by other sectors [Richter, 2023].

Like the GDPR, the DA-D also defines the term data. Art. 2 No. 1 DA-D describes data as " any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual

recording". According to the following Nos. 2, 3 and 4 of Art. 2 DA-D, as well as Recitals 14-17 and 22, the scope of the law also includes IoT applications and the data received, generated, collected or transmitted thereby. This regulatory approach is fundamentally different from the familiar scope of protection established by the GDPR: Data and information are no longer equated, which again emphasizes the role of data as a medium [Hennemann and Steinrötter, 2022; Richter, 2023]. In line with economic ambitions, the reference to persons is consistently abandoned, so that non-personal data is also included by the law - in relation to IoT applications as IoT machine data in addition to user data.

This parallelism of personal and non-personal data requires a strict and sometimes difficult demarcation in the handling of the data when implementing the requirements - a problem that is addressed in many passages in the literature [Bomhard and Merkle, 2022].

3.2.2 Data Access and Issuance Rights

The DA-D regulates the data access claims of companies and consumers to machine-generated data in Chapter 2 and general regulations for data issuance claims in B2B relationships in Chapter 3. This is consistent insofar as comprehensive regulations have so far only existed for personal data, but not for non-personal data (regulations have been made exclusively on the basis of access claims related to intellectual property or antitrust law [Podszun and Pfeifer, 2022; Grapentin, 2023]). These regulations refer to the user, i.e., the person who owns, rents, or leases an (IoT) product or uses a service (Art. 2 No. 5 DA-D) and the data owner, i.e., the person who provides the data or is able to do so by controlling the technical design of the (IoT) product or the data access (Art. 2 No. 6 DA-D).

Art. 4 No.1 DA-D regulates the right to access data: "[To the extent that] data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. [...]". The subject matter is thus the data generated by the use of the IoT product or service. Recital 7 also requires a broad understanding of the scope - data collected by the product (e.g., by integrated sensors) or by the service as such are covered in any case [Bomhard and Merkle, 2022]. Secondary analysis results, on the other hand, are not to be covered by data access law - which leads to another point of criticism, because primary and secondary data are difficult to distinguish, e.g., when using artificial intelligence, so that this can or will lead to uncertainties in the application of the law [Bomhard and Merkle, 2022].

Regarding data containing trade secrets, Article 4 No.3 DA-D provides for a restriction: "Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties"; furthermore, Article 4 No.4 DA-D regulates that the user "shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate." It remains unclear why only the product, but not the service of the IoT product mentioned at the beginning, should be covered by this prohibition of competing use.

3.3 Data Governance Act (DGA)

The Data Governance Act (DGA) published on June 03, 2022, regulates three different aspects of data use and sharing according to Article 1: (1) the reuse of public sector data, (2) data intermediaries and altruistic data organizations, and (3) data use or sharing in relation to personal and non-personal data. The common goal is to enhance the usability of existing data assets by sharing them with third parties [Hennemann and v. Ditfurth, 2022].

3.3.1 Data Intermediation Services according to the DGA

A central element of this regulation is Art. 10 et seq. DGA, i.e. the provisions on data intermediation services or data brokers (see sup. Recital 22). These are services that aim to establish business relationships between an unspecified number of data owners and data users by technical, legal, or other means for the purpose of joint use of data (keyword: data sharing), Art. 2 No. 11 DGA. This definition and legal classification has also been criticized, as it is not clear at any point in the definition that data sharing serves as the main purpose of the business relationship [Hennemann and v. Ditfurth, 2022].

Nevertheless, data intermediation services and data brokers are intended to be an important mechanism by which the EU aims to make a more effective use of existing data resources. For this reason, the regulation aims to strengthen market confidence in data intermediaries and to prevent undesirable developments (especially with regard to competition) in a timely manner.

To this end, Art. 12 DGA sets out the requirements for the data intermediary service, which essentially relate to the neutrality requirement, the prohibition of tying, the conversion of data formats, interoperability between data intermediary services, a prohibition of discrimination and transparency requirements as well as control and security obligations [Hennemann and v. Ditfurth, 2022].

3.3.2 Special case: Data Trustee

The data trustee has been included in some national data strategies as an independent concept, e.g., in the data strategy of the German federal government [BPA - Press and Information Office of the German Federal Government, 2021]. The data trustee is considered a special type of data intermediary and is characterized in particular by the fact that they represent the interests of all parties involved [Kempny et al., 2022].

However, it remains unclear how the data trustee is to be understood in detail. The complexity of the data protection requirements also depends on the extent to which the trustee can process data themselves [Kühling et al., 2020]. On the one hand, it is conceivable that the data trustee only provides assistance to the data subject in enforcing any data preferences - just as it is possible for the data trustee to become part of the data processing themselves to a limited extent. Depending on the design, different aspects of data protection and data management law have to be taken into account.

3.3.3 Special case: Data Innovator

In addition to the intermediaries considered so far, who merely ensure the technological operation of data sharing (data intermediation services) or assume a mere coordinating

function in the data flow (data trustees), the idea of a data innovator can be placed. This could be a person or institution that not only ensures availability of the data in a trustworthy manner or transfers the available data, but actually generates something entirely new from the provided data, e.g., by generating new business models, as they themselves are in a position to evaluate the provided data sets and profitably combine these "data treasures" with previously unconnected companies or to design new business models. It is precisely this ability to make its own autonomous decisions and to develop their own new business models that distinguishes the data innovator introduced here from other intermediaries such as the data trustee. As part of such an innovative process, the data innovator should be able to identify market trends at an early stage in order to be able to integrate the available data into future markets while maintaining identity, trust, and privacy and security - data innovators should be able to orchestrate data spaces and ecosystems at all levels and in all directions.

Such data innovators - which have so far only been discussed hinted at - especially in context of GAIA-X and CATENA-X as “Federation Services” [Reiberg et al., 2023] -would arguably be classified as data intermediary services according to the current conception of the DGA (Art. 10 DGA), which would then have to meet the requirements of Art. 12 DGA (cf. 3.3.1). In particular, neutrality and independency (Art. 12 lit. a DGA), transparency (Art. 12 lit. f DGA) or the assurance of interoperability (Art. 12 lit. d DGA) are required, while other essential competences, such as the technological assurance of authorization to access data [Schütrumpf, 2023], or the ability to categorize data at all according to their importance, level of secrecy, security regarding attacks, etc. in the first place, are not addressed in the DGA at all - capabilities that would, however, be urgently required for the implementation of such a data innovator concept. In general, the regulatory approach of licensing a data intermediation services by the authorities, with generic requirements that are open to interpretation, seems to contradict the idea of a data innovator operating on an economic and competitive basis.

4 Wide Variety of Implementation Possibilities: Solution Approaches

The European data economy project needs to strike a balance between different interests, which is what the European Commission is trying to do with its regulations. In particular, the interests of users - who are strengthened both in their right to informational self-determination by the GDPR and in the exercise of their data sovereignty by the Free Flow of Data Regulation, the Open Data Directive, the DA-D and the DGA - and the interests of manufacturers, who are obliged to disclose their collected personal, but above all non-personal, IoT machine data, need to be balanced. The following discussion shows that this is not an easy task. However, we also show a possible approach that enables the EU objective of a comprehensive data economy to be pursued and, at the same time, a legally secure balance of the conflicting interests to be realized: the data innovator.

4.1 Doubts and Concerns of (IoT) Manufacturers

Despite the efforts of legislators to enable free access to and free flow of data, there are still major reservations about actually using the legally conceivable and free access to data. On the one hand, users do not feel sufficiently involved when it comes to the relevance and value of their own data - there is simply a lack of sufficient transparency. There are already some existing efforts to provide this transparency, such as tools or platforms depicting this (e.g., in the shape of "traffic lights").

On the other hand, there are the companies, manufacturers and developers of IoT devices. We address their fears and reservations below. The companies' concerns are twofold: First, they fear a distortion of competition, especially due to the disclosure of their non-personal IoT machine data. Admittedly, the EU Commission also considered this circumstance when drafting the regulations. However, it is debatable whether the assessments are appropriate in practice. Second, there are concerns about extensive liability in the event of cybersecurity breaches or errors in handling the data.

4.1.1 Commercial Secrets and Distortion of Competition

The right of access to data of companies and consumers provided for by the European Commission has a significant impact on trade secrets of manufacturers and data owners. This is not least due to the broad definition of data provided in Art. 2 No. 1 DA-D (see 3.2.1). Even the non-personal raw machine data contain not only application data of the users, but moreover also secret core know-how of the device manufacturers [Grapentin, 2023]. Even before the first draft of the DA-D was published, the European Commission commissioned an expert opinion to investigate to what extent this machine data of an IoT device also constitutes trade secrets that are legally protectable (e.g., by national laws, such as the German Trade Secrets Act). This expert opinion came to a negative conclusion: The raw data collected was not subject to trade secret protection because it either had no semantic meaning, had no economic value due to its lack of secrecy, or was generally not secret [European Innovation Council and SMEs Executive Agency].

However, it remains debatable whether this line of argument is tenable - especially since the protection of know-how and thus of trade secrets is one of the central reasons why many manufacturers are reluctant to allow such free access to data and want to oppose it. From the point of view of the manufacturers of smart IoT devices, various data is collected: Sensors record technical parameters, error messages are collected in log files [Grapentin, 2023]. Such data can be used to virtually map the devices to simulate their function and to identify and eliminate vulnerabilities. The fact that secondary data are not subject to Art. 4 No.1 DA-D also offers little restriction. Even unprocessed primary data can be extracted and thus reconstructed by competent third parties so that software etc. can be optimized - all that remains of the original device is the sensor technology [Grapentin, 2023].

As a result, it remains to be stated that the raw data described, as soon as they are collected and extracted and thus also subject to the access obligations according to the DA-D, contain sensitive and critical information and are thus suitable for disclosing trade secrets [Krüger et al., 2020]. In particular, information contained in data from networked IoT devices is also considered to be protected as trade secrets [Drexl, 2018; Lorenzen, 2022; Wiebe, 2023] - not least since conclusions about the functions and

processes of a device can also be drawn from this data. This information about the structure and functioning of products resulting from the data is not common knowledge, as the expert opinion commissioned by the EU Commission asserts. Rather, it is information that is protected by manufacturers using IT security measures, which illustrates its economic value [Lorenzen, 2022; Grapentin, 2023; Wiebe, 2023].

These aspects contribute to the competition concerns that manufacturers of IoT devices have regarding data access rights. It would not be excluded that third parties offer money to a user for asking the data owner to provide the data [Paal and Götz, 2023]. Admittedly, Art. 4 No.4 DA-D contains a prohibition on using the data received for the purpose of developing competing products - but first, this does not apply to IoT services, and second, this is difficult to verify, leading to fundamental legal uncertainty for manufacturers. The bottom line is that trade secrets of the data owner cannot prevent data access in principle.

Nonetheless - trade secret protection is an entrenched legal position similar to intellectual property law and, with a hybrid character, positioned between intellectual property law and competition law [Ohly, 2019]. However, there is minimal protection against the development of competing products, the proof of which leads to problems in the first place - and manufacturers have to prove it. For this reason, companies are often reluctant to share their data with other companies - they simply fear the loss of competitive advantage [European Commission, 2020a].

In this context, the reluctance of companies to use data intermediaries should also be addressed. This is - also according to the European Commission - primarily due to trust deficiencies in the data markets. Only if companies have sufficient trust in data intermediaries can they attract a large number of users and successfully contribute to an existing data exchange in the EU [Hennemann and v. Ditfurth, 2022].

4.1.2 Liability for Data Privacy and Security

Beyond the device manufacturer concerns described above regarding the impact of the data user's right to access the data, which relate directly to the use of that data, there are additional indirect concerns. These indirect concerns are not derived from third party access to the data, but relate to the administrative costs resulting from the right of access.

Apart from the aforementioned concerns of device manufacturers about how user access to data could affect its use, there are additional concerns that are not directly related, but are nonetheless important. These indirect concerns do not relate to third party access to data, but rather to the administrative costs that result from the right to data access. As already discussed, the DA-D requires that the owner of data generated by the use of a product or related service provide this data. Since the definition of "data" in the DA-D is very broad (3.2.1), this applies to both personal and non-personal data. This could potentially lead to data protection conflicts [European Union, 2022a; Metzger et al., 2023; Richter, 2023; Steinrötter, 2023].

One possibility to resolve the conflict between data protection and data access could be to prohibit participation in the data economy with regard to personal data. When collected personal data is anonymized, it ceases to fall within the scope of the GDPR. Although the DGA requires anonymization (Art. 17 (2) lit. b), so that data protection appears to be ensured, it is debatable whether true anonymization is technically possible. [Winter et al., 2019; Hornung and Spiecker gen. Döhmann, 2023].

Once the identifiability of a data subject has been deleted at a specific instant, it cannot be excluded with any certainty that this personal allocation can be restored in the conceivable future by combining this data with other data, e.g. by hackers, due to the constant development of technologies [Roßnagel and Geminn, 2021]. The larger the data set is, the higher is the probability of re-identification of individuals based previously anonymized data [Rocher et al., 2019] Moreover, personal data are often included in mixed datasets of personal and non-personal machine data (Recital 7 and 30 DA-D). With the development of technical possibilities in the context of data processing, the risk of personalization of even seemingly impersonal raw data increases [Greveler et al., 2012]. A conclusive classification of a given data set as non-personal is (almost) impossible as the scale of the data set increases [Rücker and Dienst, 2021; Bomhard and Merkle, 2022], at least for a data intermediary who does not have the competence to recognize the personal references. In general, it seems then debatable whether assuming the (liability) risk in the event of a misjudgment is worthwhile for companies, especially SMEs, given the high fines and claims for damages imposed by the GDPR [Bomhard and Merkle, 2022].

In the event of violations of data protection law, companies might encounter fines and claims for damages, inter alia. Violations that potentially lead to fines include 1) Art. 5 and Art. 83 (5) lit. a GDPR: Breach of the principles of personal data processing (including lawfulness, transparency requirement, purpose limitation, data minimization, storage limitation, accountability) or 2) Art. 6 and Art. 83 (5) lit. a GDPR: Unlawful processing of personal data. Depending on the nature of the breach, violations are punishable by fines of up to EUR 10,000,000 or EUR 20,000,000 or up to 2% or 4% of the total annual global revenue of the previous fiscal year, whichever is higher. Pursuant to Art. 32 (1) GDPR, the controller and processor are required to implement appropriate technical and organizational measures (e.g., pseudonymization and encryption or procedures for periodic assessment of the effectiveness of technical and organizational measures to ensure the security of processing) to ensure a level of security appropriate to the risk.

A further challenge therefore arises from the GDPR's unclear requirements regarding the security of data storage and processing [Martini, 2021], which would need to be assessed not only by a company but also by a data intermediary. The damage resulting from a potential incident needs to be assessed based on various parameters to determine the required security measures [Hladjk, 2018]. If larger amounts of data are stored, the risk of hacker attacks, etc., is potentiated in relation to the expected gain from the exploitation of a security breach by third parties. For corporations whose focus is not on data sharing, the identification and implementation of appropriate security measures cannot be determined and implemented on their own without considerable effort. This can lead to uncertainty about the security measures to be taken in individual cases. This uncertainty can in turn lead to unnecessarily high fines being imposed for security measures that have not been taken yet are necessary, or to very great efforts being made to implement security measures that are not necessary in order to avoid liability.

However, the GDPR does not only provide for high fines. If data subjects have been harmed by the unlawful processing of their personal data, they can claim compensation from data controllers. This includes the damage caused to a data subject by leakage of data. In this case, the controller may also be accused of not having sufficiently complied with the IT security requirements specified in the GDPR. The claim for damages is possible for both material and non-material damages (Art. 82

GDPR). If violations of the GDPR affect large data sets and thus a large number of individuals, the claims can accumulate and thus rise to a considerable sum. In particular, since the introduction of a special declaratory action (e.g., "Musterfeststellungsklage" in Germany, see Sec. 606 et seq. of the German Code of Civil Procedure) into data protection law (Article 80 (1) GDPR), which considerably facilitates the assertion of claims for damages by data subjects, the economic risk of these claims has further increased [Kühling and Sackmann, 2019]. Due to liability risks, device manufacturers (the data owners) are already sensitized to the data protection challenges, which is expressed, for instance, in the length of the data protection declarations used [Korch, 2021]. Considering the new and upcoming data access regulations to foster the data economy, the importance of data protection law and the resulting liability risks for device manufacturers will tend to increase further for device manufacturers and data owners. The conflict between data protection law and data economy as shown is exacerbated by the fact that the relationship between GDPR, DGA and DA-D has not yet been fully clarified [Steinrötter, 2023]. As a consequence, this also leads to a significantly increased liability risk for data owners and device manufacturers [Heinzke, 2023; Steinrötter, 2023].

4.2 Data Innovator as Neutral and Qualified Third Parties

Since it has become clear that the challenges particularly consist in considering the requirements arising from existing legal regulations (e.g., on data protection or liability) within the framework of a comprehensive data exchange, it is evident that the data intermediary has a pivotal filter function. They have to identify data that might be considered as problematic and, if necessary, reverse it if it cannot be used commercially without legal conflicts. This is where the difference between the data trustee and our concept of the data innovator becomes clear, as more decision-making ability and authorization to act are required in order to be able to conduct this assessment adequately. If the data intermediary is also supposed to have the ability to act innovatively (data innovator, 3.3.3), the person or institution needs to have specific skills that are not yet included in the more generic set of requirements of the DGA (3.3.1 and 3.3.3). Here, a supplement needs to be provided.

The practical, technical and legal implementation of the data innovator concept can be based on already established phenomena. Regarding the scope of tasks of supporting data transfer, a comparison to conformity assessment bodies/notified bodies within the scope of product safety law seems to be inevitable. This is accomplished as follows: Security of physical products can be demonstrated by conformity assessment (Chapter III of the Product Safety Regulation [European Union, 2023]). The Conformity Assessment Body is the authority responsible for verifying the conformity of a product that it has predefined with the European product-related specifications (Sec. 12 (2) No. 1 of the German Product Safety Act / Article 2 No. 12 of Market Surveillance Regulation [European Union, 2019b]). To this end, it is provided primarily with the capabilities required for conformity testing (Art. R17, Annex I of Decision No. 768/2008/EC "Model Provisions for Community Harmonization Legislation on Products" [European Union, 2008]). It has to be able to accomplish all of the conformity tasks. For this purpose, it has to work e.g. in accordance with established procedures in order to ensure the repeatability of these procedures (Sec. 6 para. 2 lit. b)). According to Sec. 5 of Decision No. 768/2008/EC, Conformity Assessment Bodies and their

respective staff are required to carry out conformity assessment activities with the highest degree of professionalism and the necessary technical competence in the specific fields. In addition, Conformity Assessment Bodies are required to maintain the necessary personnel with technical knowledge and sufficient relevant experience for the assessment (Sec. 6 para. 2 lit. a, Sec. 7). Further detailed requirements are laid down in sector-specific standards [DIN]. They are intended to supplement the statutory canon of duties and competencies to a significantly higher degree of detail. This process is also conceivable for the data innovator (or team of data innovators). In detail, this means that this position needs to combine comprehensive knowledge and skills because they need to address a wide range of issues. They need to have knowledge of data (protection) law and be able to place data economy activities in a legal context in order to establish legal compatibility. They need to be able to represent the interests of consumers and, in some cases, incorporate ideal interests into the assessment decision. They also need to have economic knowledge and skills in order to incorporate business interests, but also to be able to take macroeconomic considerations into account. To ensure that the data innovator is able to act in a legally compliant manner, they need to be formally equipped with the necessary skills, which requires legal recognition.

In order to ensure a fair and legally secure balance between the various participants in data economy by the data innovator, who - as described above - has to be able to recognize and assess the risks (cf. 3.3.3) and to act innovatively, the data innovator should also be given equally precise specifications for their skills and competencies by means of standards. Here too, it is advisable to define the exact requirements for such a demanding position in standards (e.g. DIN). The latter would be developed by groups of experts in the field (e.g., computer scientists, ethicists, engineers, etc.) and could represent the state of the art in an interdisciplinary and sufficiently specific manner with regard to the technically and professionally feasible. Provided with this competence, however, the data innovators would also be responsible if the data were passed on unlawfully (recognizing this problem [Buchholtz et al., 2023] on p. 209). The latter would not be detrimental, since the sword of Damocles of liability would also ensure careful action onside the intermediary.

Only if the skills and competencies of data intermediaries can be further developed using standards they will be able to fulfill their filter function to the required extent; in fact, not until then could the intended data economy be fully developed.

5 Opportunity and Advantages of Holistic Solution Strategies

The objective of comprehensive data exchange, data usability and data access with the aim of (economically) empowering companies, as announced by the European Commission, is currently still facing multiple challenges. In addition to the considerations of mere data protection law regarding user data and the right to informational self-determination of the users of IoT devices, there are also the rights, obligations and practical concerns of the manufacturers of these devices. The aim of designing and implementing legal regulations therefore has to be to regulate the partially conflicting interests of 1) users and manufacturers of IoT devices and 2) entrepreneurs and manufacturers towards each other, and to resolve the competition and liability issues.

A neutral and qualified body - such as the data intermediary in the shape of a data innovator - offers an excellent opportunity. First, this applies from the manufacturer's immediate perspective: by establishing such an intermediary and innovator that is neutral and qualified in data exchange, liability risks are outsourced to a data protection, technical and economic expert and are thus contained. To the extent that the data intermediary is enabled to comprehensively address the issues of data protection (primarily GDPR) and data security (legally a combination of the relevant regulations mentioned above) and to incorporate the additional entrepreneurial and economic interests (thus becoming a data innovator, 3.3.3), both user interests and manufactural secrecy and competitive interests are comprehensively addressed and the risk of liability or fines is mitigated on this basis. Due to its expertise, this neutral and qualified body has a comprehensive insight into the (cyber)security law aspects and can solve them in a legally secure manner according to the interests of the addressees. In contrast to the manufacturers, they have the necessary data law know-how, which can be combined in this context and passed on to experienced employees. This allows the manufacturer to continue to concentrate on the development of technical products.

Unlike data protection authorities, for example, which can comprehensively record and balance the interests of users and manufacturers, data intermediaries (in the shape of data innovators) are also in a position to balance the second aspect of the conflicting interests of different manufacturers - the protection of competition and trade secrets. Overall, there are complex processes not only of a legal nature, but also of an economic and technical nature that can be addressed by a data innovator. This applies both with regard to the mere exchange of data as such, as well as with regard to the consideration of trade secret protection and competitive advantages or disadvantages, and especially with regard to economic exploitability in the context of business models.

Due to the diverse interests that are not limited to the mere protection of data, the data innovator - as described in 4.2 - offers the perfect, holistic solution for establishing data flows and strengthening trust in data economy law.

6 Conclusions

This paper addressed the requirements for data access to data generated in IoT devices. It is a stated objective of the European Commission to establish data sharing and to establish the EU as a leader in the field of data economy. To this end, a number of regulations have been established or are about to be enacted, such as the DGA and the DA-D. However, such a data economy in Europe requires not only legal experts to verify compliance (also with regard to the privacy of users of such devices), but also manufacturers of IoT devices. Due to the increasing popularity of IoT devices, especially in the smart home sector, the newly regulated rights of data access are also directed in particular at manufacturers, as they are obliged to hand over both personal data, but also non-personal - i.e. IoT machine data - upon request of the user. For manufacturers, this is potentially unpleasant territory from a competition law and trade secrets perspective in some cases. For this reason, they are occasionally skeptical of the EU's goals for the data economy. In addition, manufacturers of such smart products that specialize in technical development have difficulty keeping track of the potentially significant financial data law implications, which only adds to the skepticism about data sharing.

We have shown that a data intermediary developed on the basis of the DGA - namely the data innovator - offers a perfect opportunity to consider both the data protection interests of users and the competition law interests of manufacturers, right up to the data management interests of the European Commission, while handling data responsibly. As a neutral but autonomous body, they can support each of the affected operators in finding their position in the data economy market and acting there in a strengthened manner.

References

[Ametsbichler, 2019] Ametsbichler, E.: Rechtliche Fragestellungen beim Einsatz von „Smart-Home"-Technologie, In InTeR - Zeitschrift für Innovations- und Technikrecht, 2019, 169–174.

[Bisges, 2017] Bisges, M.: Personendaten, Wertzuordnung und Ökonomie. Kein Vergütungsanspruch Betroffener für die Nutzung von Personendaten, In MMR - Multimedia und Recht, 2017, 5, 301–306.

[BMBF, 2021] BMBF - German Federal Ministry of Education and Research: Big&Smart Data - Daten als Rohstoff, 2021. https://www.bildung-forschung.digital/digitalezukunft/de/technologie/daten/big-smart-data-daten-als-rohstoff.html. Accessed 7 September 2023.

[Bomhard, 2022] Bomhard, D., Merkle, M.: Der Entwurf eines EU Data Acts. Neue Spielregeln für die Data Economy, In RDi - Recht Digital, 2022, 4, 168–176.

[BPA, 2021] BPA - Press and Information Office of the German Federal Government: Data Strategy of the Federal German Government. An innovation strategy for social progress and sustainable growth, 2021.

[Bräutigam, 2017] Bräutigam, P.: Die Weiterentwicklung des E–Commerce zum E–Commerce 2.0. B. Vernetzung. Rn. 9, In E-Commerce. Rechtshandbuch, Bräutigam, P., Rücker, D., Berger, A., Eds. C.H. Beck, München, 2017.

[Bräutigam, 2015] Bräutigam, P., Klindt, T.: Industrie 4.0, das Internet der Dinge und das Recht, In NJW - Neue Juristische Wochenschrift, 2015, 16, 1137–1142.

[Buchholtz, 2023] Buchholtz, G., Brauneck, A., Schmalhorst, L.: Gelingensbedingungen der Datentreuhand – rechtliche und technische Aspekte, In NVwZ - Neue Zeitschrift für Verwaltungsrecht, 2023, 4, 206–212.

[Czychowski, 2022] Czychowski, C., Winzek, M.: Rechtliche Struktur und Inhalt von Datennutzungsverträgen. Datenwirtschaftsrecht III: Der Vertrag über ein neues Elementarteilchen?, In ZD - Zeitschrift für Datenschutz, 2022, 2, 81–90.

[DIN 2012] DIN: DIN EN ISO/IEC 17020:2012-07. Konformitätsbewertung - Anforderungen an den Betrieb verschiedener Typen von Stellen, die Inspektionen durchführen, 2012.

[Drexl, 2018] Drexl, J.: Data Access and Control in the Era of Connected Devices, Study on Behalf of the European Consumer Organisation BEUC, Brussels, 2018.

[European Commission, 2020a] European Commission: Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance; SWD/2020/295 final, 2020a.

[European Commission, 2020b] European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A European strategy for data, COM/2020/66 final, 2020b.

[European Innovation Council and SMEs Executive Agency] European Innovation Council and SMEs Executive Agency: Study on the legal protection of trade secrets in the context of the data economy: final report.

[European Union, 2002] European Union: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002.

[European Union, 2008] European Union: Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, 2008.

[European Union, 2018] European Union: Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018.

[European Union, 2019a] European Union: Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, 2019a.

[European Union, 2019b] European Union: Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, 2019b.

[European Union, 2021] European Union: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final, 2021.

[European Union, 2022a] European Union: Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, 2022a.

[European Union, 2022b] European Union: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022b.

[European Union, 2022c] European Union: 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), 2022c.

European Union: Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, 2023.

[Fries, 2019] Fries, M., Scheufe, M.: Märkte für Maschinendaten. Eine rechtliche und rechtsökonomische Standortbestimmung, In MMR - Multimedia und Recht, 2019, 11, 721–726.

[Grapentin, 2023] Grapentin, S.: Datenzugangsansprüche und Geschäftsgeheimnisse der Hersteller im Lichte des Data Act, In RDi - Recht Digital, 2023, 4, 173–182.

[Greveler, 2012] Greveler, U., Justus, B., Löhr, D.: Multimedia Content Identification Through Smart Meter Power Usage Profiles, 2012. https://www.semanticscholar.org/paper/Multimedia-Content-Identification-Through-Smart-Greveler-Justus/75b9a34cb6a0268ae7acaad34c7fcdedb450f160.

[Heinzke, 2023] Heinzke, P.: Data Act: Auf dem Weg zur europäischen Datenwirtschaft, In BB - Betriebsberater, 2023, 201–209.

[Hennemann, 2022] Hennemann, M., Steinrötter, B.: Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, In NJW - Neue Juristische Wochenschrift, 2022, 21, 1481–1486.

[Hennemann, 2022] Hennemann, M., Ditfurth, L.: Datenintermediäre und Data Governance Act, In NJW - Neue Juristische Wochenschrift, 2022, 27, 1905–1910.

[Hladjk, 2018] Hladjk, J.: DS-GVO Art. 32 Sicherheit der Verarbeitung, In DS-GVO. Datenschutz-Grundverordnung: Kommentar, Ehmann, E., Selmayr, M., Albrecht, J.P., Baumgartner, U., Bertermann, N., Eds. C.H. Beck; LexisNexis, München, Wien, 2018.

[Hornung, 2023] Hornung, G., Spiecker gen. Döhrmann, I.: Einleitung, Rn. 247, In Datenschutzrecht. DSGVO mit BDSG, Simitis, S., Hornung, G., Spiecker Döhrmann, I., Eds. Nomos, Baden-Baden, 2023.

[Jülicher, 2016] Jülicher, T., Röttgen, C., Schönfeld, M.: Das Recht auf Datenübertragbarkeit. Ein datenschutzrechtliches Novum, In ZD - Zeitschrift für Datenschutz, 2016, 8, 358–362.

[Kempny, 2022] Kempny, S., Krüger, H.S., Spindler, M.: Rechtliche Gestaltung von Datentreuhändern. Ein interdisziplinärer Blick auf „Data Trusts“, In NJW - Neue Juristische Wochenschrift, 2022, 23, 1646–1650.

[KIASH, 2024] KIASH: KIASH Projekt | KI-gestützte Anomalieerkennung für Smart Homes, 2024. https://kiash.de/. Accessed 14 March 2024.

[Korch, 2021] Korch, S.: Vertragsrecht in der Datenökonomie Datenprivatrecht zwischen europäischem Datenschutz und technischer Realität, In ZEuP - Zeitschrift für Europäisches Privatrecht, 2021, 4, 792–820.

[Krüger, 2020] Krüger, S., Wiencke, J., Koch, A.: Der Datenpool als Geschäftsgeheimnis, In GRUR - Gewerblicher Rechtsschutz und Urheberrecht, 2020, 6, 578–584.

[Kühling, 2019] Kühling, J., Sackmann, F.: Die Musterfeststellungsklage nach Datenschutzverstößen - ein unkalkulierbares Risiko für Unternehmen?, In DuD - Datenschutz und Datensicherheit, 2019, 6, 347–352.

[Kühling, 2020] Kühling, J., Sackmann, F., Schneider, H.: Datenschutzrechtliche Dimensionen. Datentreuhänder: Kurzexpertise. Forschungsbericht / Bundesministerium für Arbeit und Soziales, FB550, Berlin: Bundesministerium für Arbeit und Soziales, Institute of Labor Economics (IZA), 2020.

[Lorenzen, 2022] Lorenzen, B.: Geschäftsgeheimnisschutz und Data Act, In ZGE - Zeitschrift für geistiges Eigentum; IPJ - Intellectual Property Journal, 2022, 14, 3, 250.

[Martini, 2021] Martini, M.: DS-GVO Art. 32 Sicherheit der Verarbeitung, In Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Paal, B.P., Pauly, D.A., Ernst, S., Eds. C.H. Beck, München, 2021.

[Metzger, 2023] Metzger, A., Schweitzer, H., Wagner, G.: Datenschutz und Datenmarkt: Grundzüge einer Marktordnung für die europäische Datenwirtschaft, In ZfPW - Zeitschrift für die gesamte Privatrechtswissenschaft, 2023, 3, 227–266..

[Ohly, 2019] Ohly, A.: Das neue Geschäftsgeheimnisgesetz im Überblick, In GRUR - Gewerblicher Rechtsschutz und Urheberrecht, 2019, 5, 441–451.

[Paal, 2023] Paal, B., Götz, M.: Aktuelle Rechtsfragen zur Datenübertragbarkeit aus Art. EWG_DSGVO Artikel 20 DS-GVO. Voraussetzungen – Verantwortlichkeit – Anspruchsinhalt und -grenzen, In ZD - Zeitschrift für Datenschutz, 2023, 2, 67–72.

[Paal, 2021] Paal, B.P.: DS-GVO Art. 20 Recht auf Datenübertragbarkeit, In Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Paal, B.P., Pauly, D.A., Ernst, S., Eds. C.H. Beck, München, 2021.

[Podszun, 2022] Podszun, R., Pfeifer, C.: Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, In GRUR - Gewerblicher Rechtsschutz und Urheberrecht, 2022, 13, 953–961.

[Reiberg, 2023] Reiberg, A., Appelt, D., Smolén, A., Kraemer, P.: Datentreuhänder, Datenvermittlungsdienste und Gaia-X, 2023.

[Richter, 2023] Richter, S.: Vereinbarkeit des Entwurfs zum Data Act und der DS-GVO. Der schmale Grat zwischen Schutz personenbezogener Daten und Datenkommerzialisierung, In MMR - Multimedia und Recht, 2023, 3, 163–168.

[Rocher, 2019] Rocher, L., Hendrickx, J.M., Montjoye, Y.-A. de: Estimating the success of re-identifications in incomplete datasets using generative models, In Nat Commun, 2019, 10, 1, 3069. https://www.nature.com/articles/s41467-019-10933-3.

[Roßnagel, 2017] Roßnagel, A.: Rechtsfragen eines Smart Data-Austauschs. Datengetriebene Kooperation in der Industrie, In NJW - Neue Juristische Wochenschrift, 2017, 1-2, 10–15.

[Roßnagel, 2021] Roßnagel, A., Geminn, C.L.: Vertrauen in Anonymisierung. Regulierung der Anonymisierung zur Förderung Künstlicher Intelligenz, In ZD - Zeitschrift für Datenschutz, 2021, 9, 487–490.

[Rücker, 2021] Rücker, D., Dienst, S.: § 6 Daten, In Internet of Things. Rechtshandbuch, Bräutigam, P., Kraul, T., Bauer, S., Birnstiel, A., Eds. C.H. Beck, München, 2021.

[Samsung, 2023] Samsung: Samsung Family Hub: smarte Kühl-& Gefrierkombination | Samsung Deutschland, 2023. https://www.samsung.com/de/refrigerators/my-refrigerators/?product1=rs6ga8521b1/eg&product2=rs6ga8531s9/eg&product3=rs6ja8810s9/eg. Accessed 7 September 2023.

[Schütrumpf, 2023] Schütrumpf, M.: Anbieter von Datenvermittlungsdiensten als neue Intermediäre. Korrelationen zwischen dem Infrastrukturprojekt Gaia-X und dem Data Governance Act, In RDi - Recht Digital, 2023, 8, 373–381.

[Statista, 2023] Statista: Smart Home - Deutschland | Statista Marktprognose, 2023. https://de.statista.com/outlook/dmo/smart-home/deutschland. Accessed 7 September 2023.

[Steinrätter, 2023] Steinrötter, B.: Verhältnis von Data Act und DS-GVO. Zugleich ein Beitrag zur Konkurrenzlehre im Rahmen der EU-Digitalgesetzgebung, In GRUR - Gewerblicher Rechtsschutz und Urheberrecht, 2023, 4, 216–226.

[Wandtke, 2017] Wandtke, A.-A.: Ökonomischer Wert von persönlichen Daten. Diskussion des „Warencharakters“ von Daten aus persönlichkeits- und urheberrechtlicher Sicht, In MMR - Multimedia und Recht, 2017, 1, 6–12.

[Weiser, 99] Weiser, M.: The computer for the 21st century, In SIGMOBILE Mob. Comput. Commun. Rev., 1999, 3, 3, 3–11.

[Wiebe, 2023] Wiebe, A.: The Data Act Proposal. Access rights at the Intersection with Database Rights and Trade Secret Protection, In GRUR - Gewerblicher Rechtsschutz und Urheberrecht, 2023, 4, 227–238.

[Winter, 2019] Winter, C., Battis, V., Halvani, O.: Herausforderungen für die Anonymisierung von Daten: Technische Defizite, konzeptuelle Lücken und rechtliche Fragen bei der Anonymisierung von Daten, In ZD - Zeitschrift für Datenschutz, 2019, 11, 489–493.