Journal of
Theoretical and Applied Electronic Commerce Research

MDPI

Article

Competitive Advantage and Personal Data Ecosystems: A Typology of Personal Data Control Constellations

Ruben D'Hauwers [1,*] and Laurens Vandercruysse [2]

[1] imec-SMIT, Vrije Universiteit Brussel, 1050 Brussels, Belgium
[2] Department of Applied Economics, Vrije Universiteit Brussel, 1050 Brussels, Belgium; laurens.vandercruysse@vub.be
* Correspondence: ruben.dhauwers@vub.be

Abstract: This research investigates data providers' willingness to grant data access control to data subjects in user-centric Personal Data Ecosystems (PDEs), where individuals control their data disclosure. PDEs introduce unique challenges, as data subjects may share competitive data with rival companies, which is not addressed by existing frameworks on data sharing between businesses grounded in resource-based theory (RBT). Through 25 interviews with private sector actors in the Flemish Social Linked Data (Solid) ecosystem triangulated with 56 papers from the existing literature, a typology of strategies for data access control was developed. This typology is based on two key dimensions, data competitiveness and actor relationships, creating four strategic scenarios that guide whether data providers are likely to grant data access control. The findings offer a framework for PDE governance, helping stakeholders to develop strategies enabling data availability and ensure the long-term sustainability of PDEs.

Keywords: competitive advantage; data access control; data provider; data subject; personal data ecosystem; resource-based view; typology

Academic Editors: Mirjana Pejić Bach and Jorge Bernardino

Received: 25 September 2024
Revised: 5 December 2024
Accepted: 23 December 2024
Published: 9 January 2025

Citation: D'Hauwers, R.; Vandercruysse, L. Competitive Advantage and Personal Data Ecosystems: A Typology of Personal Data Control Constellations. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 8. https://doi.org/10.3390/jtaer20010008

1. Introduction

Data ecosystems are networks that facilitate the processing and sharing of data [1], creating opportunities for companies to innovate with new business models and new services [2,3]. However, concerns over the unethical exploitation of personal data have raised issues around autonomy and control for data subjects [4,5]. In response, different authors advocate for user-centric Personal Data Ecosystems (PDEs), which empower individuals to control their data disclosure and data usage [5,6]. PDEs achieve this through a data access control mechanism, allowing data providers and data subjects to define how their data are used by other actors [7,8]. A key factor in the sustainability of PDEs is the willingness of data providers to grant data access control to data while protecting their competitive advantage.

From a strategic point of view, data are a valuable resource that contributes to a data provider's differentiation and competitive advantage [9]. According to the resource-based theory (RBT) [10], data providers are motivated to protect resources that support their competitive advantage. In practice, data providers often hesitate to share data freely, fearing that doing so may weaken their competitive position [11,12]. While existing frameworks explore how business can share data without compromising competitiveness [11–14], they fail to address the specific challenges of PDEs, where data subjects might share competitive data with a data provider's rival [15].

This work therefore aims to add to these existing frameworks by formulating strategies for data providers granting data access control while maintaining their competitive advantage in the specific context of PDEs. Thus, the three research questions for this work are as follows:

- (RQ1) Which dimensions grounded in RBT determine data providers' willingness to grant data access control to data subjects while preserving their competitive advantage in PDEs?
- (RQ2) What strategies can data providers use to grant access control without losing their competitive edge?
- (RQ3) How can the RBT be applied to the relationship between data providers and data subjects in the context of PDEs?

This research will enable the comparison of different types of data access control scenarios which might aid practitioners and academics to develop strategies and/or theoretical assumptions concerning the granting of data access control to data subjects by data providers.

To answer these questions, we employ a mixed-methods approach. First, we conducted 25 semi-structured interviews with private sector actors in the Flemish Social Linked Data (Solid) ecosystem—a novel, user-centric PDE where data subjects control their personal data via technical means [16,17]. Solid was chosen due to its data access control standards via personal data pods, providing a strong context for exploring generalizable insights on PDEs. The Flemish Solid community was selected for its vibrant ecosystem, offering insights into how companies adopting data access control perceive its drivers and barriers. The interview insights were triangulated with 56 academic papers identified in the existing literature to develop a typology of personal data access control strategies. The typology was refined and validated for real-life applicability using an "ideal-type" methodology applied to 33 exploratory Solid use cases.

The typology developed in this research includes four distinct data access control strategies: Involuntary Shared Data Control, Exclusive Data Provider Data Control, Fully Shared Data Control, and Strategically Shared Data control. Data providers are less willing to share if data hold a competitive advantage or if the relationship with the intended data consumer is negative. This aligns with safeguarding a firm's competitive advantage. By introducing different strategic scenarios, we provide data providers and ecosystem orchestrators with insights on how to develop strategies related to granting data access control.

The rest of this article is structured as follows: Section 2 reviews the relevant literature, Section 3 outlines the methodology, Section 4 presents the research results, Section 5 discusses theoretical and practical implications, Section 6 discusses limitations and areas for further research, and Section 7 concludes this paper.

2. Literature Review

2.1. (Personal) Data Ecosystems and Data Sovereignty

Big tech companies currently dominate and control the personal data economy, sidelining smaller actors affecting individuals and organizations [5,6]. This power dynamic, termed data colonialism [18] or surveillance capitalism [19], involves exploiting personal data for profit and impacts less powerful actors by diminishing their autonomy and control over their data. Since individuals are integral in exchanging personal data [20,21], different authors advocate the need for individuals to have control over their personal data usage in user-centric PDEs. PDEs are based on personal data and incorporate a governance model that empowers individuals to control their data disclosure, allowing them to potentially receive value in return [6,22]. The most noteworthy stakeholders in the PDE include data

providers, data consumers, and data subjects. Data providers make data they control available, and data consumers receive these data [23]. A data subject refers to the individual to whom the personal data relates [7]. This research distinguishes between private data providers and data subjects seeking control over personal data. Solid builds further on the concept of PDEs, as it represents a web technology initiative aiming to facilitate the exchange of information within an interoperable online PDE [17].

In the context of PDEs, the concept of data sovereignty becomes crucial, which concerns different agents, ranging from organizations to individuals, that aim to gain power and control over data [24,25]. Data sovereignty can be achieved through data access control (AC), allowing data providers and data subjects to set terms for data usage by other actors [7,8]. This includes determining access and processing purposes, with clarity on data privacy and protection [4].

One could argue the data sovereignty in PDEs could be facilitated through policy making, as legislation like the General Data Protection Regulation (GDPR) establishes "de jure" data sovereignty. It grants the right to data portability, allowing individuals to transfer their data to another organization without hindrance. However, "de facto" data sovereignty is often limited in practice. First, data portability is often constrained by low-quality data integration tools that meet legal requirements but are not user-friendly [26]. Second, while these regulations aim to level the playing field, powerful incumbents can use them to create barriers for rivals, such as increasing costs or limiting interoperability [26,27]. Third, the emphasis on privacy of the legislations can slow the development of user services and data-driven business models [7,21,28]. Thus, to foster sustainable PDEs, a need arises to enable "de facto" data sovereignty for both data subjects and data providers. This research focuses on identifying strategies enabling granting data access control to data subjects while maintaining the competitive advantage of data providers in PDEs.

2.2. (Personal) Data in the Resource-Based and Knowledge-Based Theories

The research field of information science has a history of looking into the development of a competitive advantage by a firm based on the RBT [10] and the derived knowledge-based theory (KBT) of the firm [29]. The RBT takes an internally oriented approach by combining the resources and capabilities controlled by a firm [10,30]. Resources can be both tangible and intangible. The ones that are valuable, rare, inimitable, and non-substitutable eventually lead to a competitive advantage [10]. Thus, according to RBT, the strategy of the firm is focused on building resources and capabilities distinguishing the firm from the changing competition [10,30]. Where RBT treats all resources at the same level, KBT specifically looks into the role of "knowledge" in driving competitive advantage [29,31]. It is even argued that knowledge might be the most important competitive advantage of a firm [32]. (Raw) data can be seen as explicit knowledge that, combined with other resources, leads to a competitive advantage [9].

Previous studies within the realm of the RBT and KBT have shown that big data analysis can be a capability used within firms, driving their performance [9]. In the context of data sharing between companies, other works have shown data can be classified as shareable objects that can enhance a firm's performance [14]. However, as data can be easily shared with partners, this necessitates safeguards to prevent misuse of data [33], requiring strategies balancing between protecting data resources and data sharing [13]. Extant research has found that data sharing between companies often concerns proprietary and business-critical data [34,35], leading to a fear of damaging their competitive advantage by revealing commercial, confidential data [36,37]. Notably, companies may be unwilling to share data for fear of losing control over the resource [38].

The existing research mentioned above primarily looked in applying the RBT and KBT data sharing between companies but did not consider the context of granting data access control of personal data. However, granting data access control to data subjects present unique strategic challenges when it comes to safeguarding a data provider's competitive data [15]. For instance, a data subject may wish to share data that a data provider considers competitive with one of the provider's rivals. Nonetheless, data providers may benefit from enabling data access control, as it increases the willingness to share data with companies [39,40] and creates value for the data subject [41]. Data providers must therefore balance between granting data subjects' data access control and simultaneously preserving the competitive edge of the firm in line with the RBT.

2.3. Data Ecosystems: Existing Models in the Context of Data Sharing Between Companies

To simplify the complexity of (personal) data ecosystems, various typologies and taxonomies have emerged. They touch base with the RBT in the context of data sharing between companies. As none of the classifications below have zoomed in on the context of PDEs, we assess existing frameworks through the lens of safeguarding the competitive edge in line with the RBT. These studies can be divided into two main categories: studies centered around data competitiveness and studies focused on actor relationships.

First, regarding the level of data competitiveness, three frameworks were identified which include data sharing between companies. Two typologies have been developed in the context of data sharing between companies, keeping the RBT in mind. Loebecke's framework [13] focuses on knowledge-sharing configurations for managing the paradox of protecting or sharing knowledge. It is based on the following factors: knowledge types (tacit and explicit knowledge) and the mode of knowledge sharing (unilateral and bilateral) [13]. Kugler and Plank's data-sharing strategy framework views data from an RBT perspective. It acknowledges that data processing can create a competitive edge, and that needs to be considered when deciding to share data [12]. It focuses on steps in the data analysis process and the use of big data to identify whether data need to be protected or shared. However, it primarily examines data analytics steps and lacks insights into actor dimensions and personal data. In Enders et al., a structured review identifies factors influencing data sharing, emphasizing concepts like data coreness [11]. Core data are close to the core of the business and may thus reveal critical business information. The work of Enders did not incorporate the RBT as a theoretical basis.

Second, other frameworks position actor relationships as the key factor for data openness. These works do not take the perspective of the RBT. The choice of data-sharing partners significantly influences the protection of competitive advantages [3,42]. Some actor relationship frameworks explore supply chain data sharing [34,35,43], which includes environmental, intraorganizational, and interorganizational factors. Interorganizational factors relate to partner relationships, trust, shared vision, commitment, and connectivity [34,43]. Essentially, data providers aim to prevent sensitive business information from reaching competitors, necessitating knowledge protection in competitive networks [44]. In data and knowledge sharing, coopetition arises, involving simultaneous collaboration and competition between firms [45–47], influencing the extent of knowledge sharing between firms [48].

This research aims to contribute through a typology that integrates insights from data-sharing frameworks between companies in the context of granting data access control to data subjects in PDEs incorporating the RBT.

3. Methodology

The overview of the used methodology can be found in Figure 1, which uses a systematic research process [49].

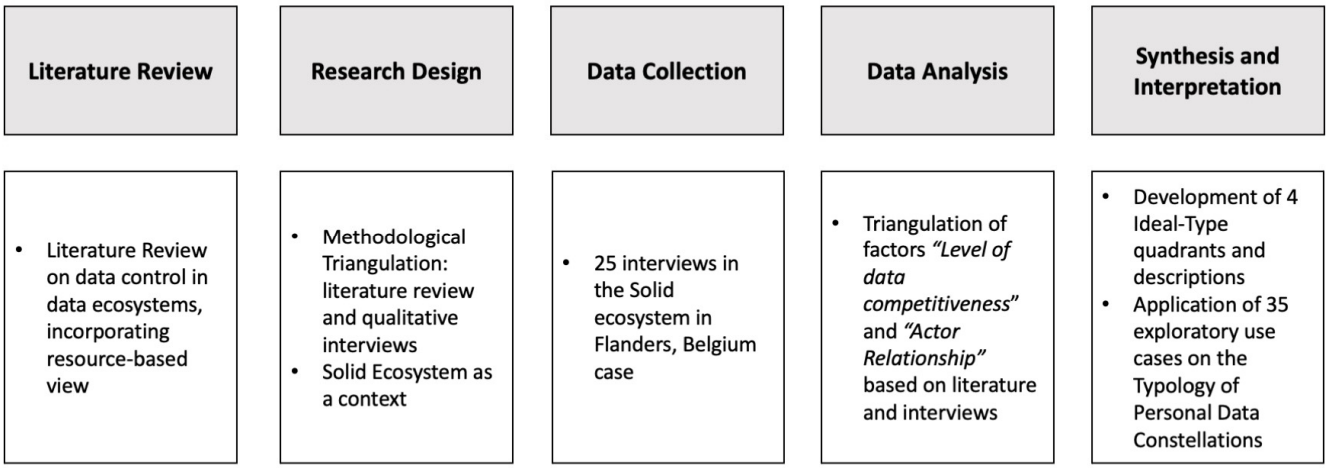

Figure 1. Methodology.

Literature review: An extensive review of the existing literature on integrating data control within data ecosystems was conducted, focusing on the application of the resource-based view in this context. The literature review is a research method designed to synthesize existing scientific knowledge on a specific topic, analyzing past research to identify trends, gaps, and foundational theories. This method contributes by establishing the theoretical context and rationale in academic inquiries [50,51]. This involved searching scholarly databases to gather a comprehensive understanding of the current state of knowledge, identify gaps, and inform the research questions and objectives. During the synthesis and interpretation stage (see below), the literature review served as the foundation for triangulating the results. The literature review was performed in Web of Science to obtain an overview of mapped factors that could influence data providers' openness to share data. Notable keywords included the following: "data access control", "data strategy", "data ecosystem", "data sharing", "open and closed ecosystem", and "data typology". In the first stage, pertinent papers were identified based on title and abstract selection. After in-depth reading, the most relevant papers were selected for the triangulation within the analysis phase.

Research design: Based on the insights gained from the literature review, the research design was formulated. This included defining the scope and objectives of this study, and determining the methodology. The research design aimed to ensure that this study addressed the research questions effectively and followed a systematic approach to data collection and analysis. This article employs a qualitative approach based on a three-step methodology: (i) semi-structured expert interviews, (ii) triangulation of interview insights with the literature, and (iii) ideal-type typology development.

(i) Semi-structured interviews within the context of the Solid ecosystem in Flanders were performed (see data collection). To ensure practical relevance, interviews were performed to align with the current state of the art in business practices related to granting data access control within the Solid ecosystem. The semi-structured interview method allows researchers to balance guided questions with the flexibility to explore respondents' perspectives in depth, blending structure with adaptability [52]. The Solid personal data ecosystem, which allows for data subject personal data control, is used as the context for the research. This has the advantage of generalizability as it offers standardization and interoperability through a W3C standards-based proto-

col [16,53]. The authors provided an explanation of general principles of data access control that extends beyond Solid, facilitating the generalizability of the findings to other technologies. The Solid ecosystem in Flanders is particularly interesting due to its active development, substantial policy stimulation, and private sector interest [54]. The Flemish government prioritizes Solid PDEs as a policy and innovation driver, and the establishment of a "data utility company" is evidence of this commitment [54]. This initiative is fostering an open ecosystem, promoting data exchange among data providers and data consumers while embedding personal data access control for data subjects [53]. Taking into account the inherent limited generalizability that springs from the case study approach, the selection of this ecosystem should offer insights that are generalizable beyond the case at hand by illustrating the emergence of data access control principles adoption.

(ii) The researchers employed methodological triangulation [55,56], combining semi-structured interviews with insights on the level of data competitiveness and actor relationships in data ecosystems from the extant academic literature. Methodological triangulation combines multiple research methods to strengthen the reliability and depth of findings, enhancing this study's validity by reducing potential biases that could arise from a single method [55]. Triangulation enhances credibility, validity, and depth of findings [56]. The logic of triangulation is based on the premise that no single method ever adequately solves the problem of rival explanations. Because each method reveals different aspects of empirical reality, multiple methods of data collection and analysis provide credibility in the results. Convergent triangulation has been applied [57], as the aim of the research is to develop and test a typology.

(iii) The theory was tested by validating the identified dimensions with the literature on data sharing grounded in the RBT. In the final step, the typology was validated using interview-based use cases. Case studies assessed whether the identified quadrants align with current business practices in granting data access control.

Data collection: To explore drivers and barriers for data providers to grant data subjects personal data access control, stakeholder interviews in an issue-focused stakeholder management approach [58] were performed. We employed a snowballing method to select interview subjects based on their interest in participating in the Flemish Solid personal data ecosystem [59]. To minimize selection bias, interviewees were chosen based on experience level (C- level or content expert), whether they performed activities in the Solid personal data ecosystem and/or were planning to do so. Potential candidates were identified based on industry experts' referrals and activity in the Solid community (https://solidcommunity.be/ (accessed on 6 January 2025)). To counter potential biases associated with snowball sampling, we triangulated interview data with the outcomes of the literature review [55]. This triangulation allowed us to validate interview findings and minimize the influence of individual biases, thereby enhancing the study's reliability. Observations were cross-checked against established theories and findings from prior studies regarding data sharing between businesses within the context of the RBT to ensure consistency and mitigate the effects of subjective framing by individual participants. The interviewees' roles in their companies and the Solid ecosystem can be found in Appendix A. The semi-structured interview method [52] was used, well suited for the exploratory nature of this research [60]. This method offers flexibility with open-ended questions and allows for follow-up queries. Guidelines provided by Myers and Newman ensured interview validity, including the use of a topic guide featuring open questions regarding drivers and barriers in data sharing within a Solid ecosystem [61]. Interviews were conducted with a standardized set of open-ended questions to reduce the influence of leading questions

and ensure that each participant's perspective was captured authentically. Interviews were conducted in Dutch or English, and Dutch quotes were translated by the researchers. We produced verbatim transcriptions, ensuring pseudonymization of the interview transcripts to establish trust. All interviews were conducted via Microsoft Teams and ranged from 1 h to 1 h 45 min in duration.

Data analysis: Following Corbin and Strauss's methodology [62], the data analysis involved a mixed approach that integrated both inductive and deductive reasoning, utilizing open coding, where initial interviews were examined to extract preliminary concepts. Subsequently, axial coding was applied to establish relationships among these codes and to categorize them systematically. Finally, selective coding was conducted to refine the categories further and iteratively identify key dimensions. This iterative process allowed for a deepened understanding of the relationships. These dimensions were then triangulated with findings from the literature, supported by a thematic analysis of the 56 identified papers in the literature review. Based on the coding, two dimensions, "the level of data competitiveness" and "actor relationships", in data ecosystems were identified. Underlying factors were "coreness" and "level of processing", and the "level of competition" and "level of collaboration", respectively. Table 1 shows examples of how the interviews were coded based on the dimensions and factors. This enabled the researchers to identify the dimensions "level of data competitiveness" and "actor relationship" both in the literature and in the interviews. This analysis was iterated to find commonalities between data providers' perspectives and literature insights until the end. The coding tree in Appendix B shows the triangulation results between the literature and the interviews.

Table 1. Examples of axial coding of the interviews.

Interview Quote	Dimension	Factor
Competitive data, like an assessment, we made, we will not share with anyone, especially not with our competitors. [Interview 3, personal communication, 16 June 2022.]	Level of data competitiveness	Level of processing
Competitive data, like an assessment, we will not share with anyone, especially not with our competitors. [Interview 3, personal communication, 16 June 2022.]	Actor relationship	Level of competition
When companies engage in a collaboration, it's an agreement to do something together which leads to a joint benefit. Thus, not only buying and selling data. In a data collaboration, there is an engagement of a data provider and data [consumer] with a benefit for both. [Interview 25, personal communication, 7 September 2022.]	Actor relationship	Level of collaboration
Some data, like address, name. . . would be possible to share as it would be useful. For other data sources, we invest a lot of money to process the data. Those data we will not share. [Interview 4, personal communication, 28 October 2021.]	Level of data competitiveness	Level of processing

The underlined sections highlight the part of the quote that has been used for axial coding of the dimension and factor.

Synthesis and interpretation: To synthesize and interpret the results over different iterations, we used triangulation to create the initial typology of personal data control constellations. A typology organizes objects into categories based on similarities and differences [63]. Ideal-type analysis [64] systematically compared cases to form ideal types that illustrate behaviors based on patterns [65]. We created four ideal-type constructs based on the level of data competitiveness and actor relationship dimensions. Ideal-type descriptions were developed via analysis of interviews. Validity and objectivity of the typology development was achieved through a code–recode strategy, where the data were initially coded, set aside, and then recoded to check for consistency. After the last iteration, all objective and subjective ending conditions proposed by Nickerson were fulfilled [66]. Specifically, we thoroughly examined all papers from the literature review and all interviews. In this final iteration, no dimensions were merged or split; each characteristic within each dimension was successfully classified, and no new dimensions or characteristics were introduced. Furthermore, dimensions remained unique and unduplicated, ensuring clarity and precision in the model. Each combination of characteristics was distinct, avoiding redundancy. The model was designed to be concise, containing only essential dimensions and characteristics necessary to differentiate every object effectively. It was also comprehensive, allowing for the classification of all objects while providing valuable, non-redundant information relevant to characterizing PDEs. Additionally, the research process was subjected to external scrutiny, with another researcher reviewing the methodology and engaging in discussions throughout this study to maintain consistency and reliability. To enhance credibility, we utilized both literature reviews and interviews as data sources. For transferability, we ensured a diverse selection of interview participants from various sectors and roles within the Solid ecosystem in Flanders, thereby enhancing the applicability of our findings across the ecosystem. Confirmability was achieved by maintaining detailed records of interview notes and the literature review process, which facilitated transparency and reproducibility.

Finally, to ensure applicability to real-world settings, the typology was validated as the two researchers independently applied the typology to 33 exemplary Solid use cases mentioned during interviews. This way, the applicability of the typology was validated and iterated in further steps. Throughout the mapping, different inconsistencies were identified in the typology and in the way the researchers mapped the dimensions, leading to three further iterations of the typology. This mapping ensures that the typology is applicable to real-life use cases, ensuring that obstacles, challenges, and unintended outcomes related to the usage of the typology were identified in the final version of the typology.

4. Results

Our theoretical framework was established originating from the RBT, which is based on the principle that private data providers primarily aim to regulate what data are available for sharing and the specific actors with which they can be shared to protect their companies' resources in the context of PDEs. Consequently, our framework comprises two key dimensions: (1) the level of data competitiveness and (2) the actor relationship. The insights gained from our semi-structured interviews triangulated with insights from the literature allowed us to further refine our understanding of these dimensions and identify the underlying factors necessary for constructing a typology. You can find an overview of the dimensions and factors in Figure 2.

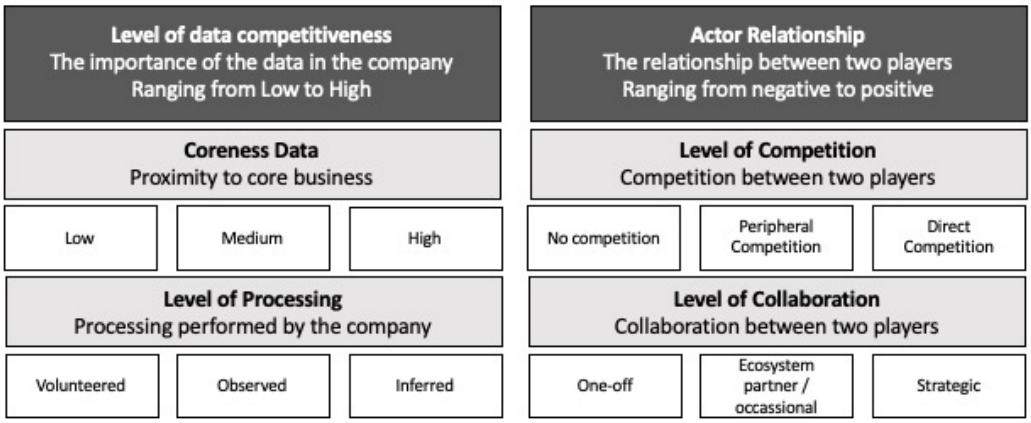

Figure 2. Overview of dimensions and factors.

4.1. Level of Data Competitiveness of Personal Data

The first dimension, the level of data competitiveness, determines which data are considered either shareable or non-shareable. If considered of high data competitiveness, they will be protected [44]. Data providers will not be inclined to grant data access control to data that are business-sensitive, or the data access control will be conditional [3,42,67]. We triangulated that the level of data competitiveness depends on the coreness of the data, i.e., proximity of the data to the core business [11], and the level of processing [12].

4.1.1. Coreness

The first factor determining the level of data competitiveness is the proximity of the data to core business operations, the "coreness" [11]. This concerns data that underpin competitive advantage and therefore must be protected [42]. One of the interviewees mentioned this explicitly: "If it's competitive data a company builds its business on, I question whether private companies will [enable data subject data access control]" [Interview 18, personal communication, 27 July 2022].

Interviewed actors consider some data as their "competitive data" and consider these as what differentiates them, as mentioned by this private actor: "Companies could enable sharing data that is not company critical. Company critical data will not be shared" [Interview 7, personal communication, 30 June 2022]. Data coreness ranges from low (e.g., medical data for a bank) to high (e.g., credit score for a bank).

4.1.2. Level of Processing

The level of data competitiveness also hinges on the extent of processing conducted by private data providers [12]. Data that are transformed into valuable information have a higher competitive advantage for companies [68]. In the context of personal data, processing levels can be categorized into volunteered or provided data (explicitly shared by individuals, e.g., on social network profiles), observed data (captured actions, like browser history or location data), and derived and inferred data (obtained through analysis of volunteered or observed data) [69,70].

Our interviews revealed that increased data processing leads data providers to regard it as their "intellectual property" (IP). For instance, one interviewee emphasized this point, stating, "It depends on where the IP of the data is. As a user, you can offer an ingredient of a cake, but our company makes the cake. So, the IP of the cake would be with our business, while the raw data will belong to the user" [Interview 23, personal communication, 10 August 2022]. Furthermore, private data providers might classify processed data as "company data". Another interviewee noted, "Derived data is complicated. Is a risk score of the user's personal data or bank data? A bank would say it is their company data"

[Interview 21, personal communication, 4 August 2022]. Companies also factor in the extent of their financial investment in the processing of the data when deciding to share them. As one interviewee mentioned, "Some data, like address, name. . . would be possible to share as it would be useful. For other data sources, we invest a lot of money. Those data we will not share" [Interview 4, personal communication, 28 October 2021].

4.2. Actor Relationship

The second dimension, actor relationship, identifies how two private actors relate to each other. Data providers want to be able to decide with which data consumer the data will be shared when data access control is granted to the data subject. The actor relationship is based on the level of collaboration and the level of competition between the data provider and data consumer, referred to as the level of coopetition [45,47,48,71]. The factor can be positive or negative. A positive relationship is associated with a higher willingness to grant data access control.

4.2.1. Level of Collaboration

If actors are collaborating and have a low level of competition, they will be willing to share data. The factor level of collaboration is the extent to which the private actors have partnerships with each other [44,71]. The fact that data providers could set up strategic alliances with other private actors to improve their position in the market was brought up by an interviewee: "We could set up strategic alliances to go to market together, and become stronger that way" [Interview 15, personal communication, 15 October 2021]. Additionally, even without strategic alliances, agreements improve the willingness grant data access control on a one-on-one basis, quoted by a respondent: "We can make agreements with other companies to share the data one one-on-one" [Interview 6, personal communication, 4 November 2021]. For this, a respondent mentioned that a common objective between the companies is required [Interview 25, personal communication, 7 September 2022]. The level of collaboration ranges from strategic alliances to being ecosystem partners to no agreements.

4.2.2. Level of Competition

The factor of the level of competition is the extent to which the players are competitive toward one another [71]. Sharing data with data consumers results in a competitive risk, as one interviewee noted: "Sharing with other companies is difficult, especially with our competitors. The risk may be too high" [Interview 4, personal communication, 28 October 2021]. Thus, when granting data access control, data providers will want to control with whom the data will be shared by the data subject, as clarified by this respondent: "We will want to be able to control who gets access to the data. If it is another sector, we would be willing to share. If it is a competitor, we will not do that. We would strengthen their offering" [Interview 5, personal communication, 28 June 2022]. The level of competition ranges from no competition to peripheral competition to direct competitors.

4.3. Typology of Personal Data Control Constellations

A typology of personal data access control constellations is created based on identified dimensions and factors based on the RBT. This typology guides data providers in formulating strategies for granting data access control to data subjects. It leverages the level of data competitiveness and actor relationships to determine the data's level of openness. The level of data competitiveness is assessed using coreness and data processing level, where higher data competitiveness corresponds to a lower willingness to grant data access control. Actor relationships depend on cooperation and competition, with positive relationships leading to a greater willingness to grant data access control. This typology results in four

quadrants, as depicted in Figure 3. Additional details on the dimensions and underlying factors related to the level of data competitiveness and actor relationships can be consulted in Figure 2. The typology facilitates comparison across four quadrants by offering a unified framework and terminology for discussing the granting of data access control by the data provider to data subjects. Table 2 showcases the definition, characteristics, and core strategic considerations to opt for a certain quadrant and the potential tactics to implement the concerned quadrant's data access control constellation.

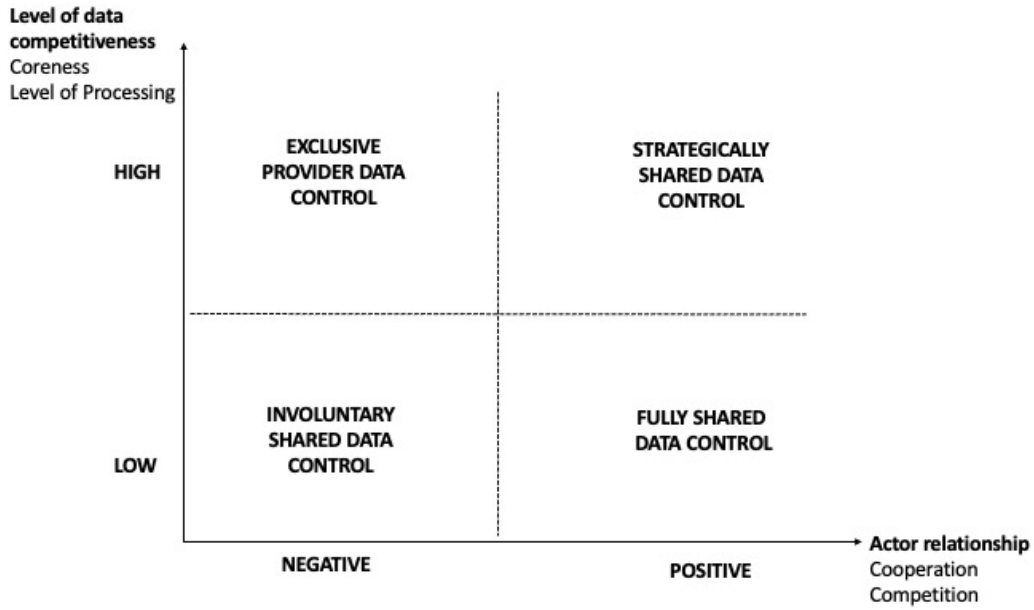

Figure 3. Typology of personal data access control constellations.

In the first quadrant, "Involuntary Shared Data Control", data providers are obliged to grant data access control to data subjects due to legal obligations or ethical considerations. This case occurs when there is a negative relationship between data providers and data consumers, possibly due to competition or a lack of collaboration. In this scenario, data providers are not openly willing to share but might give data subject data access control involuntarily since the level of data competitiveness of the concerned personal data is low. Typically, companies hesitate to share data with competitors, even if the data are not vital to their business. One interviewee noted, "Sharing data between companies is difficult, especially if they are competitors". [Interview 24, personal communication, 10 August 2022]. In this quadrant, granting data subject data access control is undesired as it could potentially strengthen competitors, particularly if this is disadvantageous for their business [among others, Interview 19, personal communication, 2 August 2022]. Some data providers fear that enabling data subject control could mitigate customers lock-in, impacting their market position [Interview 14, personal communication, 28 October 2021]. However, they might be required or obliged to grant data subject data control for this type of personal data due to legal reasons [Interview 2, personal communication, 15 June 2022]. Granting data subjects personal data access control may also be seen as an additional service to the data subject [Interview 10, personal communication, 6 July 2022]. Some companies are willing to share these data because they belong to the data subject: "Data on e.g., age, pathology. . . of a patient is not so important for us. The user can decide what he or she is doing with it if it does not damage our competitive position in the market" [Interview 22, personal communication, 8/8/2022]. They want to ensure ethical and legal usage of the data [Interview 17, personal communication, 27 July 2022]. Involuntary shared data control occurred in four of the analyzed cases. An example of involuntary shared data control concerns a bank that may share family information with a competing insurance company

upon a data subject's request due to legal obligations, as required by the Payment Services Directive 2 [Interview 2, personal communication, 15 June 2022]. Additionally, another example could be a bank opening data integration tools on bank account information to a service provider which helps freelancers with their VAT declaration. Even though banks are obliged to open data through data integration tools if the data subject desires to do so, the bank could decide in this case to open better-quality data integration tools with partners while only granting access to low-level data integration tools to non-partnering companies [Interview 2, personal communication, 15 June 2022]. Strategic considerations for this quadrant include legal compliance and ethical/customer-centric concerns. Tactics to operationalize this strategy include granting data access control over non-competitive data and potentially developing technical barriers in the form of, e.g., low-level data integration tools. The business model in the "Involuntary Shared Data Control" quadrant leverages compliance and ethical data-sharing practices by prioritizing transparency and secure data control. By allowing controlled access to non-competitive data, they can comply with regulations and ethical considerations.

In the second quadrant, "Exclusive Provider Data Control", data providers do not grant data access control to data subjects as they aim to protect critical data from competitors. This quadrant involves a negative relationship between data providers and data consumers in the PDE. In this case, the data are crucial for the data provider, and they are reluctant to grant data subject data access control to prevent indirectly sharing highly important and processed data with competitors, especially those with whom they lack a close relationship. For example, one interviewee explained, "We have different types of data, raw data of the user we can share. But we also have derived data, and data which we gather. We do not want to share this data with others, especially not our competitors" [Interview 23, personal communication, 10 August 2022]. While legal obligations may force data providers to share such data, they might be hesitant because sharing strategically important data could inadvertently strengthen their competitors. In a use case, consider a scenario where a data subject requests a recruiter to share a personal assessment with a competing recruiter. Given the importance of these data to the recruiter, they would be unwilling to share them, fearing a loss of control over competitive data and an inadvertent strengthening of the competition [Interview 5, personal communication, 28 June 2022]. Sharing highly processed data also poses concerns that competitors may derive algorithms or methodologies from the analyzed data. Exclusive Provider Data Control occurred in three cases. For example, a health startup that has developed an algorithm to measure patient movement imbalances may face this situation. Sharing these personal patient outcomes with a competitor could potentially enable the competitor to replicate the algorithm, thereby undermining the startup's competitive advantage [Interview 22, personal communication, 8 August 2022]. Another example would be the sharing of assessment data by a recruiter with another recruiter through a Solid pod. As these are competitive data, the recruiter will not be inclined to share these data as they could be used to match the candidate with a customer [Interview 10, personal communication, 6 June 2022]. These examples showcase that the strategic considerations are sensitive data protection and maintaining competitive advantage. Tactics include strictly formally, rather than substantively, complying with legal data-sharing obligations and developing technical barriers. The "Exclusive Provider Data Control" model offers limited new business potential but allows companies to strategically safeguard proprietary data. By emphasizing advanced security and confidentiality, companies in this quadrant can reduce competitive risks.

Table 2. Comparative framework for data access control strategies.

	Exclusive Provider Data Control	**Involuntary Shared Data Control**	**Strategically Shared Data Control**	**Fully Shared Data Control**
Definition	Data providers do not grant data access control to data subjects as they aim to protect critical data from competitors.	Data providers are obliged to grant data access control to data subjects due to legal obligations.	Data providers grant data access control to data subjects in strategic collaborations with partners.	Data providers fully grant data access control to data subjects.
Characteristics	High data competitiveness. Negative actor relationship.	Low data competitiveness. Negative actor relationship.	High data competitiveness. Positive actor relationship.	Low data competitiveness. Positive actor relationship.
Data access control	Data provider.	Data subject (enforced).	Data subject and data provider.	Data subject (enabled).
Core strategic and business model considerations	Sensitive data protection. Protect competitive advantage of the data provider. Limited potential for value-capturing. Focus on data security and confidentiality.	Legal compliance. Customer-centric considerations. Value-capturing by trust creation, customer relationship, and legal compliance.	Data monetization. Strategic collaboration and joint go-to-market. Value-capturing through joint partnerships and data monetization.	Consumer trust and customer centricity. Improve user experience. Value-capturing through new revenue streams and customer centricity.
Tactics	Avoid legal obligations. Develop technical barriers.	Grant data access control to non-competitive data. Develop technical barriers.	Grant data access control in strategic partnerships.	Fully grant data access control. Optimize user experience.
Amount of cases in quadrant	3 cases.	4 cases.	18 cases.	8 cases.
Case example	A health startup with an algorithm for measuring patient movement imbalances risks losing its competitive edge if it shares patient outcomes with a competitor, as these data could allow the competitor to replicate the algorithm [Interview 22, personal communication, 8 August 2022].	A bank is legally required by the Payment Services Directive 2 to share family information with a competing insurance company if requested by the data subject [Interview 2, personal communication, 15 June 2022].	A recruiter sharing personal assessments with a partnering hiring company, all resulting in mutual benefits [Interview 3, personal communication 16 June 2022].	An employer shares an employee's employment history data with a partner HR firm responsible for managing the employee's payments [Interview 8, personal communication, 14 October 2021].

In the third quadrant, labeled "Fully Shared Data Control", data providers fully grant data access control to data subjects. This scenario is characterized by a positive relationship between the data provider and data consumer, with the data not being competitively significant to the data provider. As a result, personal data access control is readily granted to the data subject, enabling sharing with players with whom the data provider has a positive relationship. For

instance, one respondent expressed, "We will be happy to share the physical address of the user. If user experience can be improved, let's do it" [Interview 23, personal communication, 10 August 2022]. Additionally, increasing customer trust is a significant driver in this quadrant [Interview 21, personal communication, 4 August 2022]. The drivers for sharing data access control in this quadrant include the potential for monetization [Interview 2, personal communication, 15 June 2022] and the desire to offer improved services to the user [Interview 8, personal communication, 14 October 2022]. However, it is important to note that the costs associated with sharing data can sometimes outweigh the benefits, leading data providers to refrain from investing in data preparation and robust data integration tools. For instance, one respondent mentioned administrative complexities, stating, "It would be a lot of administration to enable all the sharing of the data; we would need to be compensated for the costs" (Interview 8, personal communication, 14 October 2021]. In cases where financial reimbursement is not feasible, government incentives for data sharing can act as a driver [Interview 9, personal communication, 10 November 2021]. Fully Shared Data Control occurred in eight cases. An example of "Fully Shared Data Control" is a scenario in which an employer shares the employment history data of their employee with a human resource partner responsible for managing employee payments [Interview 8, personal communication, 14 October 2021]. Another example could be an electricity grid provider sharing energy consumption data with a home appliance provider using data integration tools [Interview 14, personal communication, 28 October 2021]. This approach aims to increase consumer trust and customer centricity while improving user experience. Tactics include fully granting data control and optimizing the user experience. The "Fully Shared Data Control" model enables data providers to emphasize customer-centric approaches through greater transparency and enhanced user experience. By partnering with ecosystem collaborators, companies can deliver integrated solutions that add customer value and generate new revenue streams.

In the fourth quadrant, referred to as "Strategically Shared Data Control", data providers grant data access control to data subjects in strategic collaborations with partners. This quadrant is characterized by a positive relationship between the data provider and the data consumer, involving granting data access control to the data subject over important data. As one interviewee emphasized: "When companies engage in a collaboration, it's an agreement to do something together which leads to a joint benefit. Thus, not only buying and selling data. In a data collaboration, there is an engagement of a data provider and data [consumer] with a benefit for both" [Interview 25, personal communication, 7 September 2022]. In this case, granting data subject data access control is facilitated, subject to certain conditions. Firstly, the data provider typically desires control over what happens with the data, as expressed in Interview 5 [personal communication, 28 June 2022]: "Can we control whether our data will not end up with our competitor? Who will get access to the data? If the data can end up with the competitor, we will not do so". Additionally, the data provider may expect compensation for the data or wish to receive something in return. Furthermore, strategic collaborations between data providers are common in this quadrant. These collaborations aim to strengthen their market positions through joint efforts, as pointed out by an interviewee: "For many companies, the value of data is golden. This offers many insights. Many companies set up strategic collaborations to become stronger together and have a more robust position in the market. An example can be clusters between media and telecom" [Interview 15, personal communication, 15 October 2021]. Granting data subject data access control in this quadrant allows actors to enhance their customer targeting capabilities, and they strive to mutually benefit from such collaborations [Interview 8, personal communication, 14 October 2021]. Strategically Shared Data Control occurred in 18 cases. Examples of this scenario include a doctor granting data control over

diagnostic data to indirectly share data to a partnering hospital [Interview 12, personal communication, 12 June 2022] and a recruiter sharing personality and personal assessments with a partnering hiring company, all resulting in mutual benefits [Interview 3, personal communication, 16/6/2022]. Strategic considerations include data monetization, strategic collaboration, and joint go-to-market efforts. Tactics include granting data access control within strategic partnerships. In the "Strategically Shared Data Control" model, companies focus on creating mutual value through partnerships that leverage shared data to improve insights and customer targeting. Business models may include data monetization, where partners receive compensation or reciprocal benefits, ensuring value for both parties while safeguarding sensitive information. Companies can also strengthen market positioning by developing joint go-to-market strategies that utilize each partner's unique strengths, driving competitive advantage through co-branded or co-developed offerings.

Table 2 concisely summarizes the main points of the outlined typology.

5. Discussion

5.1. Theoretical Implications

The first research question for this work is as follows: (RQ1) Which dimensions grounded in the RBT determine data providers' willingness to grant data access control to data subjects while preserving their competitive advantage in PDEs? This study identifies the level of competitiveness [11,13,35,36,38,44,72–75] and actor relationship [3,34,35,43,45–48] as the primary dimensions, which is in line with the dimensions in data sharing between companies. However, in PDEs, unlike data sharing between companies, the data subject plays a central role. Companies must decide on granting data access control while considering their relationships with other organizations, adding complexity to the process. This necessitates the second research question to help companies manage this added complexity.

The second research question is as follows: (RQ2) Which different strategies enable data providers to grant data access control while maintaining their competitive edge? Our research identifies several strategic options, captured in a typology that extends existing frameworks by focusing specifically on PDEs. This typology introduces two key factors—data competitiveness and actor relationships—as critical in shaping data providers' behavior, offering a new perspective on how data control decisions are made in PDEs. While existing frameworks explore how businesses can share data without compromising competitiveness [11–14], they fail to address the unique challenges of PDEs, where data subjects might share competitive data with a data provider's rival [15]. Our typology bridges this gap by introducing different strategies: "Exclusive Provider Data Control", "Involuntary Shared Data Control", "Strategically Shared Data Control", and "Fully Shared Data Control".

The novelty of this approach lies in its holistic view of PDEs, which involves not just the data themselves but also the dynamics between actors facilitating its exchange. This integration enables data providers to tailor their strategies, opting for open or closed data ecosystems depending on the strategic context. For instance, in the "Strategically Shared Data Control" quadrant, data providers might choose to share highly competitive personal data within trusted alliances, leveraging legal safeguards. Conversely, in the "Involuntary Shared Data Control" quadrant, if data providers lack a competitive advantage, data subjects may share their data with rivals regardless of the provider's preferences. Our comparative framework (Table 2) further highlights specific strategic considerations based on interview and case study insights. For example, when data are highly competitive and actor relationships are weak, providers may erect barriers to data sharing, as seen in the "Exclusive Data Provider Control" quadrant. In contrast, in strong actor relationships, sharing may occur even with competitive data if it benefits the broader ecosystem.

The third research question is as follows: (RQ3) How can the RBT be applied to the relationship between data providers and data subjects in the context of PDEs? Our findings contribute to the RBT by examining the dynamics of data access control in PDEs. While existing research primarily applies these theories to big data analysis [9] and data sharing between businesses [12–14], our work explores how data providers navigate the tensions between maintaining competitive advantage and granting data access control to data subjects. In the context of PDEs, the ability to control access to data—whether through Exclusive Provider Data Control, Involuntary Shared Data Control, Strategically Shared Data Control, or Fully Shared Data Control—is a key resource for firms. A key distinction between PDEs and data sharing between companies is the reliance of data providers on data subjects' decisions, as illustrated in Table 3 This interdependence marks a significant shift in the RBT, as traditional data sharing between businesses typically involves unilateral control by data providers. As data subjects become active participants in PDEs, the interdependence between data providers and data subjects becomes a valuable dynamic. The concept of "shared data control" within PDEs contributes to the RBT, emphasizing the collaborative nature of the relationship between data providers and data subjects. Companies must therefore balance their competitive advantage with the collaborative nature of the data-sharing process. Additionally, they can draw on strategic alliances with other stakeholders and engage with data subjects to enhance their data resources while ensuring long-term value creation. Companies must evaluate their data access control strategies based on their relationships with competitors and partners, alongside the level of data competitiveness. This approach allows data providers to decide whether to grant data access control.

Table 3. Comparison of RBT on data analysis, data sharing between businesses, and personal data ecosystems.

Resource-Based View on Data in Data Analysis	Resource-Based Theory on Data Sharing Between Businesses	Resource-Based Theory in Personal Data Ecosystems
Big data analysis is a core resource within the company [9]	Data are shareable and aid in developing the firm's performance [14]. Firms need to manage whether to share data or protect data, and they control with whom they share which data [12,13].	Data control is shared between the data provider and the data subject depending on data competitiveness and the relationship between data provider and data consumer, leading to four scenarios: Exclusive Data Provider Control, Involuntary Shared Data Control, Fully Shared Data Control, and Strategically Shared Data Control.

5.2. Practical Implications

This research provides valuable insights for data access control strategies aimed at data providers and serves as a valuable tool for ecosystem orchestrators, as illustrated in Table 4. For data providers, the framework outlines four distinct quadrants, each representing strategic scenarios that guide them in navigating the complexities of PDEs. These scenarios offer actionable guidance on balancing data access control with competitive advantage. Table 4 highlights strategies for each quadrant. Each type involves a different access control strategy, ranging from open access towards restricted control granted. The data providers can decide on different strategies, ranging from data protection, building customer trust, and forming alliances to enhancing customer service.

Table 4. Access control strategy and ecosystem orchestrator strategies.

Quadrant	Access Control Strategy	Data Provider Strategy	Prioritization for Ecosystem Design
Exclusive Provider Data Control	Restricted control	Data protection	Lowest potential, avoid
Involuntary Shared Data Control	Limited access control (only certain types of data)	Customer trust creation and legal compliance	Medium potential, requires (legal) enforcement
Strategically Shared Data Control	Limited access control (only partners)	Trusted alliances and joint go-to-market strategies, data monetization	Potential, requires trustworthy data-sharing mechanisms
Fully Shared Data Control	Open access	Customer services and optimal customer experience	Highest potential, requires use case identification with highest value

For ecosystem orchestrators, the typology functions as a strategic tool for designing sustainable ecosystems. By considering both the nature of the data exchanged and the extent of ecosystem participation, orchestrators can optimize ecosystem configurations. For instance, providing long-term partners with access to less sensitive data is more feasible than sharing critical data with direct competitors. In the most promising cases, this approach requires identifying specific use cases, while in other cases it requires trust-building mechanisms and/or enforcement strategies. Notably, the "Exclusive Provider Data Control" quadrant should initially be avoided. Overall, the typology supports evaluating and comparing data ecosystems, proposing strategies to evolve toward sharing more complex data with a broader range of actors. This approach helps set maturity trajectories for data ecosystems, progressing from simpler setups to more intricate configurations.

Data control strategies involve a range of legal and technical measures to manage data access effectively. In the Exclusive Provider Data Control scenario, the strategy focuses on ensuring the company's data protection by restricting access, such as not opening APIs and maintaining tight control over data sharing. In contrast, the Involuntary Shared Data Control approach includes measures to build customer trust by opening APIs selectively to other companies and providing data subjects with an interface that enables restricted data sharing, as determined by the company. This strategy is primarily aimed at ensuring legal compliance. For Strategically Shared Data Control, APIs are shared only with partners involved in a joint go-to-market strategy. To maintain control, companies develop trustworthy data-sharing mechanisms and design contracts that define specific conditions under which data can be shared. Interfaces allow data subjects to share data only with preferred partners, adding an additional layer of control. Lastly, in the Fully Shared Data Control model, a completely open ecosystem is established, where interoperability is enabled across all ecosystem participants who adhere to shared standards. In this scenario, the interface for data subjects facilitates seamless data sharing with all players in the ecosystem.

6. Limitations and Further Research

An initial limitation concerns potential restrictions regarding the generalizability of our findings to other geographies and over time. This is a result of the research's methodology as well as of its exploratory nature within the emerging Solid ecosystem in Flanders. This research aimed to transcend in-depth company-focused single case studies by offering

generalizable insights applicable to data providers aiming to grant data control. However, our focus was geographically constrained to maintain consistency. The theoretical model developed could be applied to other ecosystems with similar characteristics. For instance, ecosystems in regions with high innovation density and with similar legislation as Flanders may exhibit comparable dynamics, while those in economies with a lower innovation potential and different legislation may require adjustments to account for differences in strategic drivers and barriers regarding granting data access control. Additionally, the temporal scope has limitations due to the early development stage of PDEs. However, the framework's conceptual nature allows for adaptable high-level application and is inherently scalable to different contexts in principle. To enhance the framework's generalizability, future research should aim to validate it using real-life use cases in diverse geographical settings and in PDEs at different levels of maturity.

Second, the concrete operationalization of the presented framework to allow for use in practice is beyond the scope of our exploration. Subsequent research could focus on identifying meaningful cut-off points for the various dimensions. For example, identifying cut-off points across underlying factors is necessary to classify data as highly competitive or actor relationship as positive or negative in specific use cases. This requires a deep dive in particular contexts, blending qualitative and quantitative methods to highlight the relative significance of the identified dimensions within specific use cases. In this approach it is essential to explore each quadrant using detailed case studies to provide deeper insights into decision criteria and preferences of decision-makers. Furthermore, the hierarchy between the level of data competitiveness and actor relationships, as identified through interviews, could be explored in more detail through quantitative research, examining real-life decision-making processes.

Third, the proposed typology offers a conceptual framework that empowers companies to strategize by categorizing various approaches and tactics. This research has validated the typology through specific use cases, demonstrating its practical applicability. However, further investigation is required to understand the trade-offs that real companies face, ensuring a thorough analysis of potential obstacles, challenges, and unintended outcomes associated with adopting these strategies This study primarily relied on interviews and case studies, which, while providing valuable insights, offer a limited perspective on the broader implementation challenges, such as legal risks, data security, and technical obstacles in diverse contexts. Future research should explore these critical issues more comprehensively, incorporating diverse perspectives and contexts and examining the dynamic evolution of data control strategies in response to rapid technological advancements.

Fourth, future research could focus on providing practical implementation guidance for data access control strategies, potentially through the development of evaluation tools or frameworks that assess data sensitivity levels and measure the effectiveness of data control mechanisms. Additionally, the creation of indicators to identify the quality of these strategies could define trust-building strategies for companies. Conducting small-scale trials or surveys could further explore adoption of data access control mechanisms and identify practical challenges faced by organizations when implementing the identified data control strategies in this research.

A final limitation is the merely tangential investigation into the business models associated with different types of personal data control constellations. The quadrants within the framework could serve as foundations for unique business models for data providers. Thus, future research might delve deeper into the business models adopted by data providers within each quadrant. Additionally, further studies could investigate how companies can integrate data control mechanisms into their business models to leverage them as a competitive advantage, thereby deepening the practical relevance of this research.

7. Conclusions

This study investigates the delicate balance companies must strike when safeguarding their competitive edge while granting data subject data access control within PDEs. Our contributions extend to both the RBT and KBT, building on existing frameworks and insights from the Flemish Solid personal data ecosystem. We developed an "ideal-type" typology of personal data access control constellations in PDEs based on the level of data competitiveness and actor relationships. This typology facilitates trade-offs between protecting data providers' competitive advantages and granting data control to data subjects.

The typology identifies barriers and drivers for data providers' willingness to grant data subject data control, categorizing ecosystems into four quadrants: Involuntary Shared Data Control, Exclusive Data Provider Data Control, Fully Shared Data Control, and Strategically Shared Data Control. Data providers are less willing to share if data hold a competitive advantage or if the relationship with the intended data consumer is negative. This aligns with safeguarding a firm's competitive edge, preserving IP, and ensuring ethical and legal data sharing. While existing frameworks explore how business can share data without compromising competitiveness, they fail to address the unique challenges of PDEs, where data subjects might share competitive data with a data provider's rival. Our typology bridges this gap by introducing different strategic scenarios and adds to the RBT by introducing the notion of shared control between the data provider and data subject.

The typology holds practical implications for both data providers and ecosystem orchestrators. Firstly, it assists data providers in determining which data could or should have data subject data control based on the level of data competitiveness and actor relationships. This aids managerial decision-making in striking the right balance between safeguarding competitiveness and granting data subject data control. Secondly, the conceptual framework is valuable for ecosystem orchestrators in selecting use cases during PDE development. For PDEs, choosing an appropriate use case can be challenging. Our framework helps define suitable scoping in terms of data types and ecosystem width, addressing diverse stakeholder needs.

Author Contributions: Conceptualization, R.D. and L.V.; methodology, R.D. and L.V.; formal analysis, R.D.; writing—original draft preparation, R.D.; writing—review and editing, L.V.; visualization, R.D.; supervision, L.V.; project administration, L.V. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by EWI department (Economie, Wetenschap, Innovatie en Sociale Economie) granted by the Flemish Government in the context of the "SolidLab Vlaanderen" project. The project, referred to as V023/10, is funded through the NextGenerationEU Recovery and Resilience Facility (RRF).

Institutional Review Board Statement: Due to the nature of the study, and the absence of personal data utilization, in accordance with the laws of Belgium, the Ethics Committee approval at VUB wasn't required.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author as the subjects signed a non-disclosure agreement.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

List of interviewees.

Company	Role in Ecosystem	Profile	Date Interview
1	Data consumer/provider	Content expert	13 June 2022
2	Data consumer/provider	C-level	15 June 2022
3	Data consumer/provider	Content expert	16 June 2022
4	Data consumer/provider	Content expert	14 July 2022
5	Data consumer/provider	Content expert	28 June 2022
6	Data consumer/provider	Content expert	4 November 2021
7	Technology service provider	C-level	30 June 2021
8	Data consumer/provider	Content expert	14 October 2021
9	Data consumer/provider	Content expert	10 November 2021
10	Data consumer provider	C-level	6 July 2022
11	Technology service provider	C-level	7 July 2022
12	Ecosystem level	Content expert	12 July 2022
13	Technology service provider	Content expert	13 July 2022
14	Ecosystem level	C-level	28 October 2021
15	Ecosystem Level	C-level	15 October 2021
16	Data consumer/provider	Content expert	8 November 2021
17	Data consumer/provider	Content expert	27 July 2022
18	Technology service provider	C-level	28 July 2022
19	Technology service provider	C-level	2 August 2022
20	Data consumer/provider	Content expert	22 October 2022
21	Technology service provider	C-level	4 August 2022
22	Data consumer/provider	C-level	8 August 2022
23	Data consumer/provider	Content expert	10 August 2022
24	Technology service provider	C-level	11 August 2022
25	Technology service provider	C-level	7 September 2022

Appendix B

The coding tree below showcases the dimensions and factors that were triangulated in the interviews and the literature. "Mentions in Interviews" states the number of interviewees out of 25 that indicated that this dimension or factor is part of their decision to grant data control. The "Literature Dimension" and "Literature Factor" indicate the literature that considers the respective dimensions and factors.

Dimension (Mentions in Interviews)	Literature Dimension	Factor (Mentions)	Literature Factor
Level of data competitiveness (24/25)	[11,13,35,36,38,44,72–75]	Coreness (20/25)	[2,3,11,42,67]
		Level of processing (23/25)	[1,33,40,47]
Actor relationship (24/25)	[3,34,35,43,45–48]	Level of competition (22/25)	[45–48,71]
		Level of collaboration (21/25)	

References

1. Oliveira, M.I.S.; Barros Lima, G.d.F.; Farias Lóscio, B. Investigations into Data Ecosystems: A Systematic Mapping Study. *Knowl. Inf. Syst.* **2019**, *61*, 589–630. [CrossRef]
2. Alexy, O.; George, G.; Salter, A.J. Cui Bono? The Selective Revealing of Knowledge and Its Implications for Innovative Activity. *Acad. Manag. Rev.* **2013**, *38*, 270–291. [CrossRef]
3. Kembro, J.; Naslund, D.; Olhager, J. Information Sharing across Multiple Supply Chain Tiers: A Delphi Study on Antecedents. *Int. J. Prod. Econ.* **2017**, *193*, 77–86. [CrossRef]
4. Hummel, P.; Braun, M.; Dabrock, P. Own Data? Ethical Reflections on Data Ownership. *Philos. Technol.* **2021**, *34*, 545–572. [CrossRef]
5. Knaapi-Junnila, S.; Rantanen, M.M.; Koskinen, J. Are You Talking to Me?—Calling Laypersons in the Sphere of Data Economy Ecosystems. *Inf. Technol. People* **2022**, *35*, 292–310. [CrossRef]
6. Koskinen, J.; Knaapi-Junnila, S.; Helin, A.; Rantanen, M.M.; Hyrynsalmi, S. Ethical Governance Model for the Data Economy Ecosystems. *Digit. Policy Regul. Gov.* **2023**, *25*, 221–235. [CrossRef]
7. Scheider, S.; Lauf, F.; Möller, F.; Otto, B. A Reference System Architecture with Data Sovereignty for Human-Centric Data Ecosystems. *Bus. Inf. Syst. Eng.* **2023**, *65*, 577–595. [CrossRef]
8. Zrenner, J.; Möller, F.O.; Jung, C.; Eitel, A.; Otto, B. Usage Control Architecture Options for Data Sovereignty in Business Ecosystems. *J. Enterp. Inf. Manag.* **2019**, *32*, 477–495. [CrossRef]
9. Gupta, M.; George, J.F. Toward the Development of a Big Data Analytics Capability. *Inf. Manag.* **2016**, *53*, 1049–1064. [CrossRef]
10. Barney, J. Firm Resources and Sustained Competitive Advantage. *J. Manag.* **1991**, *17*, 99–120. [CrossRef]
11. Enders, T.; Wolff, C.; Satzger, G. Knowing What to Share: Selective Revealing in Open Data. In Proceedings of the European Conference on Information Systems, Marrakech, Morocco, 15–17 June 2020.
12. Kugler, P.; Plank, T.J. Coping with the Double-Edged Sword of Data-Sharing in Ecosystems. *Technol. Innov. Manag. Rev.* **2022**, *11*, 5–16. [CrossRef]
13. Loebbecke, C.; van Fenema, P.C.; Powell, P. Managing Inter-Organizational Knowledge Sharing. *J. Strateg. Inf. Syst.* **2016**, *25*, 4–14. [CrossRef]
14. Mamonov, S.; Triantoro, T.M. The Strategic Value of Data Resources in Emergent Industries. *Int. J. Inf. Manag.* **2018**, *39*, 146–155. [CrossRef]
15. Abbas, A.E.; van Velzen, T.; Ofe, H.; van de Kaa, G.; Zuiderwijk, A.; de Reuver, M. Beyond Control over Data: Conceptualizing Data Sovereignty from a Social Contract Perspective. *Electron. Mark.* **2024**, *34*, 20. [CrossRef]
16. Debackere, L.; Colpaert, P.; Taelman, R.; Verborgh, R. A Policy-Oriented Architecture for Enforcing Consent in Solid. In Proceedings of the WWW'22: The ACM Web Conference 2022, Lyon, France, 25–29 April 2022; pp. 516–524.
17. Verbrugge, S.; Vannieuwenborg, F.; Van der Wee, M.; Colle, D.; Taelman, R.; Verborgh, R. Towards a Personal Data Vault Society: An Interplay between Technological and Business Perspectives. In Proceedings of the 2021 60th FITCE Communication Days Congress for ICT Professionals: Industrial Data—Cloud, Low Latency and Privacy (FITCE), Vienna, Austria, 29 September 2021; IEEE: New York, NY, USA, 2021; pp. 1–6.
18. Couldry, N.; Mejias, U.A. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Telev. New Media* **2019**, *20*, 336–349. [CrossRef]
19. Zuboff, S. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *J. Inf. Technol.* **2015**, *30*, 75–89. [CrossRef]
20. Ojasalo, J.; Miskeljin, P. Proposing a Preliminary Concept for a Personal Data Ecosystem. In Proceedings of the INTED2020 Proceedings, 14th International Technology, Education and Development Conference, Valencia, Spain, 1 March 2020; pp. 7451–7459.
21. Spiekermann, S.; Acquisti, A.; Böhme, R.; Hui, K.-L. The Challenges of Personal Data Markets and Privacy. *Electron. Mark.* **2015**, *25*, 161–167. [CrossRef]
22. Lehtiniemi, T. Personal Data Spaces: An Intervention in Surveillance Capitalism? *Surveill. Soc.* **2017**, *15*, 626–639. [CrossRef]
23. Otto, B.; Teuscher, S. *International Data Spaces Association—Reference Architecture Model*; International Data Spaces Association: Dortmund, Germany, 2019; p. 118.
24. Hummel, P.; Braun, M.; Tretter, M.; Dabrock, P. Data Sovereignty: A Review. *Big Data Soc.* **2021**, *8*, 2053951720982012. [CrossRef]
25. von Scherenberg, F.; Hellmeier, M.; Otto, B. Data Sovereignty in Information Systems. *Electron. Mark.* **2024**, *34*, 15. [CrossRef]
26. Rubinfeld, D. Data Portability and Interoperability: An E.U.-U.S. Comparison. *Eur. J. Law Econ.* **2024**, *57*, 163–179. [CrossRef]
27. Lam, W.M.W.; Liu, X. Does Data Portability Facilitate Entry? *Int. J. Ind. Organ.* **2020**, *69*, 102564. [CrossRef]
28. Lauf, F.; Scheider, S.; Bartsch, J.; Herrmann, P.; Radic, M.; Rebbert, M.; Nemat, A.; Langdon, C.S.; Konrad, R.; Sunyaev, A.; et al. Linking Data Sovereignty and Data Economy: Arising Areas of Tension. In Proceedings of the Wirtschaftsinformatik 2022, Online, 21–23 February 2022.
29. Grant, R.M. Toward a Knowledge-Based Theory of the Firm. *Strateg. Manag. J.* **1996**, *17*, 109–122. [CrossRef]

30. Amit, R.; Schoemaker, P.J.H. Strategic Assets and Organizational Rent. *Strateg. Manag. J.* **1993**, *14*, 33–46. [CrossRef]
31. Spender, J.-C. Making Knowledge the Basis of a Dynamic Theory of the Firm. *Strateg. Manag. J.* **1996**, *17*, 45–62. [CrossRef]
32. Nonaka, I.; Toyama, R.; Konno, N. SECI, Ba and Leadership: A Unified Model of Dynamic Knowledge Creation. *Long Range Plann.* **2000**, *33*, 5–34. [CrossRef]
33. Dyer, J.H.; Singh, H. The Relational View: Cooperative Strategy and Sources of Interorganizational Competitive Advantage. *Acad. Manag. Rev.* **1998**, *23*, 660–679. [CrossRef]
34. Li, S.; Lin, B. Accessing Information Sharing and Information Quality in Supply Chain Management. *Decis. Support Syst.* **2006**, *42*, 1641–1656. [CrossRef]
35. Dahlberg, T.; Nokkala, T. Willigness to Share Supply Chain Data in an Ecosystem Governed Platform—An Interview Study. In Proceedings of the 32nd Bled eConference Humanizing Technology for a Sustainable Society, Bled, Slovenia, 16–19 June 2019; AIS Electronic Library (AISeL): Atlanta, GA, USA, 2019; Volume 32, pp. 619–638.
36. Jarman, H.; Luna-Reyes, L.; Pardo, T. *Private Data and Public Value: Governance, Green Consumption, and Sustainable Supply Chains*; Springer: Cham, Switzerland, 2016.
37. Klein, T.; Verhulst, S. *Access to New Data Sources for Statistics Business Models and Incentives for the Corporate Sector*; OECD Statistics Working Papers; OECD Publishing: Paris, France, 2017. [CrossRef]
38. Ensign, P.C.; Hébert, L. Competing Explanations for Knowledge Exchange: Technology Sharing within the Globally Dispersed R&D of the Multinational Enterprise. *J. High Technol. Manag. Res.* **2009**, *20*, 75.
39. Frey, R.M. The Effect of a Blockchain-Supported, Privacy-Preserving System on Disclosure of Personal Data. In Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–5.
40. Weydert, V.; Desmet, P.; Lancelot-Miltgen, C. Convincing Consumers to Share Personal Data: Double-Edged Effect of Offering Money. *J. Consum. Mark.* **2019**, *37*, 1–9. [CrossRef]
41. Zhao, J.; Zhu, C.; Peng, Z.; Xu, X.; Liu, Y. User Willingness toward Knowledge Sharing in Social Networks. *Sustainability* **2018**, *10*, 4680. [CrossRef]
42. Zanetti, D.; Capkun, S. Protecting Sensitive Business Information While Sharing Serial-Level Data. In Proceedings of the 2008 12th Enterprise Distributed Object Computing Conference Workshops, Munich, Germany, 16 September 2008; pp. 183–191.
43. Fawcett, S.; Osterhaus; Magnan, G.; Brau, J.; Mccarter, M. Information Sharing and Supply Chain Performance: The Role of Connectivity and Willingness. *Supply Chain Manag. Int. J.* **2007**, *12*, 358–368. [CrossRef]
44. Trkman, P.; Desouza, K.C. Knowledge Risks in Organizational Networks: An Exploratory Framework. *J. Strateg. Inf. Syst.* **2012**, *21*, 1–17. [CrossRef]
45. Gnyawali, D.R.; Park, B.-J. (Robert) Co-Opetition between Giants: Collaboration with Competitors for Technological Innovation. *Res. Policy* **2011**, *40*, 650–663. [CrossRef]
46. Wiener, M.; Saunders, C. Forced Coopetition in IT Multi-Sourcing. *J. Strateg. Inf. Syst.* **2014**, *23*, 210–225. [CrossRef]
47. Young, M.-L.; Kuo, F.-Y.; Myers, M.D. To Share or Not to Share: A Critical Research Perspective on Knowledge Management Systems. *Eur. J. Inf. Syst.* **2012**, *21*, 496–511. [CrossRef]
48. Seepana, C.; Paulraj, A.; Huq, F.A. The Architecture of Coopetition: Strategic Intent, Ambidextrous Managers, and Knowledge Sharing. *Ind. Mark. Manag.* **2020**, *91*, 100–113. [CrossRef]
49. Kaššaj, M.; Peráček, T. Synergies and Potential of Industry 4.0 and Automated Vehicles in Smart City Infrastructure. *Appl. Sci.* **2024**, *14*, 3575. [CrossRef]
50. Chigbu, U.E.; Atiku, S.O.; Du Plessis, C.C. The Science of Literature Reviews: Searching, Identifying, Selecting, and Synthesising. *Publications* **2023**, *11*, 2. [CrossRef]
51. Goertel, R.A. Literature Review. In *The Cambridge Handbook of Research Methods and Statistics for the Social and Behavioral Sciences: Volume 1: Building a Program of Research*; Nichols, A.L., Edlund, J., Eds.; Cambridge Handbooks in Psychology; Cambridge University Press: Cambridge, UK, 2023; pp. 65–84. ISBN 978-1-316-51852-6.
52. Fontana, A.; Frey, J.H. The Interview: From Structured Questions to Negotiated Text. In *Handbook in Qualitative Research*, 2nd ed.; Sage Publications: Thousand Oaks, CA, USA, 2000; pp. 645–672.
53. Buyle, R.; Taelman, R.; Mostaert, K.; Joris, G.; Mannens, E.; Verborgh, R.; Berners-Lee, T. Streamlining Governmental Processes by Putting Citizens in Control of Their Personal Data. In Proceedings of the Electronic Governance and Open Society: Challenges in Eurasia, St. Petersburg, Russia, 18–19 November 2020; Chugunov, A., Khodachek, I., Misnikov, Y., Trutnev, D., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 346–359.
54. Van Damme, S.; Mechant, P.; Vlassenroot, E.; Van Compernolle, M.; Buyle, R.; Bauwens, D. Towards a Research Agenda for Personal Data Spaces: Synthesis of a Community Driven Process. In *Electronic Government*; Janssen, M., Csáki, C., Lindgren, I., Loukis, E., Melin, U., Viale Pereira, G., Rodríguez Bolívar, M.P., Tambouris, E., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2022; Volume 13391, pp. 563–577. ISBN 978-3-031-15085-2.
55. Denzin, N. *Sociological Methods: A Sourcebook*; McGraw-Hill: New York, NY, USA, 1978.

56. Patton, M. Enhancing the Quality and Credibility of Qualitative Analysis. *Health Serv. Res.* **1999**, *34*, 1208.
57. Turner, S.F.; Cardinal, L.B.; Burton, R.M. Research Design for Mixed Methods: A Triangulation-Based Framework and Roadmap. *Organ. Res. Methods* **2017**, *20*, 243–267. [CrossRef]
58. Roloff, J. Learning from Multi-Stakeholder Networks: Issue-Focussed Stakeholder Management. *J. Bus. Ethics* **2008**, *82*, 233–250. [CrossRef]
59. Berg, S. Snowball Sampling—I. In *Encyclopedia of Statistical Sciences*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2006.
60. Adams, W.C. Conducting Semi-Structured Interviews. In *Handbook of Practical Program Evaluation*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2015; pp. 492–505. ISBN 978-1-119-17138-6.
61. Myers, M.D.; Newman, M. The Qualitative Interview in IS Research: Examining the Craft. *Inf. Organ.* **2007**, *17*, 2–26. [CrossRef]
62. Corbin, J.M.; Strauss, A. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 3rd ed.; SAGE Publications, Inc.: Thousand Oaks, CA, USA, 2008.
63. Mandara, J. The Typological Approach in Child and Family Psychology: A Review of Theory, Methods, and Research. *Clin. Child Fam. Psychol. Rev.* **2003**, *6*, 129–146. [CrossRef]
64. Gerhardt, U. The Use of Weberian Ideal-Type Methodology in Qualitative Data Interpretation: An Outline for Ideal-Type Analysis. *Bull. Sociol. Methodol. Méthodol. Sociol.* **1994**, *45*, 74–126. [CrossRef]
65. Stapley, E.; O'Keeffe, S.; Midgley, N. Developing Typologies in Qualitative Research: The Use of Ideal-Type Analysis. *Int. J. Qual. Methods* **2022**, *21*, 160940692211006. [CrossRef]
66. Nickerson, R.C.; Varshney, U.; Muntermann, J. A Method for Taxonomy Development and Its Application in Information Systems. *Eur. J. Inf. Syst.* **2013**, *22*, 336–359. [CrossRef]
67. Henkel, J. Selective Revealing in Open Innovation Processes: The Case of Embedded Linux. *Res. Policy* **2006**, *35*, 953–969. [CrossRef]
68. Fosso Wamba, S.; Gunasekaran, A.; Akter, S.; Ren, S.; Dubey, R.; Childe, S. Big Data Analytics and Firm Performance: Effect of Dynamic Capabilities. *J. Bus. Res.* **2016**, *70*, 356–365. [CrossRef]
69. Abrams, M. The Origins of Personal Data and Its Implications for Governance. *SSRN Electron. J.* **2014**. [CrossRef]
70. OECD. *Enhancing Access to and Sharing of Data*; OECD: Paris, France, 2019.
71. Wieninger, S.; Götzen, R.; Gudergan, G.; Wenning, K.M. The Strategic Analysis of Business Ecosystems: New Conception and Practical Application of a Research Approach. In Proceedings of the 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Valbonne Sophia-Antipolis, France, 17 June 2019; pp. 1–8.
72. Martens, B.; Duch-Brown, N. *The Economics of Business-to-Government Data Sharing 2020*; JRC Digital Economy Working Paper: Brussels, Belgium, 2020; Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540122 (accessed on 4 December 2024).
73. Coyle, D.; Diepeveen, S.; Wdowin, J.; Tennison, J.; Lawrence, K. *The Value of Data Summary Report*; Benett Institute for Public Policy: Cambridge, UK, 2020; p. 17.
74. Hallberg, N.L.; Brattström, A. Concealing or Revealing? Alternative Paths to Profiting from Innovation. *Eur. Manag. J.* **2019**, *37*, 165–174. [CrossRef]
75. Soper, D.S.; Demirkan, H.; Goul, M. An Interorganizational Knowledge-Sharing Security Model with Breach Propagation Detection. *Inf. Syst. Front.* **2007**, *9*, 469–479. [CrossRef]