Consequences of EU Data Regulation for Smart Home Data Economy: Extending Analysis with a Case Study

Paul Seidel, Felix Fischer, Dirk Labudde
Faculty Applied Computer Sciences and Biosciences
Hochschule Mittweida University of Applied Sciences
Mittweida, Germany
e-mail: {seidel6 | fische11 | labudde}@hs-mittweida.de

***Abstract*—The entry into force of the European Union (EU) Data Act 2024 creates new opportunities for the European data market, but also new challenges. One such challenge is the parallel application of the EU General Data Protection Regulation (GDPR). It is therefore necessary to analyse these two regulations and their consequences for the stakeholders in the Smart Home sector. To this end, we have researched the Smart Home sector and its stakeholders and identified potential conflicts between the EU Data Act and the EU GDPR. One such conflict arises in the management of personal data from multi-user environments. In the Smart Home in particular, several users share different devices, such as smart TVs and thus generate mixed data sets that are not compliant with the regulation. If a member of the user community wishes to transfer their data to a third party in accordance with their rights guaranteed by the EU Data Act, the third party must be able to ensure that the transferred data is not also the personal data of another user. We supplement our regulatory and technical analysis with a case study of the Bosch Smart Home Controller, which demonstrates practical approaches and unresolved issues in managing personal and non-personal data, enforcing GDPR provisions, and realizing the potential of the Data Act in actual home automation deployments.**

Keywords-EU data act; gdpr; contradiction; smart home.

I. Introduction

This extended paper builds on our earlier study of the consequences of the EU Data Act and GDPR for the modern smart home data economy, originally presented at IARIA ICDS 2025 [1]. This version supplements the regulatory analysis with a focused case study examining real-world data security and privacy practices implemented in a modern Smart Home Controller API.

Increasing digitalisation and the steady expansion of data-based business models have placed the so-called data economy at the heart of economic and technological developments. Data is regarded as the new oil of the 21st century [2] and is essential for value creation in areas such as machine learning, whose economic potential through generative models has recently been estimated at several trillion dollars [3, p. 3]. This makes the regulation and utilisation of data a key challenge for modern economies.

The Smart Home plays a central role in this data economy, as connected devices generate a wide range of data that can benefit both users through better services and manufacturers through commercial exploitation [4]. Currently, however, European consumers often do not have access to their data, which hampers innovation and competition [5]. The European Union (EU) Data Act aims to redress this imbalance by granting users extensive rights to their data, including real-time access to device-generated data [6, Art. 3]. In addition to the General Data Protection Regulation (GDPR), which already provides for the right to data portability [7, Art. 12 para. 3], the Data Act aims to promote competition and interoperability, for example through cloud switching and access to manufacturer data for repair services [6, Recital 78]. At the same time, however, there is a tension between the two regulations. While the Data Act also requires the transfer of mixed data sets, the GDPR prioritises the protection of personal data and prescribes strict sanctions for violations [6, Art. 1 para. 5]. This leads to legal uncertainties, particularly in the Smart Home, where mixed data sets are often created. With the EU Data Act becoming applicable law in September 2025, this issue is becoming increasingly relevant and requires technical solutions to take into account both regulatory requirements and the technical innovation potential.

The urgency of this study arises from that recent entry into force of the EU Data Act, which significantly reshapes the regulatory landscape for data access and sharing in Europe. Particularly in Smart Homes, where multiple users often interact with interconnected devices and generate mixed datasets, the practical application of the Data Act introduces tensions. This study examines these tensions, focusing on the legal and technical challenges of managing personal data in multi-user environments and ensuring regulatory compliance. The specific designs and implementations of the technical and legal solutions to these challenges are beyond the scope of this study.

A recent U.S. decision in the antitrust case against Google further highlights a principle that closely resonates with the EU Data Act: access to data is essential for fair competition. By obliging Google to share parts of its search data with competitors, the court recognized that control over large datasets can entrench market dominance and stifle innovation [8]. The EU Data Act builds on the same insight, seeking to open up data flows in sectors such as the Smart Home by ensuring that users can access and share the information generated by their devices. Both measures rest on the idea that unlocking data for wider use creates opportunities for new entrants and service providers, thereby fostering more dynamic and competitive digital markets. This frames the facilitation of fair access to

2025, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

data as a global and international issue.

After this introduction, the key stakeholders and challenges in the Smart Home sector are discussed in Section II, focusing on their interests and the inherent problems in this environment. Also in Section II, the concept of the Smart Home is defined, and the roles of relevant stakeholders are explored. Section III then examines the challenges posed by the data economy in Smart Homes, particularly data protection issues and power asymmetries between consumers and service providers. In Section IV, the EU Data Act and the GDPR are analyzed, providing an overview of both regulations, highlighting potential conflicts, and assessing their implications for the Smart Home sector. Section V discusses enforcement trends of the GDPR and their broader implications for compliance, while Section VI presents a case study of Bosch's Smart Home Controller as a practical example of regulatory challenges in implementation. Finally, the paper concludes with a summary of findings and directions for future work in Section VII.

II. Stakeholders and Problems in the Smart Home

The Smart Home sector is a central component of the modern data economy, in which consumers, device manufacturers and service providers operate in a complex network of economic and regulatory relationships. In order to better understand the opportunities and risks of this sector, a comprehensive analysis of the players involved and their interests is required. Therefore, the basic concepts and functioning of the Smart Home, as well as the roles of the relevant players are first examined and the potentials and risks arising from the use of the data generated in the Smart Home are analysed. The central challenges of the data economy in the Smart Home context are then analysed, with a focus on data protection problems, economic effects and power imbalances between users and providers.

A. *Smart Home - Definition and concept*

The Smart Home is based on the technologies of Embedded Systems and the Internet of Things (IoT). Embedded Systems are specialised, integrated computer systems designed to automate and simplify the functionalities of the host device [9, ch. 1]. Networking via technologies such as IEEE 802.11, usually referred to as WLAN, or Bluetooth creates the IoT, which enables communication between devices and their real-time interaction [10].

In the Smart Home, this IoT architecture is used to network household appliances and automate everyday processes [11]. The aim is to increase comfort, safety and efficiency, for example through smart thermostats that optimise energy consumption based on the habits of the residents [12][13].

An overview of the terms Embedded Systems, Internet of Things and Smart Home is summarised in Table I.

TABLE I
Definition of terms: Embedded Systems; IoT; Smart Home

Term	Definition	Examples
Embedded systems	mechanical and electrical systems with integrated software	modern cars, cash register systems, ATMs
Internet of Things (IoT)	interconnected embedded systems	Industry 4.0, car-to-car communication
Smart Home	IoT systems in home automation	vacuum/mopping robots, SmartTVs

The networking of Smart Home devices opens up numerous opportunities to make everyday life easier and to organise processes more efficiently by networking various household appliances. For example, the data collected can be used to increase comfort and energy efficiency in households [14]. In the healthcare sector in particular, wearables, such as smart watches offer the possibility of recognising medical emergencies, such as strokes or heart attacks at an early stage, enabling faster and potentially life-saving interventions [15][16]. Home automation also benefits the environment, as intelligent control systems can optimise the energy consumption of appliances. Automated adjustment of heating, lighting and other systems not only reduces costs for residents, but also helps to reduce the ecological footprint [17][18]. An illustrative example is the automatic switch-off of radiators as soon as windows are opened [19].

Smart home data is also used to improve building security. Intelligent monitoring systems can recognise break-ins at an early stage and initiate preventative measures. In addition to traditional dangers, such as burglaries, invisible risks, such as voltage peaks, critical air conditions or structural damage to buildings can also be detected and communicated to the residents [20, p. 7][21][22]. In addition, personalised functions, such as alarm clocks, music or news, enrich daily life by being tailored to the individual preferences of residents. The use of modern AI technologies makes it possible to analyse the collected data and turn it into meaningful automated decisions [23][24].

The symbiosis between AI and Smart Home technologies mutually reinforces both areas. AI relies on using large amounts of data to develop powerful models, while Smart Home devices continuously generate such data [25][26]. This creates a market in which data trading plays a central role. Companies that rely on AI-supported solutions buy the necessary data, while the owners of this data can monetise it. This creates an economic incentive, especially for companies without the technical resources to utilise their own data [6, Recital 19].

Networked systems also offer potential at a societal level, for example in public health management. During the COVID-19 pandemic, it became clear how valuable data-driven systems can be in tracing chains of contact [27]. Applications such as the *Corona-Warn-App* [28] helped to break chains of infection and slow down the spread of the virus. At the same time, however, the collection and processing of sensitive data raises questions about the protection of privacy. While the pandemic has demonstrated the benefits of such technologies, it has also revealed the risks of large-scale data collection

2025, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

and storage. Sensitive information on health, behaviour and habits could be exposed or misused by cyberattacks, causing considerable harm to the individuals concerned [29, pp. 11]. Weighing up the benefits of data-driven innovations against the risks to privacy and security therefore remains a key challenge for the Smart Home data economy.

B. Relevant stakeholders and interests

To analyze the dynamics within the Smart Home ecosystem, stakeholders were grouped along two dimensions: their level of access to data and their technical know-how to generate value from it. Four central stakeholder groups (SG) operate in the Smart Home sector. The relationships between the stakeholder groups are shown graphically in Figure 1.

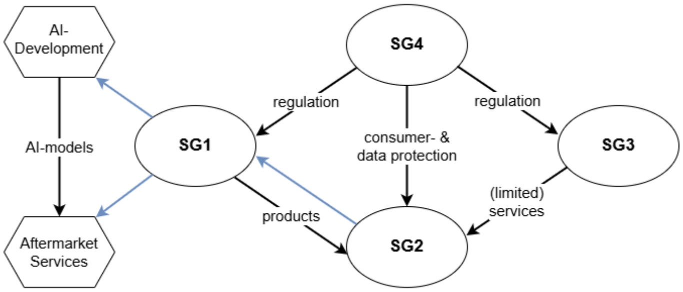

Figure 1. **Relationship diagram of the actors in the Smart Home and IoT** Legend: SG1 - Gatekeepers; SG2 - Users; SG3 - Aftermarket service providers; SG4 - Legislators and institutions; Data relations in blue.

SG1: Gatekeeper Technology companies such as Amazon and Google dominate the market by manufacturing devices and utilising data. Their focus is on increasing profits, often at the expense of data protection and despite strict regulations such as the GDPR [30][31]. As gatekeepers, they control the data that is created on devices produced by them. Therefore they have a significant influence on the market and competition [32]. Gatekeepers typically possess both privileged access to user data and the technical expertise to extract economic and strategic value from it.

SG2: Users Consumers benefit from automation and innovation, but are also the main source of data. Entertainment Systems, such as Smart TVs are the most popular among users, while building security and automation solutions are less common [33]. User priorities are security and convenience [34]. Customers and private users have limited technical capabilities and often only partial access to the data they generate.

SG3: Aftermarket service providers Companies offering repair services and cloud providers are heavily dependent on gatekeepers as they often lack access to critical data. They may have the technical know-how but face barriers in data access due to platform control and interoperability issues. This hampers innovation and fair competition [35].

SG4: Legislators and institutions Legislation, particularly at EU level, is aimed at data protection, consumer protection and a fair data market. Data from Smart Home systems could also be used in crises, such as pandemics or natural disasters [36].

III. Challenges of the data economy in the Smart Home

The data economy faces significant economic and legal hurdles, particularly in the Smart Home sector. A central problem are the gatekeepers - powerful technology companies that primarily operate outside the EU and exert considerable influence on the global flow of data. Their dominance makes it difficult to enforce European data protection regulations [37] and manifests itself in various power asymmetries vis-à-vis their customers. The trade in personal data and the data protection-compliant processing of this data pose further challenges, which can result in financial losses that threaten the existence of small and medium-sized companies in particular if the applicable regulations are not observed.

A. Data protection issues in the Smart Home

The data generated by Smart Home devices often contains sensitive and sensitive information about users and their everyday habits [6][38]. IoT technologies are expected to have a significant impact on the healthcare sector in particular, which further emphasises the sensitivity of this data [14]. Manufacturers of Smart Home devices and services have a significant influence on what data is collected and shared, while consumers are often insufficiently informed about the scope and storage of this data [39]. Without technical expertise, it is almost impossible for consumers to verify the accuracy of the specified data processing modalities and their control over the data they generate is severely limited [38]. In many cases, the only option available to users with data protection concerns is to opt out of the product or service.

Intelligent voice assistants are a particularly clear example of the lack of transparency in data processing. These systems require permanent monitoring of the acoustic environment in order to be able to react to trigger phrases [39]. Although data is only transmitted after a keyword has been recognised, voice assistants can be activated unintentionally, e.g. by similar-sounding phrases, whereby data is transmitted without the explicit request of the user [40]. Users are often left in the dark about the scope of the data collected, as detailed information can only be requested on their own initiative and in accordance with the applicable data protection laws, such as the GDPR. In addition, this data is usually not processed locally, but decentralised on the providers' cloud servers [41], which severely restricts the user's control over the transfer and processing of data.

To better understand the regulatory challenges in Smart Home environments, it is required to distinguish between different types of data and their sources. Table II classifies Smart Home data along two dimensions: the nature of the data (personal vs. non-personal) and its origin (individual users or shared use).

This classification in Table II highlights the complexity of data governance in multi-user settings, where personal and non-personal data often coexist and overlap, raising important questions about ownership and access rights.

TABLE II
CLASSIFICATION AND EXAMPLES OF SMART HOME DATA BY USER AND TYPE

Data Type	User 1	User 2	Shared
Personal Data	voice assistant queries, health data	TV preferences, fitness data	shared calendar, living room camera footage
Non-Personal Data	generic device usage statistics (e.g., light switches)	app update logs, battery charging cycles	energy consumption, network diagnostics

The decision on how to handle the collected data often lies with the manufacturers, while the users, despite legal requirements such as [7, Art. 12-14], has no direct insight into or control over access to their data. In many cases, this data is sold to third parties or used by the provider to develop new services, often without the express consent of the user [39]. Even after the use of Smart Home devices, many providers retain the collected data, which increases the risk of future misuse or disclosure through security incidents [42].

Consumers are also dependent on manufacturers and service providers in their ability to protect their data, as they store the data in cloud systems [41][43]. Data protection-friendly functions, such as encryption or multi-factor authentication are often missing and can only be implemented by the manufacturer [39]. Particularly in connection with identifying data, such as payment or geolocation data, which by its very nature can be assigned to individuals, the security of this personal data depends largely on the security precautions taken by the cloud provider. In the event of a data leak, serious consequences, such as identity theft or financial damage can occur [44]. For companies that rely on networked devices, data protection incidents can also lead to a loss of sensitive business secrets, which harbours considerable economic risks [45].

There is a further risk in the second-hand trade for IoT and Smart Home devices. Due to the frequent lack of user interfaces on embedded devices, resetting used devices to factory settings is difficult and can result in the previous owner's personal data remaining on the device [46]. The new owner could unintentionally or maliciously gain access to this data or use functions that are linked to the previous owner's account.

B. Power asymmetries between consumers and service providers

In the course of the increasing networking of household appliances and the data-driven economy, power asymmetries between consumers and service providers (specifically SG1 'gatekeepers') are becoming ever more apparent. These result not only from the technical complexity, but also from the legal and economic conditions, which restrict consumers' scope for action and make access to the data they generate more difficult.

A central feature of these asymmetries are non-negotiable user agreements dictated by the provider. Particularly in the area of Smart Home technologies, providers impose opaque contractual terms and conditions [38], which can usually only be accepted by accepting or waiving the service. These often contain clauses that grant extensive rights of use to personal data or severely limit the provider's liability [47]. The exact scope of data use often remains opaque, which increases consumer mistrust [38]. The lack of transparency about data processing and the invisibility of processes that take place in remote data centres [41] further increase this scepticism. Access to and management of personal data often takes place via complex, less user-friendly platforms [48], which makes it difficult for many users to exercise their rights under the GDPR.

A particularly clear example of this power asymmetry is Amazon's Alexa voice assistant system. Here, the consumer has little control over the extent of data usage, as these processes are decentralised and hidden [49]. Users are dependent on a continuous connection to the cloud in order to use the service [50]. This increases dependency on the provider and makes it difficult to switch to alternative providers.

In addition, the lack of interoperability of cloud services makes it difficult to switch between different providers, as many systems are proprietary [51]. The repair options for Smart Home devices are also limited, as often only the manufacturer can carry out repairs [52].

These structural imbalances are leading to a loss of trust among consumers, who are increasingly trying to remove their data from the providers' streams. Data protection-oriented technologies such as Brave or the Tor browser, as well as specialised 'data removal services', are therefore gaining in importance [53]. This loss of trust, especially with regard to the technical security of networked devices, could damage the Smart Home sector in the long term as the value of the data collected decreases [33].

IV. EU DATA ACT AND GDPR IN THE SMART HOME

In this section, two central and widely applicable EU regulations with great relevance for the Smart Home and the data generated therein are analysed: the GDPR and the EU Data Act. These regulations aim to regulate the handling of personal and machine-generated data, strengthen consumer rights and address the issues analysed in Section II, such as data protection problems and power asymmetries between service providers and users.

Together with other legislative measures, for instance the EU Digital Markets Act, the EU Digital Services Act and the EU Data Governance Act, they form the basis of the European Commission's digital strategy.

A. Overview of the EU Data Act

The EU Data Act (EU Regulation 2023/2854) is a central element of the European data strategy and regulates access to and use of the generated data collected by digital technologies such as Smart Home devices and cloud computing. The regulation was adopted in November 2023, has been in force since the beginning of 2024 and will be applicable law from September 2025 [54]. The aim is to ensure fair access to

2025, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

data and a fair distribution of data between different market players [5].

Manufacturers and service providers (data owners) are obliged to grant users prompt access to their generated data [6, Art. 3 para. 1]. This also includes the right to pass the data on to third-party providers who can use it to develop innovative products and services [6, Art. 5]. In the Smart Home sector in particular, this should help to ensure that not only large companies benefit from the data economy, but also smaller players [6, Recital 30 & 32].

The processing of personal data remains subject to the provisions of the GDPR, which takes precedence in the event of conflicts [6, Art. 1 para. 5]. The regulation is intended to give users more control over their data, as many consumers or companies do not have the resources to utilise the full economic value of their data themselves [6, Recital 3 & 19 & 40]. One example of implementation is the management of data by virtual assistants. These collect information about Smart Home users, for example to control heating or lighting. The EU Data Act enables users to manage this data and pass it on to third-party providers, which could give rise to new smart assistance systems [6, Recital 22].

In order to curb the market dominance of large platforms, gatekeeper companies defined under the EU Digital Markets Act may not use data that does not originate from their own devices [6, Art. 5 para. 3]. This is intended to prevent excessive concentration of market power [55][56]. In addition, the EU Data Act is intended to help better manage such public emergencies as pandemics or cyberattacks. In such cases, public authorities can request relevant data, whereby the modalities are clearly defined and companies may be compensated for providing it [6, Art. 14 & 17].

Figure 1 can thus be extended to Figure 2.

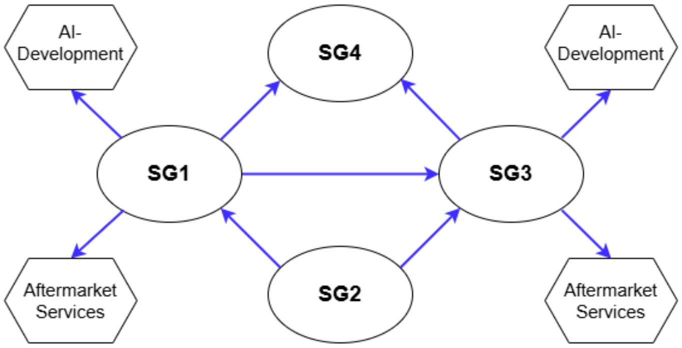

Figure 2. **In terms of the EU Data Act, modified relationship diagram of the actors in the Smart Home and IoT area from Figure 1**
Legend: SG1 - Gatekeepers; SG2 - Users; SG3 - Aftermarket service providers; SG4 - Legislators and institutions; Data relations in blue.

With the EU Data Act becoming applicable law, data that was previously exclusively accessible to gatekeepers (SG1) will be available to all authorised interested parties (see Figure 2). This enables European companies (SG3) to develop their own data-based services, while public authorities (SG4) can manage crises more efficiently.

However, the extended availability of data harbours security risks. Data owners are responsible for securing access and data, but can use modern security measures, for example encryption or smart contracts [6, Art. 3 para. 1, Art. 11 para. 1]. Users and recipients may only adapt these measures with the consent of the data controller without being restricted in their use of data.

Another key issue is cloud switching: users should be able to switch more easily between cloud providers, such as AWS or Microsoft Azure. Providers must support customers when switching [6, Art. 25 para. 2a], ensure business continuity and, from 2027, no longer charge fees for the move [6, Art. 29]. This incentivises structured, machine-readable data formats and technologies for smooth data migration [6, Recital 78 & 84].

Smart contracts are proposed as possible interfaces for automated data transfers to enable the secure and traceable execution of agreements [6, Art. 2 para. 39]. The EU Data Act requires high security standards, protection against manipulation and audit-proof archiving of the generated data [6, Art. 36]. Providers must regularly submit declarations of conformity to prove compliance with the regulations.

The regulation also emphasises security in critical infrastructures, for example energy and water supply [6, Recital 14]. In addition to the GDPR, security checks and measures such as pentests and encryption are also to be performed and implemented for non-personal data [6, Recital 102].

For implementation, national authorities are to be appointed or established to impose effective sanctions in the event of violations [6, Art. 37 & 40]. If several authorities are involved, a data coordinator will be appointed for coordination, while GDPR supervisory authorities will remain responsible for personal data [6, Art. 37 para. 3].

The EU Data Act addresses the asymmetric market power in the IoT sector in favour of users and strengthens competition [57, p. 26]. However, there are challenges: User consent remains a weak point, and interactions with the GDPR are still unclear [57, pp. 23]. Further legal and technical coordination is required in order to realise the full benefits of the EU Data Act.

B. *Overview of the GDPR*

The General Data Protection Regulation (GDPR) has been in force as binding law in the EU since 2018 and aims to ensure the protection of personal data [7]. It was introduced in response to increasing digitalisation and the growing amount of data collected [58]. Large tech companies in particular benefit from analysing and using such data [7, Recital 6].

A clear legal framework has been created to regulate data processing, which obliges companies to meet high standards and provides for sanctions in the event of violations [7, Recital 7]. In practice, however, there are difficulties with enforcement, particularly in cross-border cases [37].

The GDPR defines key terms such as *personal data*, *processing* and *profiling* [7, Art 4] and sets out binding principles for the handling of personal data. These include lawfulness, purpose limitation, data minimisation and accountability [7, Art. 5].

Data subjects have extensive rights, including rights to information, access and erasure [7, Art. 13-17]. Data controllers must ensure that these rights are respected and are obliged to appoint data protection officers and report data breaches within 72 hours [7, Art. 24 & 33].

An evaluation of the GDPR from 2024 emphasises the central role of data protection officers, especially for small and medium-sized enterprises [59, p. 3]. In addition, the regulation should be made less bureaucratic to enable more efficient and risk-based implementation [59, pp. 4]. Digital service providers should also be more closely integrated into the obligations of the GDPR in order to improve users' control over their data [59, pp. 5].

C. Comparison and conflicts between the two regulations

The GDPR and the EU Data Act have different priorities, but are not fundamentally contradictory. While the GDPR prioritises the protection of personal data and consumer protection, the EU Data Act focuses on promoting a data-driven economy and facilitating access to non-personal data [60]. Both sets of regulations share the goal of supporting the free movement of data within the EU by striving for a balance between data protection and the commercial use of data.

Both the GDPR and the EU Data Act contain provisions for crisis situations: While the EU Data Act permits the provision of relevant data, the GDPR authorises public bodies to process personal data in certain cases [7, Art. 2 para. 2d][6, Art. pp. 14]. These regulations can be helpful in the context of pandemics or disaster management, for example, but raise questions in the area of law enforcement and anti-terrorism measures. The centralised availability of data via data traders could also open up new opportunities for fighting crime, the effects of which need to be investigated further.

A central area of tension arises when networked devices generate personal data, as the EU Data Act makes it clear that it must not affect the GDPR and takes second place to it in the event of a conflict [6, Recital 34][6, Art. 1 para. 5]. This becomes particularly problematic in multi-user scenarios: A single user could share or sell data that also affects other people without their consent. This would be a violation of the GDPR [7, Art. 13]. At the same time, the EU Data Act obliges providers to provide non-personal data [6, Art. 3], which creates a legal dilemma: A refusal could violate the EU Data Act, a disclosure could violate the GDPR.

The distinction between personal and non-personal data poses a further challenge, especially in the case of mixed data sets. The EU Data Act requires a clear classification in order to provide commercially usable data, while the GDPR comprehensively protects personal data [6, Art. 3, 7, Art. 18]. It is particularly critical that originally non-personal data can become personal information through correlation or analytical procedures [61, p. 6 & 16][62]. This could lead to data protection provisions being circumvented through clever contractual constructions.

The practical implementation of both sets of regulations also poses challenges for companies. Small and medium-sized enterprises in particular are confronted with considerable bureaucratic effort due to the parallel requirements of the GDPR and the EU Data Act, which ties up resources and can inhibit innovation processes [59][60].

Approaches such as anonymisation or selective data sharing are being discussed to resolve these conflicts, although their technical feasibility and effectiveness remain questionable. A more precise regulation on the separation of personal and non-personal data as well as a clear legal handling of multi-user scenarios are necessary in order to make the coexistence of both sets of rules practicable [6, Recital 7].

D. Relevance for the Smart Home

Smart home devices, as part of the IoT, collect a lot of data in the home environment and are explicitly mentioned in the EU Data Act [6, Recital 23]. Currently, however, these systems are often limited by incompatibilities, while users find it difficult to access their own data [35][63]. The EU Data Act is intended to counteract this by promoting better data accessibility and interoperability between manufacturers [6, Recital 32]. This not only enables personalised services, but also facilitates the repair of defective devices through improved data access [6, Recital 32].

As considerable amounts of data are generated in the Smart Home, these are not only of economic interest to users, but also to companies. The EU Data Act obliges providers to make this data available - both to consumers and to third parties, including competitors [6, Recital 39].

The data collected affects many areas of life, from health to entertainment [64], and offers both individual and economic benefits [6, Recital 64]. At the same time, they are often personal [38] and are therefore subject to the GDPR, which creates data protection risks, especially through the detailed recording of user behaviour [38].

Heino et al. [38] describes four central data protection problems in the Smart Home:

(1) Unclear legal scope of application,
(2) Lack of transparency in data processing,
(3) preset data collection with opt-out instead of opt-in and
(4) uncertainties regarding retention periods. Added to this is the principle of data minimisation, which conflicts with the usefulness of many devices, as more data often means better functionality [61, p. 15][65, p. 3].

Following our analysis, we would expand this list based on the differences between the kinds of data generated in the smart home as described in Table II:

(5) Blurred boundaries between personal and non-personal data, especially in shared or mixed-use contexts,
(6) Ambiguity in attributing data to specific individuals in multi-user environments,
(7) Unclear responsibilities for data governance when data is co-generated or shared across devices and users,

2025, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

(8) Conflicts between user rights under the Data Act (e.g., data portability) and the privacy rights of other users under the GDPR.

Since the GDPR came into force, users in countries with GDPR-compliant legislature are increasingly aware of data security risks and have a higher perceived level of control [66]. The multi-user operation of Smart Home devices makes GDPR compliance more difficult. In households, several people share devices, which makes it challenging to clearly assign and control personal data. A flexible solution is needed to combine data protection and usability.

V. Enforcement of the GDPR: Trends and Implications

Since the GDPR entered into force in 2018 [7, Art. 99], supervisory authorities across the EU have regularly imposed fines for infringements.

By September 2024, total fines amounted to roughly €5 billion across more than 2,000 cases [67], demonstrating active enforcement and significant financial consequences. The sharp increases in July 2021 and May 2023 are linked to rulings against *Amazon* (€750 million) [68] and *Meta Platforms* (€1.2 billion) [69].

The most striking case remains *Meta Platforms*, fined more than €2 billion since 2018 [67]. These sanctions primarily concern the lawfulness of processing [7, Art. 6], data processing principles [7, Art. 5], and insufficient technical and organizational safeguards [7, Art. 32]. Yet, with 2023 revenues of €134.9 billion [70], these fines account for less than 1.5 % of Meta's annual turnover, raising doubts about their deterrent effect.

Beyond Meta, fines often stem from violations of lawful processing [7, Art. 6], fundamental processing principles such as integrity and confidentiality [7, Art. 5f & 32], and failure to respect data subject rights [7, Art. 15ff.]. Smaller cases frequently involve non-compliance with access or erasure obligations, with fines ranging from €100 to €10,000 [67]. For SMEs, the administrative burden of meeting these requirements without dedicated compliance units poses a significant challenge [71].

The effectiveness of the GDPR as a deterrent remains contested [31][59][60][68]. Large repeat offenders like Meta call into question the impact of fines, while SMEs often comply more carefully, as penalties can threaten their existence. Thus, the deterrent effect of sanctions appears uneven across company sizes and sectors.

Regardless of its ultimate efficacy, the history of imposed fines underlines the prominent role of sanctions in enforcing regulatory standards, especially in the domain of data protection. Given the parallels in scope and ambition, similar enforcement intensity can be expected under the Data Act. As discussed in Section IV, the combination of GDPR and Data Act obligations creates particularly complex challenges in multi-user environments such as Smart Homes. Proactive compliance strategies are therefore essential to safeguard both user rights and companies from future sanctions.

VI. Case Study: Bosch Smart Home Controller

An illustrative case study is provided by Bosch's Smart Home Controller, which is documented in an openly available GitHub repository under https://github.com/BoschSmartHome/bosch-shc-api-docs. The system enables the centralized management of supported Smart Home devices and the data they generate. It serves as a useful example of how Smart Home ecosystems can be structured in a way that aligns with the requirements of the EU Data Act. In particular, Bosch provides standardized interfaces for accessing device data and facilitates interoperability with third-party services, which reflects the Act's emphasis on data availability and portability.

The Bosch Smart Home Controller exposes a local REST API, allowing developers and integrators access to a comprehensive set of functionalities: device status queries, event subscription, automation rules management, and retrieval of historical logs. API communication is encrypted with TLS 1.2, and authorized clients must register via secure key exchange, setting a technical baseline for secure integration. The system also supports modern connectivity protocols such as Zigbee and Matter, enabling compatibility with a wide range of third-party devices and aligning with broader interoperability goals in the smart home market.

However, a closer analysis reveals some shortcomings with regard to user-level data governance. The controller does not implement device-level access control for different household members. Instead, the designated administrator account has unrestricted access to all data generated within the Smart Home environment, including personal data of other users. While this design significantly increases usability and system maintenance, it stands in direct tension with the principle of user-specific rights over personal data under the GDPR[7, Art. 12-23]. The absence of mechanisms to separate or shield multi-user data illustrates a critical challenge for ensuring compliance in real-world Smart Home infrastructures.

Additional concerns relate to the granularity and transparency of data handling. Although Bosch provides well-documented APIs for data access and integration, the system lacks fine-grained role management and user-specific permission settings. Logs of who accessed or exported which data are not visible to individual users, thereby limiting transparency and accountability. Furthermore, while interoperability with external services is supported, safeguards for preventing the uncontrolled sharing of mixed datasets remain underdeveloped. The availability of technical integration points is an important step toward data portability, but the absence of robust audit mechanisms and user-centered access controls highlights a gap between the formal requirements of EU data governance frameworks and practical implementation in commercial smart home solutions.

These observations underline the difficulty of bridging the gap between competing regulatory aspirations and the current state of technical implementation in Smart Home platforms, highlighting the need for privacy-by-design features that operationalize legal requirements.

2025, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

VII. Conclusion and Future work

The Smart Home has been identified as an increasingly relevant component of the data economy, in which the residents of a networked living space generate a large amount of data through their use of intelligent devices. This data offers significant potential for new services, such as personalised energy management systems or health-applications, but also creates risks. These include data protection problems, security gaps and the possibility of commercial exploitation of user data by third parties.

The Smart Home sector is characterised by a wide range of actors, including manufacturers of IoT devices, service providers, public authorities and consumers themselves. These players often pursue divergent interests: While providers primarily aim to monetise user data, consumers demand stronger data protection measures and easy ways to control their data. The power asymmetries between large technology providers and their customers or small to medium-sized enterprises were identified as particularly problematic, as they hinder innovation and competition in the sector.

The forthcoming applicability of the EU Data Act and the existing requirements of the GDPR are having a significant impact on the Smart Home sector. The EU Data Act addresses the current power asymmetry by facilitating data access for data-generating customers and third-party providers, thereby promoting competition and innovation.

The GDPR, on the other hand, emphasises the protection of personal data and defines strict requirements for its processing. In combination, these two regulations create a complex legal framework and therefore pose considerable challenges. Conflicting objectives arise, particularly in the case of mixed data sets that contain both personal and non-personal information of several users: while the EU Data Act requires the release of non-personal data, the GDPR demands strict protective measures for personal data. This leads to uncertainties as to how the two regulations can be harmonised without violating data protection regulations and fearing sanctions. If such uncertainties are not adequately addressed, the Data Act may have the opposite of its intended effect and hinder innovation through diminished customer acceptance and reduced trust in data-driven services.

Our analysis of GDPR enforcement demonstrates that sanctions play a crucial role in ensuring compliance, though their effectiveness varies significantly between large technology firms and smaller companies. At the same time, the Bosch Smart Home Controller case study illustrates the practical challenges of implementing regulatory requirements in real-world systems, where multi-user environments and insufficient access controls create gaps between legal obligations and technical practice. Taken together, these findings underline both the necessity of effective enforcement mechanisms and the importance of privacy-by-design solutions if the goals of the GDPR and the EU Data Act are to be realized in the Smart Home sector.

The Bosch Smart Home Controller case study illustrates both achievements and ongoing challenges in aligning smart home systems with EU Data Act and GDPR requirements. While Bosch demonstrates progress in data accessibility and interoperability through standardized APIs, the system lacks the fine-grained user controls and transparency mechanisms necessary for GDPR compliance, particularly in multi-user households. Specifically, the centralized administrator model grants unrestricted access to all household data without role-based separation, creating tension with GDPR principles of individual user rights. These findings underscore that effective compliance requires privacy-by-design features embedding user-specific data governance at the infrastructure level, not merely API documentation and interoperability support.

In view of regulatory developments and the increasing spread of Smart Home technologies, several relevant research questions arise. One key issue is the practical implementation of the EU Data Act in the area of conflict with the GDPR, particularly with regard to the separation of personal and non-personal data within mixed data sets. There is a need for further clarification here to ensure that both data protection requirements and economic interests are adequately taken into account.

Another research approach is the development of technical solutions for more data protection and data sovereignty in the Smart Home. Approaches such as federated learning or edge computing could help to make data processing more decentralised in order to reduce security risks and power asymmetries. There is also a need for further research into how users can obtain intuitive and effective control mechanisms over their data without compromising the user-friendliness of Smart Home systems.

Finally, the economic and social impact of the new regulations must also be analysed. It remains to be seen to what extent the EU Data Act will actually promote competition in the Smart Home market or whether new challenges will arise due to regulatory uncertainties. Further research could focus on what adjustments the industry needs to make in order to fulfil the legal requirements and develop innovative, data protection-compliant business models.

VIII. Acknowledgment

This paper was funded by the European Union and the Free State of Saxony (Germany).

Kofinanziert von der
Europäischen Union

Freistaat Sachsen

Diese Maßnahme wird mitfinanziert durch
Steuermittel auf der Grundlage des vom
Sächsischen Landtag beschlossenen Haushaltes.

References

[1] P. Seidel, F. Fischer, and D. Labudde. "Consequences of the EU Data Act and the EU General Data Protection Regulation for the Modern Smart Home Data Economy". In: *Proceedings of the 19th International Conference on Digital Society (ICDS 2025)*. IARIA. 2025. ISBN: 978-1-68558-267-8. URL: https://www.thinkmind.org/articles/icds_2025_1_40_10025.pdf.

[2] M. Szczepanski. *Is data the new oil?* accessed: 09.04.2025. Jan. 2020. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf.

[3] M. Chui et al. *The economic potential of generative AI - the next productivity frontier*. accessed: 09.04.2025. 2023. URL: http://dln.jaipuria.ac.in:8080/jspui/bitstream/123456789/14313/1/The-economic-potential-of-generative-ai-the-next-productivity-frontier.pdf.

[4] Publications Office of the European Union. *Data Act — Factsheet*. accessed: 09.04.2025. 2022. DOI: 10.2775/636433. URL: https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet.

[5] Council of the EU. *Data Act: Council adopts new law on fair access to and use of data*. accessed: 09.04.2025. Nov. 2024. URL: https://www.consilium.europa.eu/en/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/.

[6] European Parliament and Council of the EU. "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). In: *Official Journal of the European Union* (Dec. 2023). accessed: 09.04.2025. URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj.

[7] European Parliament and Council of the EU. "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). In: *Official Journal of the European Union* (May 2016). accessed: 09.04.2025. URL: https://data.europa.eu/eli/reg/2016/679/oj.

[8] D. Kerr, N. Robins-Early, and J. Bhuiyan. "'Slap on the wrist': critics decry weak penalties on Google after landmark monopoly trial". In: *The Guardian* (Sept. 2025). URL: https://www.theguardian.com/technology/2025/sep/03/google-monopoly-case-ruling.

[9] S. Heath. *Embedded Systems Design*. accessed: 09.04.2025. 2003. ISBN: 0-7506-5546-1. URL: https://books.google.de/books?hl=en&lr=&id=BjNZXwH7HlkC&oi=fnd&pg=PP1&dq=embedded+systems&ots=xk1jG-BMkP&sig=_hYgwJ2cR_bfy4DNTNK3M3PCsN4&redir_esc=y#v=onepage&q=embedded%20systems&f=false.

[10] Federal Network Agency. *Federal Network Agency - Internet of Things*. accessed: 10.04.2025. Oct. 2024. URL: https://web.archive.org/web/20250328092032/https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Internet/IoT/start.html.

[11] Ibm. *Internet of Things*. May 2024. URL: https://www.ibm.com/de-de/topics/internet-of-things.

[12] B. L. Risteska Stojkoska and K. V. Trivodaliev. "A review of Internet of Things for smart home: Challenges and solutions". In: *Journal of Cleaner Production* 140 (2017). ISSN: 0959-6526. DOI: 10.1016/j.jclepro.2016.10.006. URL: https://www.sciencedirect.com/science/article/pii/S095965261631589X.

[13] L. Ferreira, T. Oliveira, and C. Neves. "Consumer's intention to use and recommend smart home technologies: The role of environmental awareness". In: *Energy* 263 (2023), p. 1. ISSN: 0360-5442. DOI: 10.1016/j.energy.2022.125814. URL: https://www.sciencedirect.com/science/article/pii/S0360544222027001.

[14] A. Al-Fuqaha et al. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications". In: *IEEE Communications Surveys & Tutorials* 17.4 (2015), pp. 2347–2376. DOI: 10.1109/COMST.2015.2444095.

[15] B.-O. Bat-Erdene and J. L. Saver. "Automatic Acute Stroke Symptom Detection and Emergency Medical Systems Alerting by Mobile Health Technologies: A Review". In: *Journal of Stroke and Cerebrovascular Diseases* 30.7 (2021), p. 105826. ISSN: 1532-8511. DOI: 10.1016/j.jstrokecerebrovasdis.2021.105826. URL: https://www.strokejournal.org/article/S1052-3057(21)00229-9/fulltext.

[16] NHLBI. *Novel sensor can detect a heart attack in just minutes*. accessed: 09.04.2025. Oct. 2021. URL: https://www.nhlbi.nih.gov/news/2021/novel-sensor-can-detect-heart-attack-just-minutes.

[17] M. Zehnder et al. "Energy saving in smart homes based on consumer behavior: A case study". In: *2015 IEEE First International Smart Cities Conference (ISC2)*. 2015. DOI: 10.1109/ISC2.2015.7366231.

[18] A. Anvari-Moghaddam, H. Monsef, and A. Rahimi-Kian. "Optimal Smart Home Energy Management Considering Energy Saving and a Comfortable Lifestyle". In: *IEEE Transactions on Smart Grid* 6.1 (2015), pp. 324–332. DOI: 10.1109/TSG.2014.2349352. URL: https://ieeexplore.ieee.org/abstract/document/6895131.

[19] Telecom. *SmartHome Ideas: Heating Control*. accessed: 09.04.2025. Aug. 2024. URL: https://web.archive.org/web/20240915162832/https://www.smarthome.de/ideen/smarte-heizungssteuerung.

[20] M. Bräuer. *ABUS Safety Study 2023*. 2023.

[21] J. Dahmen et al. "Smart Secure Homes: A Survey of Smart Home Technologies that Sense, Assess, and Respond to Security Threats". In: *Journal of reliable intelligent environments* 3.2 (2017), p. 1. DOI: 10.1007/

2025, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

s40860-017-0035-0. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC5616189/.

[22] L. Miller. *Integrating Smart Building Predictive Maintenance to Your System*. Ed. by L. Miller. accessed: 09.04.2025. Oct. 2024. URL: https://web.archive.org/web/20240814031401/https://www.buildingsiot.com/blog/integrating-smart-building-predictive-maintenance-to-your-system-bd.

[23] P. L. Austin. *What Will Smart Homes Look Like 10 Years From Now?* accessed: 10.04.2025. July 2019. URL: https://time.com/5634791/smart-homes-future/.

[24] X. Guo et al. "Review on the Application of Artificial Intelligence in Smart Homes". In: *Smart Cities* 2.3 (2019), p. 1. ISSN: 2624-6511. DOI: 10.3390/smartcities2030025. URL: https://www.mdpi.com/2624-6511/2/3/25.

[25] L. Budach et al. *The Effects of Data Quality on Machine Learning Performance*. 2022. URL: https://api.semanticscholar.org/CorpusID:251223513.

[26] Y. Chen. "IoT, cloud, big data and AI in interdisciplinary domains". In: *Simulation Modelling Practice and Theory* 102 (2020), p. 1. ISSN: 1569-190X. DOI: 10.1016/j.simpat.2020.102070. URL: https://www.sciencedirect.com/science/article/pii/S1569190X20300083.

[27] Council of the EU. *Data Act: Council adopts new law on fair access to and use of data*. accessed: 10.04.2025. Oct. 2024. URL: https://commission.europa.eu/strategy-and-policy/coronavirus-response/travel-during-coronavirus-pandemic/contact-tracing-and-warning-apps-during-covid-19_de.

[28] R. K. Institute. *Digitally interrupt chains of infection with the Corona-Warn-App*. accessed: 11.04.2025. May 2024. URL: https://www.rki.de/DE/Themen/Infektionskrankheiten/Infektionskrankheiten-A-Z/C/COVID-19-Pandemie/CoronaWarnApp/Warn_App.html.

[29] D. P. Conference. *Use of digital contact tracing services for event, facility, restaurant and business visits to prevent the spread of Covid-19: Guidance from the Conference of Independent Federal and State Data Protection Supervisory Authorities*. Apr. 2021.

[30] EU Commission - Representation in Germany. *Fair digital markets: gatekeepers must comply with all DMA rules starting today*. accessed: 10.04.2025. Mar. 2024. URL: https://germany.representation.ec.europa.eu/news/faire-digitale-markte-torwachter-mussen-ab-heute-alle-dma-regeln-einhalten-2024-03-07_de.

[31] European Commission. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Second report on the application of the General Data Protection Regulation (GDPR)*. accessed: 10.04.2025. July 2024. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52024DC0357.

[32] European Parliament and Council of the EU. "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). In: *Official Journal of the European Union* (Dec. 2023). accessed: 09.04.2025. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R1925.

[33] Deloitte. *Consumer IoT fact check: The Internet of Things in the everyday lives of German consumers*. accessed: 09.04.2025. 2021. URL: https://web.archive.org/web/20231214185700/https://www.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/Consumer_IoT_2021_Deloitte.pdf.

[34] B. K. Sovacool, D. D. Furszyfer Del Rio. *Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies*. accessed: 10.04.2025. 2022. URL: https://www.sciencedirect.com/science/article/pii/S1364032119308688.

[35] European Commission. *Data Act – Questions and Answers*. June 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114.

[36] European Commission. *European data strategy*. accessed: 10.04.2025. Nov. 2024. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

[37] EU Commission - Representation in Germany. *General Data Protection Regulation: EU Commission wants to improve enforcement*. accessed: 10.04.2025. July 2023. URL: https://germany.representation.ec.europa.eu/news/datenschutzgrundverordnung-eu-kommission-will-durchsetzung-verbessern-2023-07-04_de.

[38] T. Heino, S. Rauti, and R. Carlsson. "An assessment of privacy policies for smart home devices". In: *Proceedings of the 24th International Conference on Computer Systems and Technologies (CompSysTech '23)*. Ed. by T. Vassilev and R. Trifonov. ACM Other conferences. New York, NY, United States: Association for Computing Machinery, 2023, p. 1. ISBN: 979-8-4007-0047-7. DOI: 10.1145/3606305.3606332. URL: https://dl.acm.org/doi/fullHtml/10.1145/3606305.3606332.

[39] R. Herold. *Five Common Privacy Problems in an Era of Smart Devices*. accessed: 10.04.2025. Jan. 2020. URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/five-common-privacy-problems-in-an-era-of-smart-devices.

[40] L. Schoenherr, M. Golla, T. Eisenhofer, J. Wiele, D. Kolossa, and T. Holz. *Unacceptable, where is my privacy?* accessed: 09.04.2025. Nov. 2021. URL: https://unacceptable-privacy.github.io/index.html.

[41] A. R. Biswas and R. Giaffreda. "IoT and cloud convergence: Opportunities and challenges". In: *Internet of Things WF-IoT*. 2014. DOI: 10.1109/WF-IoT.2014.6803194.

[42] N. Olsen. *Voice Assistants and Privacy Issues - Privacy Policies*. Ed. by N. Olsen. accessed: 10.04.2025. June 2022. URL: https://www.privacypolicies.com/blog/voice-assistants-privacy-issues/.

[43] Consumer advice center. *Smart Home - The intelligent Home*. accessed: 10.04.2025. Oct. 2024. URL: https://www.verbraucherzentrale.de/wissen/umwelt-haushalt/wohnen/smart-home-das-intelligente-zuhause-6882.

[44] Federal Office for Information Security. *Identity theft via data leaks and doxing*. URL: https://www.bsi.bund.de/dok/6692610.

[45] J. Thorpe-Smith. *Data Leaks: The Biggest Risks, Consequences, Causes & How to Prevent Them — Metomic*. Nov. 2024. URL: https://www.metomic.io/resource-centre/what-are-the-biggest-risks-of-data-leaks.

[46] dpa Service. *Securely networked?: how data protection works in the smart home*. accessed: 10.04.2025. May 2021. URL: https://www.zeit.de/news/2021-05/20/so-geht-datenschutz-im-smarthome.

[47] Dr. T. J. Heydn. *Advice on drafting contracts for the Internet of Things (IoT)*. accessed: 10.04.2025. 2021. URL: https://www.tcilaw.de/hinweise-zur-vertragsgestaltung-beim-internet-of-things-iot/.

[48] Consumer advice center NRW. *Data disclosure: How to find out what companies know about you*. accessed: 10.04.2025. 2023. URL: https://www.verbraucherzentrale.nrw/wissen/digitale-welt/datenschutz/datenauskunft-so-erfahren-sie-was-unternehmen-ueber-sie-wissen-44238.

[49] Amazon.de. *Amazon.de Privacy Notice*. accessed: 10.04.2025. 2024. URL: https://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=GX7NJQ4ZB8MHFRNJ&language=en_GB.

[50] Amazon.de. *Alexa Terms of Use*. accessed: 10.04.2025. 2023. URL: https://www.amazon.de/gp/help/customer/display.html?nodeId=201809740.

[51] *What is AWS Database Migration Service? - AWS Database Migration Service*. accessed: 09.04.2025. 2024. URL: https://docs.aws.amazon.com/dms/latest/userguide/Welcome.html.

[52] European Commission. *Right to repair: Questions & Answers*. accessed: 10.04.2025. 2023. URL: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_23_1795/QANDA_23_1795_EN.pdf.

[53] Q. Baterna. *6 Ways to Make It Harder for Data Brokers to Collect Your Data*. accessed: 10.04.2025. Nov. 2021. URL: https://www.makeuseof.com/ways-to-make-it-harder-for-data-brokers-collect-your-data/.

[54] Federal Ministry for Digital and Transport. *EU verabschiedet Data Act*. accessed: 10.04.2025. 2023. URL: https://web.archive.org/web/20250323125138/https://bmdv.bund.de/DE/Themen/Digitales/Digitale-Gesellschaft/EU-Data-Act/eu-data-act.html.

[55] European Commission. *Frequently Asked Questions - Data Act*. accessed: 10.04.2025. 2024. URL: https://digital-strategy.ec.europa.eu/de/library/commission-publishes-frequently-asked-questions-about-data-act.

[56] Dr. D. Pauly and Dr. A. Lohbeck. *EU: Data Act – How fair is the draft regulation for more fairness in the data economy?* accessed: 10.04.2025. 2022. URL: https://linklaters.de/insights/publikationen/tmt/datenschutz/2022/februar/eu-data-act.

[57] Prof. Dr. W. Kerber. *The EU "Data Act": A Critical Analysis*. accessed: 10.04.2025. 2022. URL: https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/prof-wolfgang-kerber/presentation/2022_03_21-kerber-pres-data-act.pdf.

[58] European Data Protection Supervisor. *History of the development of the GDPR*. accessed: 10.04.2025. Dec. 2024. URL: https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_de.

[59] Stiftung Datenschutz (Foundation for Data Protection), BDV e.V., and DIHK. *Data Act and GDPR: For more legal clarity on data access and use*. accessed: 10.04.2025. 2022. URL: https://dsgvo-2024.org/wp-content/uploads/2022/08/BvD_Stiftung-Datenschutz_DIHK_Positionspapier_Data-Act-und-DSGVO_v1.pdf.

[60] M. Goetz and Prof. Dr. B. P. Paal. *Between data use and data protection: The relationship between the GDPR, Data Act and Data Governance Act*. Dec. 2024. URL: https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/zwischen-datennutzung-und-datenschutz-438.

[61] S. Piasecki. "Expert perspectives on GDPR compliance in the context of smart homes and vulnerable persons". In: *Information & Communications Technology Law* 32.3 (2023), pp. 385–417. ISSN: 1360-0834. DOI: 10.1080/13600834.2023.2231326. URL: https://www.tandfonline.com/doi/full/10.1080/13600834.2023.2231326#d1e109.

[62] Harvard Business School Online. *Data Analytics Privacy Issues & How to Avoid Them*. accessed: 10.04.2025. 2015. URL: https://online.hbs.edu/blog/post/data-privacy-issues.

[63] K. Ahuja and M. Patel. *There's No Place Like A Connected Home: Perspectives on the connected consumer in a world of smart devices*. accessed: 10.04.2025. Nov. 2020. URL: https://www.mckinsey.com/spContent/connected_homes/index.html.

[64] J. Bugeja, A. Jacobsson, and P. Davidsson. "An Empirical Analysis of Smart Connected Home Data". In: *Internet of Things - ICIOT 2018*. Ed. by D. Georgakopoulos and L.-J. Zhang. Information Systems and Applications, incl. Internet/Web, and HCI. Cham: Springer International Publishing and Imprint: Springer, 2018, pp. 134–149. ISBN: 978-3-319-94370-1. DOI: 10.1007/978-3-319-94370-1_10. URL: https://link.springer.com/chapter/10.1007/978-3-319-94370-1_10.

[65] D. Bastos et al. *GDPR Privacy Implications for the Internet of Things*. 2018. URL: https://www.

researchgate . net / publication / 331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things.

[66] V. Dahl and M. Österlin. *Impact of GDPR on Data Sharing Behavior of Smart Home Users*. Oct. 2020.

[67] enforcementtracker.com. *GDPR Enforcement Tracker - list of GDPR fines*. accessed: 02.12.2024. 2/12/2024. URL: https://www.enforcementtracker.com/?insights.

[68] M. Holzhofer. “746 Mio. Euro Bußgeld gegen Amazon Europe Core S.à r.l”. In: *Compliance Essentials GmbH* (30/07/2021). accessed: 02.12.2024. URL: https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-amazon-europe-2021-07-30-LU-1448.php.

[69] European Data Protection Board. “Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR”. In: (2023). accessed: 12.02.2024. URL: https://www.edpb.europa.eu/system/files/2023-05/edpb_bindingdecision_202301_ie_sa_facebooktransfers_en.pdf.

[70] META Platforms Inc. *Meta Reports Fourth Quarter and Full Year 2023 Results; Initiates Quarterly Dividend*. accessed: 09.04.2025. 1/02/2024. URL: https://investor.fb.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx.

[71] C. Runte et al., eds. *Enforcement Tracker Report 2024*. accessed: 09.04.2025. 2024. URL: https://cms.law/en/media/international/files/publications/publications/gdpr-enforcement-tracker-report-may-2024?v=5.

2025, © Copyright by authors, Published under agreement with IARIA - www.iaria.org