Identification of Key Requirements for the Application of Data Sovereignty in the Context of Data Exchange

Steffen Biehs
Fraunhofer ISST
steffen.biehs@isst.fraunhofer.de

Jonas Stilling
Fraunhofer ISST
jonas.stilling@isst.fraunhofer.de

Abstract

With the growing digitization in our modern world, data is becoming an increasingly valuable business asset. Therefore, it is crucial that individuals and organizations are aware of their data sovereignty when it comes to selling and sharing data assets. This research paper aims to identify the essential requirements for the application of data sovereignty in the context of data exchange. Currently, the literature falls short of providing a comprehensive overview of this subject. The study conducts a literature review and expert interviews to identify key requirements for applying data sovereignty in the context of data exchange. The result identifies eight key requirements including access control, usage control, location, technical aspects, legal considerations, organizational compliance, monetization, and data quality. Understanding and considering these requirements can enable organizations to achieve data sovereignty and facilitate secure and trusted data exchange.

Keywords: Data Sovereignty, Requirements, Data Exchange, Literature Review, Interviews

1. Introduction

Data is becoming increasingly critical to business success. It is therefore not surprising that in the top ten of Forbes magazine's annual ranking of brand value, six of the listings are directly or indirectly related to digitization or data-driven business models (Forbes, 2022). Individual voices even increasingly see data as the world's most valuable resource (Parkins 2017). However, the ongoing developments are inevitably accompanied by a shift away from purely goods-based with commodity-based business principles towards service-oriented business logics (Lusch & Vargo, 2006). In order to meet these demands, data management is of paramount importance.

In an industrial ecosystem, it is essential to maintain total control over data, particularly once it is to be shared (Otto et al., 2020). This ability is denoted as data sovereignty. It should be applied at all stages in the lifecycle of a data asset, especially where the data is exchanged. Because often exchanging data means relinquishing control (Otto et al., 2019). Due to the importance of this topic, major initiatives have emerged in Europe in recent years with the aim of establishing guidelines and standards for sovereign data exchange in larger networks (e.g., Gaia-X, International Data Spaces Association (IDSA), Catena-X). To perform a data exchange in a sovereign manner, various mechanisms can be used. In addition to data aggregation and technical mechanisms, the literature frequently discusses and applies only access and usage control (Opriel & Schmelting, 2022; Usländer et al., 2022; Hillermeier et al., 2021; Zrenner et al., 2019).

If these mechanisms are to be used for sovereign data exchange, other questions inevitably arise as to how the data exchange can be carried out in a sovereign manner and which conditions must be met for its realization. Unfortunately, there is no general overview of data sovereignty requirements in the literature. This makes it difficult for organizations to assess what they need to consider in order to successfully apply data sovereignty. The existing reviews on data sovereignty either distinguish data sovereignty from other sovereignties (Hummel et al., 2021; Hellmeier & von Scherenberg, 2023), concentrate on implementing data sovereignty requirements (Hellmeier et al., 2023), or set their focus only on usage control, access control, and other technical mechanisms, as previously explained.

Since the overview of the requirements for the application of data sovereignty has been poorly surveyed, the number of articles and papers that reflect general requirements of data sovereignty is manageable. In summary, the specific requirements for applying data sovereignty remain unknown. Furthermore, data sovereignty as well as sovereign data exchange are widely discussed topics (Schmidt et al., 2022, Pettenpohl et al., 2022 Bader et al., 2020), but with a limited and inconsistent number of requirements. We aim to address these issues by

URI: https://hdl.handle.net/10125/106896
978-0-9981331-7-1

identifying key requirements from the literature and expert interviews for applying data sovereignty to address the aforementioned research gap of the non-existing overview of data sovereignty requirements. For identifying the requirements, we limit our focus to the context of data exchange, as there are other contexts, such as indigenous population, governmental organizations, and countries, discussed in the literature (Hummel et al., 2021).

From this point of view, the following research question arise:

RQ: Which key requirements for the application of data sovereignty in the context of data exchange can be derived from the literature with the support of expert interviews?

To answer this question, we will first conduct a literature review to collect and aggregate data sovereignty requirements. Subsequently, expert interviews will be conducted to verify and refine the previously aggregated results. The result of both approaches will be key requirements for the application of data sovereignty in the context of data exchange.

2. Fundamentals

2.1. Data Sovereignty

In academic literature, data sovereignty appears as a multifaceted issue with numerous implications (Hummel et al., 2021). Nevertheless, data sovereignty can be defined as the concept of self-determination and the ability of an individual or corporate entity to determine and exercise their right to use their data (Otto, 2016). The term data sovereignty is used to emphasize technical solutions for protecting data assets. It is about self-determination and control over data assets themselves, but it is often mentioned alongside digital, technological, and cyber sovereignty, which are about political discussions and legal constraints. (Hellmeier & von Scherenberg, 2023). One important aspect of enabling data sovereignty is the exchange of data itself, which is further discussed in the next section.

2.2. Sovereign Data Exchange

Referring to the aforementioned definition of data sovereignty, sovereign data exchange is defined as the ability of a data owner to share its data with data consumers without losing its data sovereignty (Schmidt et al., 2022). It aims to ensure that data providers have control over their data assets not only before but after data is shared with others. This means that a data owner can define usage restrictions to their data, before sharing it with data consumers. Data consumers must accept the usage restrictions before they can request and use the data.

Sovereign data exchange is a widely discussed topic and often overlaps with data sovereignty or is used as a synonym (Schmidt et al., 2022, Pettenpohl et al., 2022, Bader et al., 2020). There are several approaches to ensure sovereign data exchange, such as the International Data Spaces (IDS) initiative (Otto et al., 2019) or GAIA-X (Niebel et al., 2022). The interconnection of different platform and service providers (Schrauf et al., 2020) to form data ecosystems underscores the need for effective mechanisms for a sovereign data exchange. Only when ecosystems guarantee an appropriate form of data sovereignty the fears of losing control over data can be mitigated (Otto, 2019).

3. Research Method

To achieve the goal of identifying key requirements for the application of data sovereignty in the context of data exchange, the consideration of practical knowledge is of particular importance. Therefore, we take a qualitative research approach by combining two different data sources. The first is a systematic literature review and the second is interviews with experts with scientific and practical knowledge. In the following, we describe the research approach for the two data sources separately. Figure 1 depicts the research approach graphically.

3.1. Literature Review

As a first step, this paper reports on a systematic literature review to uncover the requirements of data sovereignty. We followed Webster and Watson's (2002) well-established guidelines for literature reviews. The first task **(1)** was to search for appropriate literature. We decided to use two databases. Initially, AISeL was selected as the leading database for information systems (IS) research, including some journals and the major IS conferences (e.g., ECIS, HICSS, and ICIS). Second, we supplemented the database by using Scopus to search for IS journals.

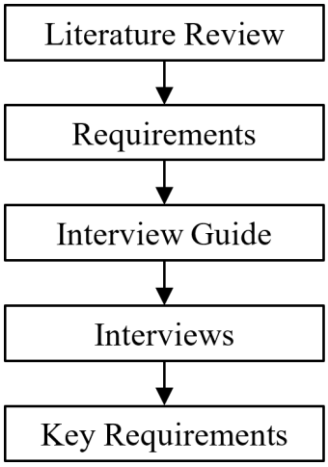

Figure 1. Research Method Process.

In the second task **(2)**, we identified keywords that would yield results that fit our research question. A first finding from the literature review is the synonymous and overlapping use of the terms *data sovereignty* and *sovereign data exchange*. Since one of our goals is to differentiate or classify the two terms, we searched for both keywords.

Table 1 lists the keywords and the results they produced for each database. We used the title and abstract search in both databases, producing 13 (AISeL) and 322 (Scopus) papers.

Table 1. Literature Review - Keywords and Results

Database	Keywords	Results
AISeL	title: "Data Sovereignty" OR abstract: "Data Sovereignty" OR title: "Sovereign Data Exchange" OR abstract: "Sovereign Data Exchange"	13
Scopus	TITLE ("Data Sovereignty") OR ABS ("Data Sovereignty") OR TITLE ("Sovereign Data Exchange") OR ABS ("Sovereign Data Exchange")	322
3 Iterations	AISeL & Scopus	19

In a third step **(3)**, we filtered and reviewed the papers in three iterations. **First**, we assessed the thematic fit of the papers, excluding ones that did not focus on data sovereignty or sovereign data exchange by examine the title and abstract. We also excluded papers that were inaccessible to us, as well as duplicate papers. In the **second** iteration, the resulting papers were reviewed in their entirety and roughly skimmed to see if they addressed the thematically relevant content. This drastically reduced the number of relevant papers to two papers in AISeL and four papers in Scopus. Based on the results of the second iteration, relevant papers were added in the **third** iteration through forward and backward searches. In addition, other papers were reviewed and added to the result set. These include articles from the Catena-X and Gaia-X projects, both of which are freely available. The articles all have a strong focus on sovereign data exchange by using the IDS approach.

This resulted in 19 papers that were further investigated with respect to the requirements for the application of data sovereignty. During the investigation, various requirements were identified, which could afterwards be grouped into individual requirements. For example, *the user can attach usage policies to its data*. This requirement was derived of "Each participant can define usage policies and attach them to outbound data" (Otto et al., 2019). These requirements form the basis for the interview guide. Table 2 shows the identified requirements with their respective references.

Table 2. Extracted Requirements.

Requirements	References
The user has full control over access to their own resources	Usländer, 2022
Only selected users are allowed to view the offers of a resource	Catena-X, 2023; Schmidt et al., 2022
The user can attach usage policies to its data	Otto et al., 2019
The provider has full control over its usage policies	Zrenner et al., 2019; Catena-X, 2023; Otto & Jarke, 2019
Mechanisms exist to enforce the usage policies	Otto et al., 2019; Zrenner et al., 2019; Altendeitering et al., 2022; Opriel & Schmelting, 2022
It must be known where the data is stored	Zrenner et al., 2019; Esposito et al., 2016; Amoore, 2018; Polatin-Reuben & Wright, 2014
It must be known where the servers of the data	Zrenner et al., 2019; Peterson et al., 2011; Hippelainen et al., 2017

receiver are located	
Authentication & authorization services are required	Otto et al., 2019; Opriel et al., 2021; Otto & Jarke, 2019; Schmidt et al., 2022; Hillermeier et al., 2022
There must be a kind of certification	Otto et al., 2019; Opriel et al., 2021; Otto & Jarke, 2019; Schmidt et al., 2022; Hillermeier et al., 2022
The technical prerequisites for the use of data sovereignty should be as low as possible	Schmidt et al., 2022
There is technical interoperability	Zrenner et al., 2019; Schmidt et al., 2022; Altendeitering et al., 2022
Secure communication	Otto et al., 2019; Niebel et al., 2022; Otto & Jarke, 2019; Schmidt et al., 2022; Hillermeier et al., 2022
Usage control processes must be transparent	Zrenner et al., 2019; Catena-X, 2023; Jarke et al., 2019
Compliance with applicable legislation (e.g., GDPR)	Opriel & Schmelting, 2022; Niebel et al., 2022; Schmidt et al., 2022
Compliance with common rules and standards	Niebel et al., 2022
All usage and access policies must be enforced	Altendeitering et al., 2022

3.2. Expert Interviews

The key requirements developed in this paper are based on qualitative interviews with six experts from industry and research practice. When selecting the experts, it was important that they come from as many different disciplines as possible in order to diversify the responses. For research purposes, interviews are an accepted method of data collection that is firmly rooted in the experiences of industry practitioners and in the social environment (Schultze & Avital, 2011; Myers, 1997).

We selected interview partners based on various stakeholder roles to obtain the most comprehensive view for identifying key requirements in terms of the application of data sovereignty in the context of data exchange. Each interview was conducted using a semi-structured guide. Thus, the research keeps structure and comparability, but still leaves enough flexibility to adapt to ad hoc situations in the interviews (Mayring, 2014).

The interviews are divided into two parts: First, we asked general questions about recent projects and initiatives related to the application of data sovereignty. In addition, we asked about challenges and requirements for the application of data sovereignty. The second part of the interview is dedicated to the requirements from Table 2. Based on these requirements, the experts are asked to contribute their knowledge on how the requirements apply to their projects from part one of the interview.

All interviews were conducted virtually, last an average of 31 minutes, and were recorded and transcribed for further analysis. Table 3 provides an overview of the experts and the length of each interview as well as their index number for further referencing.

Table 3. Overview of the Expert Interviews

Experts	Duration (h)	ID
Data space expert	00:36	I1
Security expert	00:37	I2
AI expert	00:25	I3
Usage control expert	00:25	I4
Data sharing industry	00:29	I5
Telecommunication industry	00:32	I6

Experts I1 to I4 come from the area of research. I5 and I6 are from industry. Geographically, they are all classified in the Central and Southern European region. All experts have several years of experience in their respective fields.

Based on the transcribed interviews, we conducted a qualitative content analysis to analyze the content of the interviews using MaxQDA. Qualitative content analysis (Krippendorff, 2019; Mayring, 2014) is a flexible (Mayring, 2014) research technique that allows the analysis and interpretation of meanings from qualitative data (Krippendorff, 2019; Weber, 1990) as it delivers “replicable and valid inferences from texts […]” (Krippendorff, 2019). The analytical process focuses on coding elements of the documents (Weber, 1990). In the qualitative content analysis, six codes with a total of 20 subcodes, which were deductively derived from the literature analysis, were used. In addition, further codes were formed inductively in the process of the analysis. Central for

every qualitative content analysis is the system of categories, which can either be deducted from theory, inductively derived from the text, or determined by a combined method (Mayring, 2014). At the beginning of the qualitative content analysis, five categories were deductively identified, derived directly from the literature review requirements in Table 2.

4. Findings

Based on the interviews, eight key requirements for the application of data sovereignty in the context of data exchange were derived from the literature review and the interviews. The resulting key requirements are described in more detail below. This section answers **RQ**.

4.1. Access Control

Access control is a technique used to regulate which entities in a system are allowed to access certain data resources. It is a fundamental security concept that minimizes the risk of unauthorized access to a data resources. Formulating access control restrictions (access policies) by a data owner helps on preventing data breaches, theft, or misuse of sensitive data (Zrenner et al., 2019). Access policies are used to set requirements for users who want to get access to data assets and for programs that run on behalf of users (Munoz-Arcentales et al., 2020). To enforce access control in a system architecture, an identity service is required to ensure the identity of specific users so that access to data can be managed on a per-user basis. This can be achieved through a variety of means, including credentials, privileges, and multi-factor authentication. It involves granting permissions to subjects (users or entities) based on different access control models (Jung & Dörr, 2022).

On the one hand, this technique is mentioned in the literature as an important requirement (Hillermeier et al., 2022) and, on the other hand, seen by the interviewees (I1, I2, I5) in general as an important and necessary requirement for the application of data sovereignty in order to protect one's own data.

Access control mechanisms have existed for a long time (I5), e.g., for multiple-user resource sharing on computer systems (Browne & Steinauer, 1971). This is an advantage for this requirement since there is less of a hurdle to overcome in the application.

4.2. Usage Control

According to Opriel and Schmelting (2022), usage control is the second equally important mechanism for ensuring data sovereignty. It extends the aforementioned access control technique by providing solutions for restricting the use of data assets after the access has been granted. Thus, usage control focuses on defining and enforcing restrictions on the use of a data asset (Jung & Dörr, 2022). It enables data owners to apply technical constraints (usage policies) to their data and ensure that it is processed, aggregated, and distributed according to their constraints (Jung & Dörr, 2022). These constraints can be applied at all levels of the data processing pipeline, including the storage of the data assets (Park & Sandhu, 2022). The primary purpose of usage control is to establish and enforce restrictions in a data exchange environment (Akaichi & Kirrane, 2022). It can therefore be understood as protection for the data provider himself.

The results of the literature review show that usage control is a crucial requirement for the application of data sovereignty (Opriel et al., 2021; Catena-X, 2023; Niebel et al., 2022; Schmidt et al., 2022; Hillermeier et al., 2022). This is also consistently understood by the experts. According to them, this leads to implementation problems and thus challenges in the realization of these key requirements (I5). One possible solution suggested by the experts is a single usage control standard, such as HTTP for communication or JSON for data format (I5). This would greatly facilitate the application of data sovereignty. Policy enforcement also imposes several requirements to facilitate the application of data sovereignty. For example, it was mentioned that the system architecture must follow security by design (Waidner et al., 2013) principles from the ground up and be designed for policy enforcement (I4). This is the best way to ensure that policies are followed. Ultimately, the degree of enforcement depends on the use case. For example, if someone is participating in a research project where usage control is not a top priority, then the mechanism serves more as a tool and policies play a secondary role (I5).

However, what cannot be ignored when it comes to policies, experts say, is quality (I4). As with a computer program, errors can lead to serious security problems. Therefore, it is important to implement mechanisms for early error detection in order to maintain a high level of policy quality to prevent misuse (I2, I5).

4.3. Location

The third key requirement covers relevant aspects related to the location of data and servers. The experts interviewed also found the requirements behind this key requirement to be relevant across the board (I1, I2,

I4, I5, I6). Especially in the context of international data exchange. For a successful application of data sovereignty, it must be ensured that a user (in this case the data provider) can track exactly where the servers of a data consumer are located (Zrenner et al., 2019; Peterson et al., 2011; Hippelainen et al., 2017), e.g., in order to comply with applicable regulations (I2, I5). To that end, the consumer has two options for where to run their server: On-premises or in the cloud (I2). On-premises servers are more secure in terms of location (I4, I6). The provider can see exactly where the servers are located. The situation is different in the cloud, where there are now enough options to determine the physical location of the server (I2). Care must be taken to ensure that the consumer's information remains transparent.

However, in addition to the location of the server, the location of the data on the consumer side may be differ from the location of the server (Zrenner et al., 2019; Esposito et al., 2016; Amoore, 2018; Reuben & Wright, 2014). Again, the provider has a legitimate interest in knowing this, e.g., to comply with location restrictions (I5).

What mattered to the experts at this point was that the consumer should have the freedom to choose which cloud host to use, as long as the locations were also transparently shared (I2, I5).

4.4. Technical

Technical requirements were the most important category for the experts (I1, I2, I3, I4, I5, I6), along with usage control, for the successful application of data sovereignty in the context of data exchange. The literature review also reveals a similar statement (Jarke et al., 2019). In addition to the requirements authentication & authorization services (Otto et al., 2019; Opriel et al., 2021; Otto & Jarke, 2019; Schmidt et al., 2022; Hillermeier et al., 2022) and certification (Otto et al., 2019; Opriel et al., 2021; Otto & Jarke, 2019; Schmidt et al., 2022; Hillermeier et al., 2022), the focus here is on both low-level technical prerequisites for the applying of data sovereignty (Schmidt et al., 2022) as well as technical interoperability between systems and participants (Zrenner et al., 2019; Schmidt et al., 2022; Altendeitering et al., 2022) and secure communication during data exchange (Otto et al., 2019; Niebel et al., 2022; Otto & Jarke, 2019; Schmidt et al., 2022; Hillermeier et al., 2022).

The interviews revealed that authentication and certification are the most important requirements from the perspective of the reviewers (I1, I3, I4, I5, I6). Before exchanging data, users want to know who they are dealing with and if they can trust them (I4). A certificate serves as a contract of participation in the data space (I1). The same applies to the components to be used and their algorithms. These must also be secured by a certificate (I3). Otherwise, the user runs the risk of other algorithms, for example, recalculating the raw data from the processed data. This can be remedied, for example, by using a trusted execution environment for data processing (I3).

Regarding the need for secure communications, there was unanimous agreement that this must now be standard in electronic communications (I1, I2, I5, I6). However, care must be taken to ensure that these and other security mechanisms are efficient, e.g., in terms of computing power, so that they do not become a hindrance in the end (I2). Security takes time and effort - and this must not be at the expense of data sovereignty. At the beginning, security is always a hindrance because it is initially complex and costly to implement (I2). However, as participation in the data space progresses, the trend should be reversed. A solid security substructure within the own architecture can help (I2).

A clear picture emerged from the interviews regarding the requirements for technical interoperability and the low technical prerequisites for applying of data sovereignty. The fact that additional software has to be integrated into the company's own IT landscape for sovereign data exchange was clearly identified as a hindrance for applying of data sovereignty (I1, I4). The integration may require special controls, which increases the effort (I1). According to the experts, it can be advantageous to use ready-made and standardized software. It is therefore important to try to keep the effort of integrating new software for sovereign data exchange as low as possible (I1).

4.5. Legal

This key requirement is considered relevant by the experts (I1, I2, I3, I5, I6). According to the experts, the transfer of a product must always be based on a contract (I4). In addition, there may be legal requirements that restrict the transfer of products. What is regulated by import and export restrictions for tangible goods also exists for intangible products such as data. In this case, both national and international regulations apply (I5). If data is to be exchanged within the EU, the GDPR, among others, must be observed (Opriel & Schmelting, 2022; Niebel et al., 2022; Schmidt et al., 2022). In addition, common rules and standards should be agreed upon within a data space (Niebel et al., 2022). Legal rules need to be integrated so that access and usage control processes can be controlled, enforced (Altendeitering et al.,

2022) and made transparent (Zrenner et al., 2019; Catena-X, 2023, Jarke et al., 2019). Furthermore, every nation has its own regulations (I6).

In research contexts, the focus is on technical implementation, legal requirements for government data exchange have not yet received much attention (I2). As a result, policy requirements on the consumer side often only become effective through legal contracts (I1).

4.6. Organizational Compliance

The interviews revealed that each company must comply with its own regulations (I2, I3, I5). They reflect the rules of the company, e.g., no child labor or human trafficking, CO2-neutral production, responsible handling of data (Lauf et al., 2022) (I5) or which host may be used (I5) and can depend on the individual case (I6). Within the technical and legal framework, various compliance requirements can be imposed on the company's own data exchange. For example, compliance may mean that critical data must not be shared (I3). However, compliance can also be interpreted so strictly that it stands in the way of data exchange. If every incoming packet is to be inspected, this will certainly discourage data providers, since data sovereignty is at risk at this point (I2). Compliance has an impact on data access, usage policies, and location, and is therefore a critical factor in leveraging data sovereignty in the context of data exchange (I4).

4.7. Monetization

This key requirement also was not previously identified in the literature review. It was directly derived from the expert interviews.

When a data exchange takes place, the data consumer has a strong interest in the data (Hellmeier et al., 2023) e. g., it has a high monetary value. During the data exchange, the data to be exchanged is a commodity that is transferred from the data provider to the consumer. For the consumer, the cost of the data exchange must be worthwhile, otherwise it is not worthwhile from a business perspective. To meet this requirement, the provider must ensure that the data it offers meets this monetary value, e.g., because the data is so worth protecting that data exchange is worthwhile through data sovereignty (I2).

4.8. Data Quality

The last key request follows the previous one. During the interviews, the experts repeatedly referred to data quality in the context of data becoming a product (I1, I5, I6). Looking at the purchase of real goods from a business perspective, the buyer has a strong interest in the quality of the good (I6). This can also be applied to data exchange. According to interviewee I6, the trend should not be towards *Big Data*, but towards *Better Data*.

5. Discussion

In this study, we aimed to identify the key requirements relevant for the application of data sovereignty in the context of data exchange. Our research revealed eight key requirements. In this section, we discuss the creation of these key requirements by the connection between the findings from the literature review and those from the interviews. In addition, the resulting implications are discussed.

To identify the requirements for data sovereignty, a literature review was conducted as a first step. The focus was on identifying data sovereignty requirements in the context of data exchange from a conceptual perspective. That is, requirements for implementation or concrete realization were not considered. This decision was made in order to obtain a holistic and independent view of data sovereignty requirements.

As part of a literature review, we examined 19 papers to identify data sovereignty requirements. We identified 16 distinct requirements, which provided a comprehensive overview of each author's understanding of data sovereignty, contrary to our initial assessment. It should be noted, however, that outside of these 19 papers, the term data sovereignty is often understood in very different contexts (Zrenner et al., 2019; Hellmeier & von Scherenberg, 2023). This shows that research on data sovereignty is still very young and has only become better known in recent years through research projects in connection with the IDSA.

For the **RQ** this means that we were able to identify 16 requirements through the literature review, which served as the basis for the next research method which was the expert interviews. This provided the opportunity to obtain even more detailed requirements for applying of data sovereignty. At the same time, we were aware of the problem that experts could have completely different opinions.

The experts were asked about current or past projects related to data sovereignty and how the identified requirements relate to them. The result was eight key requirements: *Access Control*, *Usage Control*, *Location*, *Technical*, *Legal*, *Organizational Compliance*, *Monetization* and *Data Quality*.

The difference to previous works in the literature is that there is no collected overview of data sovereignty requirements in general. The context of the requirements elicitation is stated according to the topic of each paper. Opriel & Schmelting (2022) describe data sovereignty as an elementary requirement for enterprises, but only address usage control and access control and a few approaches to legal requirements in their article. Usländer et al. (2022) also consider usage control and access control as requirements in their requirements analysis for data sovereignty in the field of manufacturing but no more. Also focusing on usage control, access control and technical aspects are Hillermeier et al. (2021) in their paper. Schmidt et al. (2022) broadened the focus of their study. However, here too, only the technical aspects as well as usage control and access control are considered. Furthermore, there is no work that substantiates their requirements through expert interviews. Thus, only the key requirements *Access Control*, *Usage Control*, *Location*, *Technical* and *Legal* are consistent with findings from the literature. For the three other ones, *Organizational Compliance*, *Monetization* and *Data Quality*, no requirements or findings could be identified. This is because most authors have prioritized usage control, access control, and technical aspects pertaining to data sovereignty. This represents a knowledge gap in the elicitation of data sovereignty requirements. In addition, it has become clear that some key requirements are interrelated. For example, *Organizational Compliance* can have a direct impact on *Technical* and *Legal* requirements if specific hardware is required and data can only be exchanged with partners in one country. Or the key requirement *Legal* may have an impact on the choice of the server location.

Based on the interviews, it can be said that the authors of the studies examined generally have a very similar understanding of data sovereignty. The results obtained are in line with the authors of the literature. The findings from the interviews complement them.

With this work, we created a new overview of requirements to be able to apply data sovereignty in the context of data exchange in a way that all aspects for a successful data exchange can be considered and so overcome our research gap. Previous research has shown that mainly technologies like usage control and access control as well as technical aspects like authentication and certification have been addressed. We were able to show that much more expertise, such as in the legal field or the location of the server, is needed for the application of data sovereignty. In addition, our research has shown that there is much more to the application of data sovereignty. This is reflected, among other things, in appropriate data quality or a company's organizational compliances, which can make the use of data sovereignty obsolete if not addressed.

The resulting implications for practice are that users and researchers are provided with an outline of requirements, allowing them to define and adapt their tools to fully apply data sovereignty. This may be necessary, for instance, when new data spaces are created. Participants join who may never have had prior contact with the topic of data exchange or data sovereignty. By utilizing the key requirements of this paper, these participants now have a tool to evaluate all facets of data sovereignty in the context of data exchange. This also applies to pre-existing data spaces. The findings may be utilized to refine current frameworks to holistically address data sovereignty within the scope of data exchange. They can also enable organizations to achieve data sovereignty and facilitate secure and trusted data exchange.

6. Further Research

In this paper, a theoretical approach has been taken to provide a first overview and thus a basis for the requirements of data sovereignty. The approach should be further deepened in the future. Building on the results of this paper, this can be done, for example, through a further and larger survey study in the context of an industrial sector, in order to derive design principles from the key requirements. A pilot project would also be conceivable, in which the project partners could use the results and verify them.

Another approach would be to analyze the application of data sovereignty in European initiatives such as Catena-X and Gaia-X and compare it with the results of this paper.

Additionally, it would be beneficial to explore the contexts in which data sovereignty can be further examined besides the implementation landscape (Hellmeier et al., 2023) or term examination (Hummel et al., 2021; Hellmeier & von Scherenberg, 2023). A legal evaluation of the topic would also enhance the findings of this paper and bolster the legal framework of data sovereignty.

As the interviewees all come from similar geopolitical backgrounds, it would be interesting to conduct another interview study with a wider selection of partners to see if this can lead to new requirements for the application of data sovereignty in the context of data exchange, or if the need for specific requirements is weighted differently.

7. Conclusion

In this work, eight key requirements for the application of data sovereignty in the context of data exchange were identified. To do this, we first conducted a literature review on data sovereignty requirements, from which we were able to identify 16 requirements. Based on the results, expert interviews were conducted to gain deeper insight and validate the requirements. Eight key requirements for the application of data sovereignty in the context of data exchange emerged. The results were then discussed as well as the practical implications.

In particular, the three key requirements for data sovereignty from the expert interviews - *Organizational Compliance*, *Monetization*, and *Data Quality* - can show researchers and practitioners that there are more requirements for applying data sovereignty than the literature has previously revealed.

Data sovereignty also extends to more processes than just data exchange. Negotiating a usage policy and enforcing it after the data exchange are also part of data sovereignty. However, this paper only considers data sovereignty in the context of data exchange. What data sovereignty requirements apply in other contexts, such as the fulfillment of usage policies, is a subject of further research.

Data sovereignty will increasingly become an enabler in the future and is frequently discussed nowadays. In analogy to today's standard encryption in electronic communication, the following quote was made during an expert interview: "I think data sovereignty is a hygiene factor in the long run. You just must have it with you, you have to take these principles into account somehow" - this is what the paper is supposed to contribute to in the long term.

7. References

Akaichi, I., & Kirrane, S. (2022). Usage Control Specification, Enforcement, and Robustness: A Survey. https://arxiv.org/abs/2203.04800 (accessed 02/23)

Altendeitering, M., Pampus, J., Larrinaga, F., Legaristi, J., & Howar, F. (2022). Data sovereignty for AI pipelines. https://doi.org/10.1145/3522664.3528593

Amoore, L. (2016). Cloud geographies. Progress in Human Geography, 42(1), 4–24. https://doi.org/10.1177/0309132516662147

Bader, S., Pullmann, J., Mader, C., Tramp, S., Quix, C., Müller, A., Akyürek, H., Böckmann, M., Imbusch, B. T., Lipp, J., Geisler, S. & Lange, C. (2020). The International Data Spaces Information Model – An Ontology for Sovereign Exchange of Digital Content. In Lecture Notes in Computer Science (S. 176–192). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-62466-8_12

Browne, P., & Steinauer, D. D. (1971). A model for access control. https://doi.org/10.1145/1734714.1734734

Catena-X. (2023). 0018 ECLIPSE DATASPACE CONNECTOR - PLATFORM CAPABILITY: SOVEREIGN DATA EXCHANGE. v1.0.1. URL: https://catena-x.net/de/standard-library (accessed 02/23)

Esposito, C., Castiglione, A., & Choo, K. R. (2016). Encryption-Based Solution for Data Sovereignty in Federated Clouds. IEEE Cloud Computing. https://doi.org/10.1109/mcc.2016.18

Forbes (2022). The World's Most Valuable Brands. URL: https://www.forbes.com/powerful-brands/list/ (accessed 08/23)

Hellmeier, M., Pampus, J., Qarawlus, H. & Howar, F. (2023) Implementing Data Sovereignty: Requirements & Challenges from Practice. In Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). Association for Computing Machinery, New York, NY, USA, Article 143, 1–9. https://doi.org/10.1145/3600160.3604995

Hellmeier, M. & von Scherenberg, F. (2023). A Delimitation of Data Sovereignty from Digital and Technological Sovereignty. ECIS 2023 Research Papers. 306. https://aisel.aisnet.org/ecis2023_rp/306

Hillermeier, O., Punter, M., Schweichhart, K., & Usländer, T. (2021). Data Sovereignty – Critical Success Factor for the Manufacturing Industry. In Zenodo (CERN European Organization for Nuclear Research). European Organization for Nuclear Research. https://doi.org/10.5281/zenodo.5675873

Hippelainen, L., Oliver, I., & Lal, S. (2017). Towards Dependably Detecting Geolocation of Cloud Servers. In Lecture Notes in Computer Science. Springer Science+Business Media. https://doi.org/10.1007/978-3-319-64701-2_51

Hummel, P., Braun, M., Tretter, M. & Dabrock, P. (2021). Data Sovereignty: A Review. Big Data & Society, 8(1), 205395172098201. https://doi.org/10.1177/2053951720982012

Jarke, M., Otto, B., & Ram, S. (2019). Data Sovereignty and Data Space Ecosystems. Business & Information Systems Engineering, 61(5), 549–550. https://doi.org/10.1007/s12599-019-00614-2

Jung, C., & Dörr, J. (2022). Data Usage Control. In Springer eBooks (pp. 129–146). https://doi.org/10.1007/978-3-030-93975-5_8

Krippendorff, K. (2019). Content analysis. SAGE Publications, Inc., https://doi.org/10.4135/9781071878781

Lauf, F., Scheider, S., Bartsch, J., Herrmann, P., Radic, M., Rebbert, M., Nemat, A. T., Schlueter Langdon, C., Konrad, R., Sunyaev, A., & Meister, S. (2022). Linking Data Sovereignty and Data Economy: Arising Areas of Tension. In Wirtschaftsinformatik. Proceedings. 19. https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/19 (accessed 02/23)

Lusch, R. F., & Vargo, S. L. (2014). The Service-Dominant Logic of Marketing. In Routledge eBooks. https://doi.org/10.4324/9781315699035

Mayring, P. (2014). Qualitative Content Analysis: Theoretical Background and Procedures. In Advances in mathematics education (pp. 365–380). Springer Nature. https://doi.org/10.1007/978-94-017-9181-6_13

Munoz-Arcentales, A., López-Pernas, S., García-Pozo, A., Alonso, Á., Salvachúa, J., & Huecas, G. (2020). Data Usage and Access Control in Industrial Data Spaces: Implementation Using FIWARE. Sustainability, 12(9), 3885. https://doi.org/10.3390/su12093885

Myers, M. D. (1997). Qualitative Research in Information Systems. Management Information Systems Quarterly, 21(2), 241. https://doi.org/10.2307/249422

Niebel, C., Reiberg, A., Kraemer, P. (2022). Gaia-X für KMU. Gaia-X Hub Deutschland, URL: https://gaia-x-hub.de/publikationen/ (accessed 02/23)

Opriel, S., Möller, F., Burkhardt, U. E., & Otto, B. (2021). Requirements for Usage Control based Exchange of Sensitive Data in Automotive Supply Chains. https://doi.org/10.24251/hicss.2021.051

Opriel, S., & Schmelting, J. (2022). Datensouveränität. In Springer eBooks (pp. 41–54). https://doi.org/10.1007/978-3-662-63956-6_3

Otto, B. (2016). Digitale Souveränität: Beitrag des Industrial Data Space. Hg. v. Fraunhofer-Gesellschaft. https://www.isst.fraunhofer.de/content/dam/isst-neu/documents/Publikationen/Industrial-Data-Space/Fraunhofer-IDS_Digitale-Souver%C3%A4nit%C3%A4t_Brosch%C3%BCre_DE_2016.pdf (accessed 02/23)

Otto, B. (2019). Interview with Reinhold Achatz on "Data Sovereignty and Data Ecosystems." Business & Information Systems Engineering, 61(5), 635–636. https://doi.org/10.1007/s12599-019-00609-z

Otto, B., Steinbuss, S., Teuscher, A., & Lohmann, S. (2019). IDS Reference Architecture Model. In Zenodo (CERN European Organization for Nuclear Research). European Organization for Nuclear Research. https://doi.org/10.5281/zenodo.5105529

Otto, B., & Jarke, M. (2019). Designing a multi-sided data platform: findings from the International Data Spaces case. Electronic Markets, 29(4), 561–580. https://doi.org/10.1007/s12525-019-00362-x

Otto, B., Mohr, N., Roggendorf, M. & Guggenberger, M. (2020). Data sharing in industrial ecosystems - Driving value across entire production lines.

Pampus, J., Jahnke, B., & Quensel, R. (2022). Evolving Data Space Technologies: Lessons Learned from an IDS Connector Reference Implementation. In Lecture Notes in Computer Science (pp. 366–381). Springer Science+Business Media. https://doi.org/10.1007/978-3-031-19762-8_27

Park, J., & Sandhu, R. (2002). Towards usage control models: beyond traditional access control. https://doi.org/10.1145/507711.507722

Parkins, D. (2017). Regulating the internet giants: the world's most valuable resource is no longer oil, but data. In The Economist 413(9039):7. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (accessed 02/23)

Peterson, Z. N. J., Gondree, M., & Beverly, R. (2011). A position paper on data sovereignty: the importance of geolocating data in the cloud. In IEEE International Conference on Cloud Computing Technology and Science (p. 9). https://doi.org/10.5555/2170444.2170453

Pettenpohl, H., Spiekermann, M., & Both, J. C. (2022). International Data Spaces in a Nutshell. In Springer eBooks (pp. 29–40). https://doi.org/10.1007/978-3-030-93975-5_3

Polatin-Reuben, D., & Wright, J. (2014). An Internet with {BRICS} Characteristics: Data Sovereignty and the Balkanisation of the Internet. In Foundations of Computational Intelligence. https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf (accessed 02/23)

Schmidt, K., Garrido, G. M., Mühle, A., & Meinel, C. (2022). Mitigating Sovereign Data Exchange Challenges: A Mapping to Apply Privacy- and Authenticity-Enhancing Technologies. In Springer eBooks (pp. 50–65). https://doi.org/10.1007/978-3-031-17926-6_4

Schrauf, S., Geissbauer, R., Schneider, J., & Hermans, M. (2020). Connected and autonomous supply chain ecosystems 2025. PwC. https://www.pwc.de/de/digitale-transformation/connected-and-autonomous-supply-chain-ecosystems-2025-web.pdf (accessed 02/23)

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. Information and Organization, 21(1), 1–16. https://doi.org/10.1016/j.infoandorg.2010.11.001

Usländer, T. (2022). Data Sovereignty – Requirements Analysis of Manufacturing Use Cases. In Zenodo (CERN European Organization for Nuclear Research). European Organization for Nuclear Research. https://doi.org/10.5281/zenodo.6668994

Weber, R. J. (1990). Basic Content Analysis. In SAGE Publications, Inc. eBooks. https://doi.org/10.4135/9781412983488

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: writing a literature review. Management Information Systems Quarterly, 26(2), 3. https://web.njit.edu/~egan/Writing_A_Literature_Review.pdf (accessed 02/23)

Waidner, M., Backes, M., Müller-Quade, J., Bodden, E., Schneider, M., Kreutzer, M. (2013). Entwicklung sicherer Software durch Security by Design. SIT Technical Reports, SIT-TR-2013-01. Hrsg: Waidner, Michael. https://publica.fraunhofer.de/entities/publication/88aba001-1438-4a41-8d7e-f48e00567831/details (accessed 04/23)

Zrenner, J., Möller, F., Jung, C., Eitel, A., & Otto, B. (2019). Usage control architecture options for data sovereignty in business ecosystems. Journal of Enterprise Information Management, 32(3), 477–495. https://doi.org/10.1108/jeim-03-2018-0058