Technology in Society 83 (2025) 102953

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

# Data sovereignty in personal data mobility ecosystems: A business model perspective

Ruben D'Hauwers [a,*], Laurens Vandercruysse [b], Pieter Ballon [a]

[a] imec-SMIT, Vrije Universiteit Brussel, 1050, Brussels, Belgium
[b] Applied Economics, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium

ARTICLE INFO

*Keywords:*
Personal data ecosystem
Data access control
Data sovereignty
Data provider
Personal data
Business model
Mobility ecosystems

ABSTRACT

The shift to Personal Data Ecosystems (PDEs) calls for sustainable business models that strike a balance between data sovereignty for individuals and data providers. In PDEs, data subjects gain by retaining control over their data. However, data providers relinquish some control when they grant this data subject control, as sharing data may risk exposing commercially sensitive details to competitors. This is especially relevant in mobility ecosystems where the lack of data control and privacy hinders data sharing. This research applies a business model perspective to data sovereignty and PDE research, offering a comprehensive framework for understanding the strategic decisions data providers make regarding data access control in PDEs. Concretely, we investigate the business dimensions that influence data providers' willingness to grant data access control to data subjects via a two-staged methodology. In a first step, 25 interviews identified key business dimensions, representing a trade-off between value proposition (user- and ecosystem value), value network (collaboration and competition), value finance (value capturing and privacy risk) and value architecture (coreness of data and level of processing of data). In a second stage, a use case analysis of a mobility PDE was performed, utilizing an Analytic Hierarchy Process (AHP) to quantify the preferences of data providers within a mobility ecosystem involving 21 mobility and data experts. The findings show value proposition and value finance are the most salient dimensions in this mobility ecosystem. However, they also reveal critical sector-specific (MaaS Vs. C-ITS) trade-offs between the business model dimensions. The findings reveal sector-specific variations in granting data access control, particularly in MaaS and C-ITS. Key differences shaping business models include data processing levels, privacy risks, and differences in user versus ecosystem orientation. Our results enable deeper understanding of drivers for willingness to grant data access control from the data provider perspective, providing valuable insights into the economic viability and strategic considerations of PDEs, contributing to the broader discourse on data sovereignty and business models.

## 1. Introduction

Business models increasingly depend on data as a core operational resource (Hartmann et al., 2016). To ensure data availability, they may rely on bilateral data sharing between companies (Abraham et al., 2019). Two major evolutions in data usage and data sharing within companies are emerging, driving innovation. First, there is an uptake in use of personal data, leading to the development of personal data markets (S. Spiekermann et al., 2015), raising ethical concerns (Hummel, Braun, & Dabrock, 2021). Second, data ecosystems are emerging (S. Oliveira et al., 2019) in which multiple actors collaborate to foster innovation. These evolutions push companies to develop collaborative business models that take into account personal data rights and safeguard user trust (Wiener et al., 2020). Also in the mobility context, the pursuit of new revenue streams involving data of mobility users (Anthony, 2023) drives such an evolution.

Against this backdrop, a user-centric Personal Data Ecosystem (PDE) is advocated. Such an ecosystem is based on personal data and incorporates a business model that empowers individuals to control their data disclosure, allowing them to potentially receive value in return (Koskinen et al., 2023; Lehtiniemi, 2017). PDEs empower individuals to control their data disclosure and data usage (Knaapi-Junnila et al., 2022). However, despite ongoing development of PDEs, user and business adoption is lagging (Van Damme et al., 2022), partly due to a lack of

* Corresponding author. Imec – SMIT, Vrije Universiteit Brussel, Pleinlaan 9, 1050, Brussels, Belgium.
*E-mail addresses:* Ruben.dhauwers@vub.be (R. D'Hauwers), aurens.vandercruysse@vub.be (L. Vandercruysse).

https://doi.org/10.1016/j.techsoc.2025.102953
Received 26 November 2024; Received in revised form 19 May 2025; Accepted 22 May 2025
Available online 29 May 2025

data availability (Fallatah et al., 2023). Also mobility ecosystems, such as in Mobility as a Service (MAAS) and Cooperative Intelligent Transport Systems (C-ITS) ecosystems, face challenges due to limited data sharing between organizations and users, largely due to privacy concerns (Kapp et al., 2023; Pulkkinen et al., 2019). Research suggests that empowering users with data control can foster data sharing (Rohunen & Markkula, 2019), making a PDE solution a promising enabler in mobility ecosystems (Hoffmann et al., 2021, pp. 1–6).

To ensure the availability of data in PDEs, such as in mobility ecosystems, distributing and enforcing data sovereignty is crucial (Hellmeier & Scherenberg, 2023; Otto & Jarke, 2019). Data sovereignty concerns different agents, ranging from organizations and individuals, having power and control over data (Hummel, Braun, Tretter, & Dabrock, 2021; von Scherenberg et al., 2024). This can be achieved through mechanisms like access control (AC) and usage control (UC) allowing data providers and data subjects to set terms for data usage by other actors (Scheider et al., 2023; Zrenner et al., 2019). However, granting data access control to data subjects may conflict with data providers' own data sovereignty (Abbas et al., 2024), as a data subject might choose to share data that a provider considers commercially sensitive with a competitor. Therefore, the granting of data access control over personal data may be seen as a risk for competitiveness (Gupta & George, 2016). Nonetheless, legal frameworks on privacy, like the General Data Protection Regulation (GDPR), incorporate individual data protection and portability rights (Solove & Schwartz, 2020) ensuring de jure partial shared data sovereignty. In practice, de facto shared data sovereignty is often complicated (Gal & Rubinfeld, 2019; Lam & Liu, 2020; Lauf et al., 2022; Rubinfeld, 2024).

Thus, this study examines the factors influencing data providers' decisions to grant de facto access and usage control to data subjects to balance data sovereignty within mobility ecosystems. Existing studies explore data sovereignty in business-to-business contexts (Zrenner et al., 2019) and Personal Data Ecosystems (Scheider et al., 2023), but they offer little insight into the strategic trade-offs data providers face in mobility-related PDEs. While research on mobility ecosystems (Mügge et al., 2023) and data marketplaces (Abbas et al., 2024) addresses organizational data sharing and personal data rights protection, it does not fully examine how data providers balance enabling data sovereignty for subjects with maintaining a competitive advantage. This research addresses the research gap in understanding the key business model dimensions that shape data providers' strategic decisions when navigating trade-offs in granting data access control, particularly in mobility PDEs. This study investigates these dimensions through the lens of networked business models (Al-Debei & Avison, 2010) identifying the most decisive business dimensions shaping data providers' willingness to grant data access control, leading to the following research questions.

- RQ1: What business dimensions influence data providers' willingness to grant data access control to data subjects in PDEs?
- RQ2: What is the relative importance of business dimensions influencing data providers' willingness to grant data access control to data subjects in a mobility PDE?

The remainder of this article is structured as follows: Section 2 comprises the literature review, Section 3 covers the methodology, Section 4 presents our research results, Section 5 constitutes the discussion, and Section 6 concludes.

## 2. Literature review

### 2.1. Evolutions of data usage in businesses in mobility ecosystems

As data becomes central to business model development (Hartmann et al., 2016), companies increasingly view it as a resource to be protected and leveraged internally (Gupta & George, 2016). Therefore, earlier information systems (IS) research focused on managing data as a strategic enterprise asset (Panian, 2010). Subsequently, to ensure data availability, bilateral data sharing, where organizations buy or sell data in business-to-business relationships, emerged (Abraham et al., 2019). In this context, research has shown companies strive to balance safeguarding and disclosing valuable data to protect their competitive advantage in the context of inter-organizational data sharing (Loebbecke et al., 2016; Trkman & Desouza, 2012).

First, it is clear that bilateral data sharing becomes more complex when it concerns personal data (S. Spiekermann et al., 2015), as this raises concerns about how and by whom data is, and should be, used and shared (Leidner & Tona, 2021; Zuboff, 2015). While studies have investigated individuals' privacy concerns (Prince et al., 2023) as well as their willingness to share data with organizations (Bélanger & Crossler, 2011, 2019), there is a growing need to research the design of business models which include data subjects (Koskinen et al., 2023).

Additionally, another key trend is the emergence of data ecosystems, which are complex, networked communities of actors sharing a common interest in processing and sharing data to foster innovation and co-create value (S. Oliveira et al., 2019). Data ecosystems raise the complexity for companies significantly. This is especially the case in mobility ecosystems, where collaboration among organizations becomes crucial, in view of new business models involving mobility users' data (Anthony, 2023). We refer to mobility ecosystems as Mobility as a Service (MAAS) and Cooperative Intelligent Transport Systems (C-ITS) ecosystems in this work. MAAS unifies multiple transport modes into a single platform (Hensher et al., 2021) while C-ITS enables real-time data exchange to improve road safety and traffic flow (Javed et al., 2019; Kang et al., 2023). Both shift the model from product ownership to data-driven service use, with users actively contributing data. This contrasts with the traditional automotive ecosystem, which is centered on vehicle production and sales, where consumers purchase a physical product (Jacobs & Singhal, 2020; Rachinger & Müller, 2024). While data exchange exists in automotive contexts, it typically involves manufacturing data shared among industry players (Mügge et al., 2023). In contract, in mobility ecosystems, a broader range of stakeholders, including service providers, governments, telecoms, and users, must collaborate around (personal) data sharing and governance (Sanchez-Iborra et al., 2020; Schulz et al., 2020, 2024). However, as user data becomes central, business models in mobility ecosystems must adapt to this collaborative, data-centric environment ensuring an ethical usage of mobility data (Anthony, 2023; Kamargianni & Matyas, 2017a, b).

In (mobility) data ecosystems, IS resources, including data, are located with other actors beyond the control of a single organization (Winter et al., 2014). IS research should therefore explore how strategic and economic value can be created in data ecosystems (Lis & Otto, 2020) or in inter-organizational networks (Abraham et al., 2019).This shift drives companies to develop innovative business models that prioritize ethical data usage (Hummel, Braun, & Dabrock, 2021) and respect personal data rights (Wiener et al., 2020). In this context, Personal Data Ecosystems emerge, which are discussed in section 2.2, with a specific focus on personal mobility data ecosystems.

### 2.2. Personal (mobility) data ecosystems

To enable these evolutions, different PDEs arise aiming to mitigate the power of large dominant players in contemporary data markets (Moiso & Minerva, 2012, pp. 202–209). PDEs are data ecosystems based on information about individuals based on a "user-centric" governance model (Rantanen & Koskinen, 2020). They enable data subjects to control their data by defining how it is disclosed and to whom (Fragidis, 2017; Lehtiniemi, 2017; Scheider et al., 2023). PDEs can take the form of a single cloud storage such as Dropbox (Caviglione et al., 2016) or more advanced, automated privacy aware PDE (Singh et al., 2021). PDEs are operationalized in, among others, initiatives such as Social Linked Data (Solid) (Sambra et al., 2016) and the MyData community (Poikola et al.,

2020). In the context of PDEs, the most noteworthy stakeholders include data providers, data consumers and data subjects. A data provider refers to the organization controlling data (Otto & Teuscher, 2019, p. 118). A data subject refers to the individual to whom the personal data relates (Scheider et al., 2023). Data consumers receive personal data from data providers or directly from data subjects (Otto & Teuscher, 2019, p. 118).

Several concepts are related to PDEs, including data ecosystems, data spaces, and data marketplaces. Data Ecosystems are socio-technical networks where various actors collaborate to find, archive, publish, consume, or reuse data. These networks foster innovation, create value, and support new businesses (S. Oliveira et al., 2019). Personal Data Ecosystems, a specific type of data ecosystem, focus on ensuring that data subjects maintain control over their personal data. Data Spaces are digital infrastructures designed to provide a shared environment for participants to exchange data securely and sovereignly (Curry, 2020; Scerri et al., 2022). These spaces address concerns organizations have when sharing data with other organizations, such as the risk of misappropriation or losing control over shared data (Mügge et al., 2023). In contrast, PDEs emphasize data sovereignty for the data subject, with a primary focus on enabling their control over personal data. Data Marketplaces are digital intermediaries that facilitate the exchange and monetization of data by connecting data providers and consumers. These platforms ensure that data quality, pricing, and regulatory compliance are maintained under standardized contractual terms (Koutroumpis et al., 2017; M. Spiekermann, 2019). The key distinction between these three concepts with PDEs lies in their focus and governance on data subjects. While data ecosystems, data spaces, and data marketplaces typically focus on organizational data sharing with governance managed by the involved organizations, Personal Data Ecosystems are user-centric environments. In these ecosystems, individuals retain control over how their personal information is disclosed and shared, empowering them with direct governance over their data (Fragidis, 2017; Rantanen & Koskinen, 2020).

IS research highlights the need to further explore how different data intermediary services in PDEs can sustainably enable digital innovations with personal data (Davidson et al., 2023). To date, PDE related initiatives did not reshuffle power imbalances as intended (Lehtiniemi, 2017), as they have had a limited breakthrough in the daily lives of people and businesses. From a business perspective, identifying viable business models for organizations to adopt PDEs is a concern (Van Damme et al., 2022). Lack of data availability and accessibility within the ecosystem are concrete drawbacks (Fallatah et al., 2023). Sustainable PDE emergence necessitates economically viable intermediary services, including business incentives to grant data access control (Scheider et al., 2023).

Mobility ecosystems are hindered by the lack of data sharing between organizations and users (Pulkkinen et al., 2019; Pütz et al., 2019), with privacy being a major blocking factor (Kapp et al., 2023; Tu et al., 2018). Solutions enabling PDEs are seen as a promising enabler to enhance privacy when sharing data in mobility ecosystems (Hoffmann et al., 2021, pp. 1–6). As some research shows that data sharing in mobility can be encouraged by giving users control over their data (Rohunen & Markkula, 2019), the emergence of PDEs in mobility can enable the sharing of data. Thus, data availability in mobility data ecosystems requires giving data subjects control over their personal data.

However, the shift toward PDEs, where individuals gain control over personal data that companies currently hold exclusively, introduces strategic challenges, particularly in protecting a data provider's competitive data (Abbas et al., 2024). For example, a data subject might choose to share information that a provider considers commercially sensitive with a competitor. Despite this risk, enabling PDEs can benefit data providers by increasing data subjects' willingness to share their data with companies (Frey, 2017, p. 409; Weydert et al., 2019) and by creating value for the data subjects themselves (Zhao et al., 2018). Therefore, data providers must carefully balance their own data sovereignty with that of the data subjects when deciding whether to participate in a PDE.

### 2.3. Balancing data sovereignty between data subjects and data providers in PDEs

The evolution towards PDEs makes data sovereignty an important concept to investigate. **Data sovereignty** has been explored in various contexts, including cloud computing (Banse, 2021, pp. 153–154; Irion, 2012), between enterprises (Jarke et al., 2019), between businesses and individuals (Nagel & Lycklama, 2021), and national data governance (Irion, 2012). While the term is often associated with meaningful control, ownership, and claims over data or data infrastructure, its precise interpretation varies depending on the perspective (Hummel, Braun, Tretter, & Dabrock, 2021). In discussions on the self-determination of data providers and data subjects, the dominant approach in literature emphasizes a control-centric view of data sovereignty (Hellmeier & Scherenberg, 2023). Data sovereignty concerns different agents, ranging from organizations and individuals, having power and control over data (Hellmeier & Scherenberg, 2023; Hummel, Braun, Tretter, & Dabrock, 2021). Other authors define data sovereignty as the ability of data owners to independently determine how their data is shared and used (Sarabia-Jácome et al., 2019). This includes establishing self-defined usage rules, influencing and tracing data flows, and freely deciding whether, when, and where to share or migrate data (Lauf et al., 2022). In this work, we explore the context of data sovereignty between organizations and data subjects from a data control perspective. We explore the rebalancing of data sovereignty in personal data ecosystems, focusing on shifting control from companies to the individuals the data concerns, and examining companies' willingness to support this shift.

It is important to distinguish the concept of data sovereignty from data protection and privacy. Data sovereignty, from a control perspective, refers to the actual, exclusive power to control and utilize data. In contrast, data protection and privacy focuses on mitigating data usage risks and preventing harms for individuals (Wright & Raab, 2014). While these concepts can complement each other, since mechanisms that give data subjects greater control may also be used to enhance privacy (Abbas, 2024; Hummel, 2021), they are typically supported through different means. Data protection and privacy are often enforced through legal frameworks, such as the right to reject or not be subject to specific data uses (see e.g.Bieker (2022)). European legislation like the General Data Protection Regulation (GDPR) and Payment Services Directive II (PSD II) establish "de jure" data protection and/or data sovereignty to data subjects, offering individuals certain formal rights to their data. GDPR grants the right to data portability, allowing individuals to transfer their data to another organization without hindrance. PSDII mandates banks to provide APIs to third-party providers upon data subjects' request. However, "de facto" data sovereignty is often limited in practice. First, data portability is often constrained by low-quality APIs that meet legal requirements but are not user-friendly (Rubinfeld, 2024). 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 (Lam & Liu, 2020; Rubinfeld, 2024). Third, the emphasis on privacy of the legislations can slow the development of user services and data-driven business models (Lauf et al., 2022; Scheider et al., 2023; S. Spiekermann et al., 2015). In this work, however, we examine how control over data can be rebalanced between individuals and organizations through de facto means that empower both data subjects and data providers. In that sense, key mechanisms for enabling data sovereignty from a control perspective are access control (AC) and usage control (UC). These serve as de facto tools to establish data sovereignty between data subjects and data providers within PDEs, which is the central focus of this research. AC and UC allow data providers and data subjects to set terms for data usage, specifying which actors in ecosystems can access and use the data (Scheider et al., 2023; Zrenner et al., 2019).

For data subjects, different authors advocate for mechanisms to

enable control over their personal data usage, including determining access and processing purposes (Hummel, Braun, & Dabrock, 2021). Data sovereignty would thus enable individuals to view, store, track, delete and share their personal data (Lauf et al., 2022).However, for data providers, granting data access control to data subjects may complicate data usage and control (Abbas et al., 2024). Data providers often view personal data as a key competitive asset (Gupta & George, 2016). As data subjects take on a central role in PDEs, and may decide to share competitive data prevously controlled by the data provider with rivals, it forces companies to establish strategies to protect their competitive advantage (D'Hauwers & Vandercruysse, 2025). The strategies defining whether they want to share data has been researched in the context of inter-organizational data sharing (Fawcett et al., 2007; Kugler & Plank, 2021; Li & Lin, 2006; Loebbecke et al., 2016; Trkman & Desouza, 2012). Research has shown that, within mobility ecosystems and manufacturing ecosystems, the usage and access control requirements set by data providers are crucial to enable organizational data sharing (Möller et al., 2024; Mügge et al., 2023). However, further investigation is needed in the specific context of PDEs. Previous studies have indicated that data providers can benefit from enabling PDEs, as increased data access control (Frey et al., 2017, pp. 1–5; Weydert et al., 2019), can create value for the user (Zhao et al., 2018), thereby increasing their willingness to share data with companies.

As de jure data sovereignty has been unable to overhaul the status quo, it is worth looking into whether previous data sovereignty research included the perspective of data providers regarding motivations to grant de facto data sovereignty to data subjects. First, three studies offer literature reviews to conceptualize data sovereignty in IS, but none of these literature reviews address data providers' perspectives or the decision of data providers to grant data access control to data subjects from a business model standpoint. A first literature review differentiates between data sovereignty, digital sovereignty, and technical sovereignty, but merely provides definitions (Hellmeier & Scherenberg, 2023). Another study identifies seven core aspects of data sovereignty, including trust, data infrastructure, contractual agreements, and data assets (von Scherenberg et al., 2024). Last, Hummel defines data sovereignty based on dimensions like context, agents, and value, showing different types of data sovereignty exist (Hummel, Braun, Tretter, & Dabrock, 2021). However, none of these literature reviews address data providers' perspectives or the decision of data providers to grant data access control to data subjects from a business model standpoint.

Two other studies focus on defining a (technical) reference system architecture for data access control but neglect strategic considerations from the data provider's viewpoint. One study focuses on a business-to-business context (Zrenner et al., 2019) and another on Personal Data Ecosystems (PDEs) (Scheider et al., 2023). The latter introduces a reference system architecture to enable data sovereignty within PDEs, considering legal, ethical, economic, and technical constraints. Additionally, another study examines data sovereignty from the perspective of data providers within a mobility ecosystem focused on organizational data sharing. However, it does not involve data subjects, and therefore, it lacks insights on data sovereignty within personal data ecosystems in a mobility context (Mügge et al., 2023). A last study on data sovereignty develops a conceptual framework for data marketplaces (Abbas et al., 2024), addressing rights protection, participation, and basic rights provision, while considering contextual factors like data type and business data sharing. Although this study includes a data provider perspective, it does not explore the strategic trade-offs for data providers and does not focus exclusively on personal data ecosystems.

Balancing data sovereignty between data subjects and providers in PDEs requires a strategic decision to grant individuals control over their personal data while safeguarding competitive interests. This shift impacts business models, as companies must find ways to create value while managing potential risks.

### 2.4. Business models at a network level as an analytical framework

Adopting a strategic perspective is crucial for aligning PDE participation with sustainable business goals and competitive advantage. In this work, business models serve as the analytical framework for this alignment. In IS, business models represent an organization's resources, their configurations, and core competencies, as well as its position in the value system, relationships and transactions with stakeholders (Al-Debei & Avison, 2010). Foundational business model literature distinguishes between business models defined at the firm level (Andreini et al., 2022; Osterwalder et al., 2005) and those at the network level (Al-Debei & Avison, 2010; Rocca & Snehota, 2017). As PDEs concern interactions of data providers at a networked level, these frameworks are more appropriate for this work.

In business models literature at the network level, key questions revolve around shifting organizational boundaries in complex value networks (Walravens & Ballon, 2013), which revolve around balancing value and control, where companies must make strategic decisions to align their business models effectively: "Who controls the value network and the overall system design" and "Is substantial value being produced and captured by this model in the value network. A business model is feasible when trade-offs between dimensions create a "strategic fit," enabling differentiation and alignment with strategy (Globocnik et al., 2020). The analytical framework by Al-Debei used in this work consists of four dimensions representing this trade-off, which can be seen in Fig. 1: value network, value proposition, value finance, and value architecture (Al-Debei & Avison, 2010). The value proposition describes the market offerings of an organization as well as its interactions with customers. Value finance captures how the organization's cost structure, pricing methods, and revenue streams are structured. Value architecture refers to an organization's core resources and capabilities, which includes the technological infrastructure and organizational infrastructure that allows the provisioning of products and services in addition to information flows. Finally, the value network depicts the interactions and relationships of an organization with key external partners and other stakeholders.

Business model frameworks at a network level have been applied and adapted to data ecosystems in previous research (D'Hauwers et al., 2022). However, there is limited research on data providers willingness to grant data access control in PDEs. Two literature reviews highlight the need to explore the business models of data providers in enabling privacy and data control in PDEs (Günther et al., 2017; Wiener et al., 2020). Some studies have examined business models of data intermediaries, particularly focusing on PDEs. One study explored how PDEs enable the balancing of data demands with privacy through legal, conceptual, and technical measures (Spiekermann & Novotny, 2015). Another research investigated business models of different types of data intermediaries including PDEs (Micheli et al., 2023). However, these studies neglect the perspective of data providers in PDEs, particularly in the context of mobility.

Business model research on mobility ecosystems highlights their rapid evolution toward connected, autonomous, and service-oriented businesses (Turienzo et al., 2022). These changes drive the adoption of digital platforms that rely on data management to enable personalized services (Turienzo et al., 2023, 2024). As data usage and exchange become widespread, they significantly impact the business models and strategies of mobility ecosystem stakeholders (Pérez-Moure et al., 2023). To comply with regulations like the GDPR, business models must integrate data protection measures, necessitating a shift toward privacy-centric frameworks (Costantini, 2017). This transition requires stakeholders to develop capabilities in data exchange, integrating both data management and privacy protections into their business models (Cabanelas et al., 2023). While research underscores the need to balance data sharing with strong privacy safeguards (Armingol et al., 2018), there is still limited research on specific business models for PDEs in mobility ecosystems, particularly regarding the business model of data

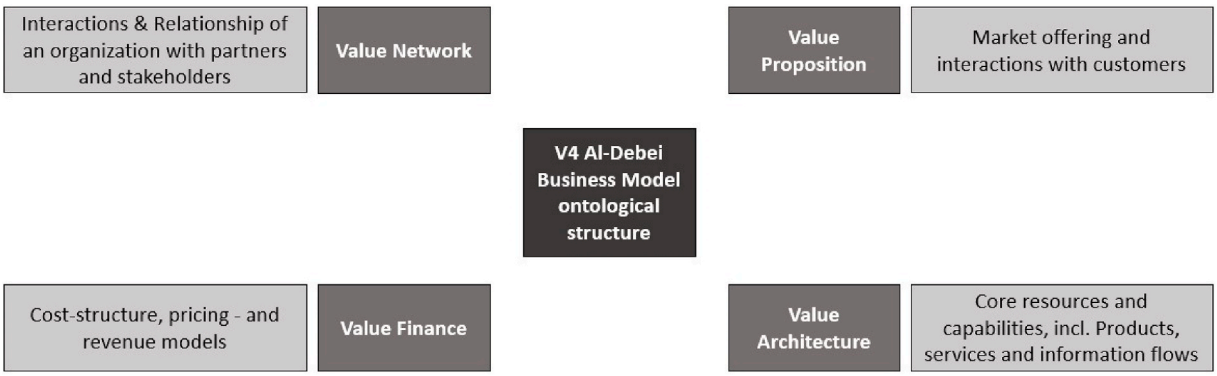



**Fig. 1.** Business Model ontological structure, own adaptation based on (Al-Debei & Avison, 2010).

providers related to granting data access control over their data.

Sector-specific research beyond mobility ecosystems has also examined business models enabling privacy and control measures, including smart tourism ecosystems (Gretzel et al., 2015), a PDE on personal data in health data (Vezyridis & Timmons, 2015), and the impact of a PDE on the business model health insurance providers (Iivari et al., 2017). Nonetheless, none address the business model decisions data providers must make to grant data access control, particularly not in mobility contexts.

## 3. Methodology

An overview of the methodology used for this work can be found in Fig. 2, which consists of two major steps: exploratory interviews in the Solid ecosystem in Flanders, and an AHP analysis on the use of a mobility PDE.

### 3.1. Exploratory interviews

Exploratory interviews were conducted within the Solid Ecosystem in Flanders, which emphasizes personal data control and has notable policy support, development, and private sector interest (Van Damme et al., 2022) with a focus on mobility (Mobilidata, 2023). The Flemish government prioritizes Solid PDEs as a policy and innovation driver (Digitaal Vlaanderen, 2022) fostering an open ecosystem for data exchange while ensuring data control for data subjects (Verbrugge et al., 2021). The 25 multi-stakeholder interviews were performed in an issue-focused stakeholder management approach (Roloff, 2008). We employed a snowballing method to select interview subjects based on their interest in participating in the Flemish Solid personal data ecosystem (Berg, 2006). The interviewees' roles in their companies and the Solid ecosystem can be found in Annex 1. The Solid ecosystem in Flanders is particularly interesting due to its active development, substantial policy stimulation, and private sector interest (Van Damme et al., 2022). The Flemish government prioritizes Solid PDESs as a policy and innovation driver, and the establishment of a "'data utility company"' is evidence of this commitment (Digitaal Vlaanderen, 2022). 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 (Buyle et al., 2020; Verbrugge et al., 2021). While interviews have inherent limitations in generalizability, studying this ecosystem with a sample size of 25 provides broader insights into the emergence of data access control principles. As the current ecosystem is rather small, this captures a large portion of the sample at hand, ensuring representative insights. Additionally, the authors outline general data access control principles that extend beyond the Solid technology, supporting the applicability of findings to other technologies and contexts.

The semi-structured interview method was used, well -suited for the exploratory nature of the first step of the research to identify the business dimensions (Adams, 2015). It allows researchers to balance guided questions with the flexibility to explore respondents' perspectives in depth, blending structure with adaptability (Fontana & Frey, 2000). This method offers flexibility with open-ended questions and allows for follow-up queries. The major objective is for neutral interviewers to obtain comparable information from a potentially large number of interviewees (Edwards & Holland, 2013). Guidelines specific for semi-structured interviews in IS research ensured interview validity (Myers & Newman, 2007). 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. Interview guides can be found in Annex 3. All interviews were conducted via Microsoft Teams and ranged from 1 h to 1 h 45 min in duration.

To identify the different dimensions from the interviews, axial coding, a mixed-method approach combining inductive and deductive reasoning, was applied (Corbin & Strauss, 2008). The analysis was structured using the business model framework (Al-Debei & Avison, 2010) incorporating the dimensions of value proposition, value network, value finance, and value architecture. The framework was used as a coding structure to define the primary dimensions.[1] To identify sub-dimensions, initial interviews were examined to extract preliminary concepts, with axial coding applied to establish relationships among these concepts and systematically categorize them. Finally, selective coding was conducted on the sub-dimensions to refine the categories further and iteratively identify key sub-dimensions. This iterative process provided a deeper understanding of the relationships between the identified dimensions, ensuring a structured and comprehensive analysis. Fig. 3 shows a decision tree, and Table 1 provides examples of the axial coding of the interviews based on the value and control framework. To illustrate our coding approach, consider the following quote from an HR company, also included in Table 1:

"*We could share HR data in an ecosystem. However, competitive data, like an assessment we made, we will not share with anyone. We do tests, role playing games … to generate this data (….) However, if a company would pay for this data, that may be a new revenue model for us"* (Interview 3). We coded the first part of this quote under the dimension "value architecture," as it highlights what the company considers a core resource, namely, the competitive data generated through assessments. As a sub-dimension, we assigned it to "level of processing," since the reluctance to share this data is tied to the significant effort invested in producing it through tests and role-playing activities. The second part of the quote, referring to potential monetization, was coded under the dimension

[1] The authors examined the same interviews in a separate study, this time using the resource-based theory as their analytical framework, as detailed in their published work (D'Hauwers & Vandercruysse, 2025).

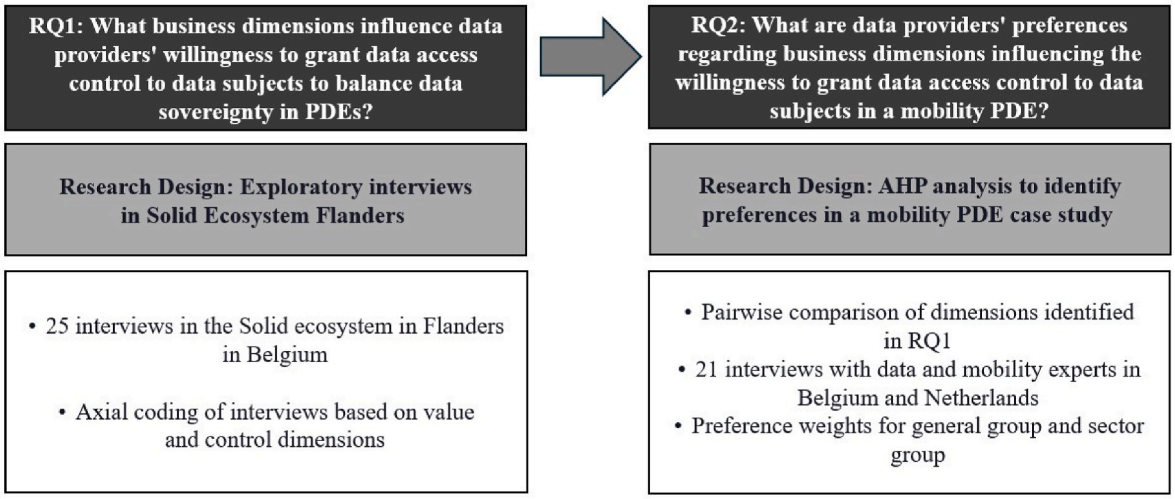



**Fig. 2.** Methodology.

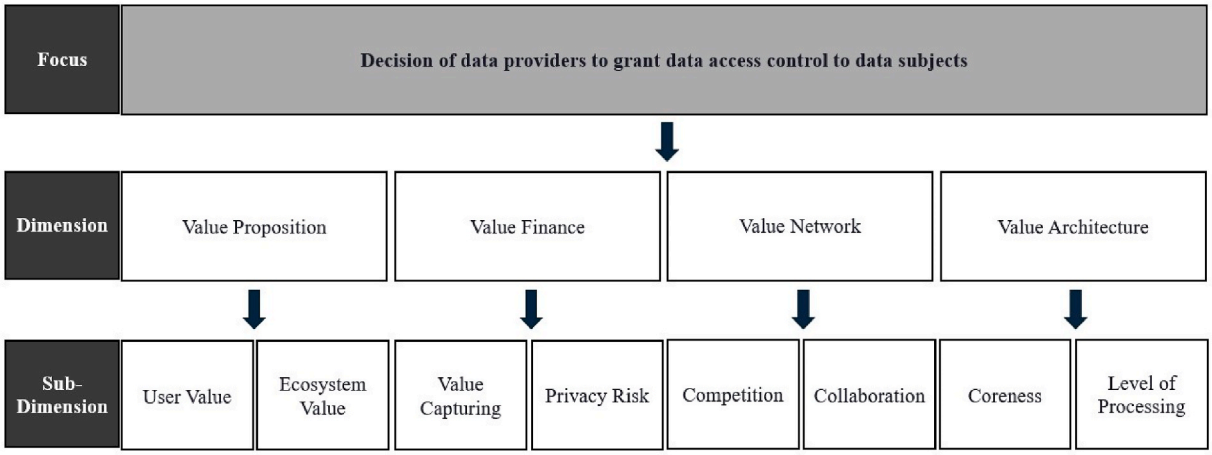



**Fig. 3.** Decision tree exploratory interviews.

"value finance," as it relates to the company's financing model. More specifically, we categorized it under the sub-dimension "value capturing," as it suggests that enabling access control over data could generate new revenue streams.

The data analysis followed a "reliable witness" epistemological approach, treating interviewees' insights as trustworthy sources of knowledge on data access control (Whittle & Reissner, 2025). To ensure the validity and objectivity of the interview analysis, a code-recode strategy was used. This involved initially coding the data, setting it aside, and later re-coding it to check for consistency. Validity and credibility were further strengthened by quantifying the frequency of each dimension across interviews, verifying whether key themes were widely mentioned. Additionally, the research process underwent external scrutiny, with another researcher reviewing the methodology and contributing to discussions throughout the study to maintain consistency and reliability. To support transferability, interview participants were selected from diverse businesses and roles within the Solid ecosystem in Flanders, broadening the applicability of the findings. Finally, confirmability was ensured by keeping detailed records of verbatim interview notes.

### *3.2. AHP analysis on a mobility PDE context*

The analytical hierarchical process (AHP) methodology was employed to research the preferences of data providers in a mobility PDE context. The Analytic Hierarchy Process (AHP), developed by Saaty, is a widely used tool for complex decision-making (T. Saaty, 1994). While it is primarily employed to rank policy alternatives based on predefined, scorable criteria, AHP can also assess the importance of different dimensions to be made within a specific context (Amponsah, 2011). As a leading multi-criteria decision-making (MCDM) method that integrates subjective qualitative data (Ramanathan & Ganesh, 1995). AHP is well-suited for addressing research question RQ2, which focuses on identifying the key business dimensions for granting data access control.

To introduce the concept of PDEs in the MAAS and C-ITS ecosystems, participants in the study were first given an overview of how these systems function. A mobility PDE stores personal mobility data while granting data subjects control over access and usage. Private data providers can enable this by offering data access and usage control to data subjects through APIs. For example, a car-sharing provider may allow users to access and manage their profile and usage data. Data subjects can then decide how to share their information within MAAS and C-ITS ecosystems. Through an interface, they can choose whether to share specific data, such as their profile information, with a bike-sharing provider or other mobility services.

The analytical hierarchical process (AHP) methodology was employed to research the preferences of data providers in the mobility ecosystem. Saaty developed the AHP methodology as a structured approach to tackle wicked decision problems involving multiple criteria

**Table 1**
Examples of axial coding based on value and control framework.

| Interview Quote | Dimension | Sub-dimension |
|---|---|---|
| "Several use cases involve improving the customer journey of the user, e.g. succession planning, mortgages, where enabling users to share data would make the customer journey more convenient for the user. "(Interview 2) | Value Proposition | User Value |
| "When granting data access control, it can help an ecosystem of small business owners to create new offerings. E.g., if my company (a telecom provider), would share location data, restaurants could provide more targeted offerings to their customers." (Interview 20) | Value Proposition | Ecosystem Value |
| "We could share HR data in an ecosystem. However, competitive data, like an assessment we made, we will not share with anyone. We do tests, role playing games … to generate this data." (Interview 3) | Value Architecture | Level of Processing |
| "A recruitment company claims it has a database of 250 000 resumes. This database is what their competitive advantage is based on. They will not want to just share the resumes of their database." (Interview 10) | Value Architecture | Coreness |
| "Sharing data between companies will be very difficult. I cannot imagine companies will allow data to be shared with competitors. It will not happen." (Interview 24) | Value Network | Competition |
| "Sharing data is possible for organizations that are collaborating. There will be collaboration for getting common market insights, if they agree to do something together." (Interview 25) | Value Network | Collaboration |
| "If we want to enable sharing of data, we need to ask for consent of the customer. This can be a long process. If she sharing of data can be done by the citizen in the vault, and they consent to share data, this is more efficient. Thus, GDPR is a driver, as the cost to save and process data can be outsourced to a Solid pod." (Interview 2) | Value Finance | Legal Risk |
| "We could generate new income streams by enabling data subjects to share data, and through data validation." (Interview 3) | Value Finance | Value Capturing |

and alternatives (R. W. Saaty, 1987; T. Saaty, 1994). In this work, the AHP was used to determine the preference of the business dimensions for granting data access control (Amponsah, 2011; Mehregan, 2011; Shahin & Mahbod, 2007). An overview of the different steps taken are shown in Fig. 4. We followed a step by step approach similar to another work (Vandercruysse et al., 2021). First, the list of relevant dimensions is initially compiled based on the results from the interviews conducted in the Solid Ecosystem during research step 1. Second, the preferences of data providers were ranked by experts through a pairwise comparison (Chen & Wang, 2010; Taherdoost, 2017). A decision tree can be found in Annex 3 (T. Saaty, 1994). The respondents rated the relative importance or preference using a numerical scale from 1 to 9. A rating of 1 indicates that both dimensions are equally important, while a rating of 9 means the first theme is significantly more important than the second. The AHP was conducted through telephone interviews with 21 mobility and data experts in Belgium and the Netherlands (Annex 2). Fig. 5 illustrates an example of the concrete scoring mechanism used in a pairwise comparison. Third, the pairwise comparisons are converted into individual result matrices, based on each respondent's scores for the dimensions. Fourth, the individual result matrices are used to calculate the leading eigenvectors, which determine the relative weights of the dimensions. These weights are then standardized to sum to one, allowing for the derivation of relative importance at the individual level. Fifth, the individual result matrices are aggregated into result matrices for each stakeholder group and the entire sample. This is done by computing the geometric means of the individual matrices. The standardized leading eigenvectors once again represent the respective relative weights. This analysis was performed on a group and entire sample level, avoiding bias that may be present when the judgements are considered from a single expert (Forman & Peniwati, 1998; Ossadnik et al., 2016). Sixth, to establish a global ranking of interests at both the group and sample levels, we compute the result matrices using the geometric means of the stakeholder group and sample-level matrices. The findings were analyzed across the entire participant group as well as within the MAAS and C-ITS subgroups. Using the geometric mean of the individual result matrices, the group matrices are calculated of the different stakeholder groups (Ishizaka & Labib, 2011). Last, the consistency ratio was calculated, for which 0.1 is considered to indicate a tolerable consistent ranking for grouped responses (T. L. Saaty & Tran, 2007). The "ahpsurvey" package in R was used to analyze the results (Cho, 2019).

## 4. Results

### 4.1. Business model of data providers in personal data ecosystems to grant data access control

We aimed to analyze the decision-making process of data providers in granting data access control to data subjects through the lens of the business model framework by Al-Debei and Avison (2010). We identified various dimensions influencing the willingness to grant data access control based on expert interviews. The following subsections will cover the value proposition, value finance, value network and value architecture dimensions influencing the decision to grant data access control, based on the insights from the interviews. These dimensions build further upon a previously published typology of personal data control configurations by the authors, which was analyzed from a different perspective using the resource-based view (D'Hauwers & Vandercruysse, 2025). In all the quotes below, adding data to a vault, a Pod, or Solid in general reflects the core principle of Solid: empowering data subjects with control over who can access their data and enabling them to share it with third parties. Participants were introduced to a workflow illustrating how data access control is granted in Solid, and the follow-up questions focused on identifying the drivers and barriers to implementing such mechanisms for sharing data with third parties, as detailed in the interview guide (see Annex 3). To give more context, we have added between *[…]* more context regarding the quotes.

#### 4.1.1. Value proposition

In this section we zoom in on how data providers create a value proposition for other actors by granting data access control, and how this influences the willingness to grant data access control to data subjects. The value proposition of data providers is directed to two distinct angles: the ecosystem value and user value that is created. Both identified dimensions have a positive effect on the willingness to grant data control to the data subject.

*4.1.1.1. Ecosystem value.* Ecosystem value refers to the benefits created for other stakeholders in the PDE by fostering reciprocity, ensuring data availability, and addressing shared challenges. According to sixteen interviewees, the willingness to grant data access control is influenced by these factors, including the exchange of value, access to high-quality data, and the resolution of common issues within the ecosystem.

Firstly, reciprocity plays a significant role. By granting data access control and enabling users to share data, organizations create value for the ecosystem. This, in turn, encourages other participants to reciprocate, potentially increasing data access for the initial data provider. As one interviewee noted, "*The added value to adding data to a vault would be on data that would be exchangeable. If other actors add data to the vault [by enabling data subject data access control], we can also access their data (…). If we don't enable the sharing of data for users [by enabling data subject data access control], we cannot ask others to enable data sharing with us*"

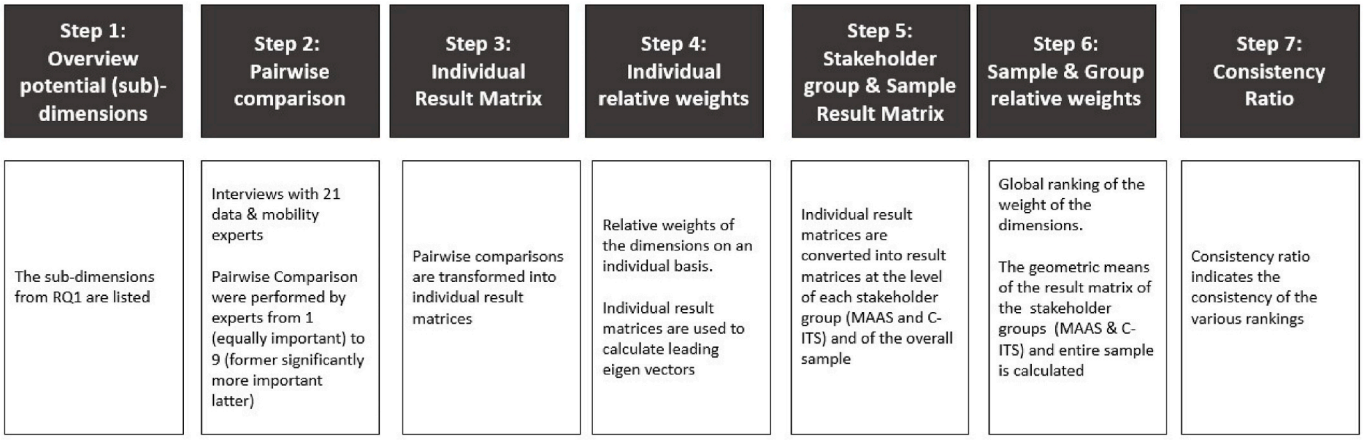



**Fig. 4.** AHP analysis step by step.

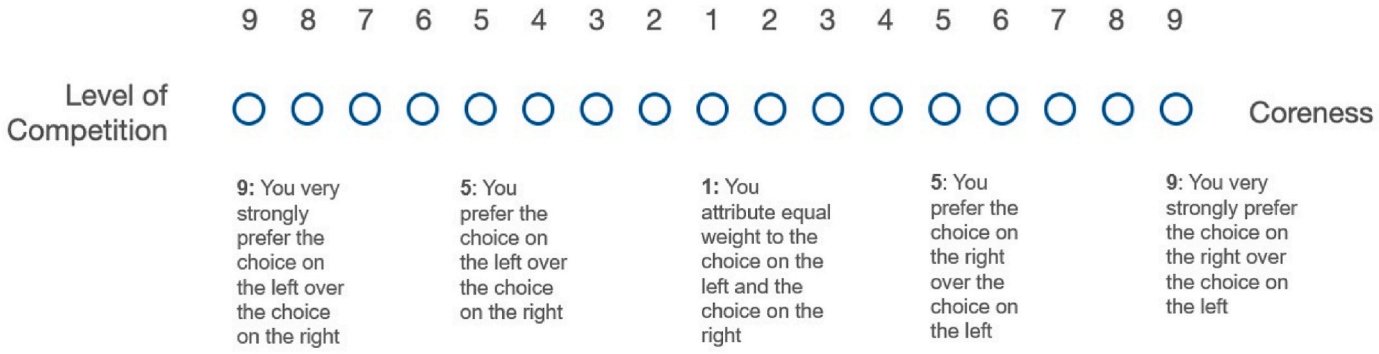



**Fig. 5.** Example of pairwise comparison.

*(Interview 8)*.

Secondly, the use of a PDEs within an ecosystem enhances the availability of high-quality data. The value of the ecosystem is often tied to having up-to-date, accurate data. Allowing users to control data access ensures that high-quality data is available to all participants: *"The paradigm change Solid enables is that we can create a single version of the truth of data [by enabling data subject data access control]. This enables us to store data in one place, close to the citizen, which facilitates data re-use" (Interview 7)*.

Additionally, the ecosystem's value is influenced by the presence or absence of companies willing to address common challenges. By collaborating and creating joint value by enabling data access control, they enable the sharing of data in the ecosystem. One interviewee stated, *"When joining Solid [by enabling data subject data access control], different partners in an ecosystem want to solve a joint issue: improve the relationship with customers and offer a better end-service" (Interview 13)*.

A high ecosystem value positively impacts the willingness to grant data subject access control due to reciprocity, qualitative data in the ecosystem and joined challenges that are being solved in the ecosystem through the sharing of data.

*4.1.1.2. User value.* The user value dimension refers to the benefits of granting data access control for the data subject or user, such as enhancing the customer journey and increasing trustworthiness. According to twenty interviewees, the willingness to grant data access control is strongly influenced by whether it creates user value.

Firstly, the potential improvement in the customer journey is a significant factor. For instance, *"If a user can share his data [by enabling data subject data access control] with different parties with one click of a button, it could dramatically improve the customer journey" (Interview 1)*. In this way, data providers might be more willing to grant data access control as it can strengthen their relationship with data subjects.

Furthermore, PDEs could greatly enhance the trustworthiness of data providers toward data subjects. One interviewee noted, *"We need to give insights into the data and communicate clearly. We need to deserve our role of being trustworthy. These are the fundamentals in our business" (Interview 2)*. As companies want to keep access to data, they currently get access to, this creation of trust is crucial to keep on receiving consent of the user *"Currently we have a high number of consents of the user, and our business model relies on that. We have a challenge to keep the number of consents to the same level as it currently is" (Interview 4)"*.

Overall, high user value positively impacts the willingness to grant data access control, due to improved customer journeys and user trust.

*4.1.2. Value finance*

In this section we zoom in on how value financing is organized by data providers to grant data access control. The value financing of data providers is directed to two distinct angles: value capturing and (costs related to) legal risk. Value capturing has a positive impact on the willingness to grant data access control, legal risk may both have a positive and a negative one.

*4.1.2.1. Value capturing.* The value capturing dimension refers to how data providers can derive benefits through revenue models and cost reduction. Twenty-four interviewees highlighted its importance, emphasizing that value capturing can involve developing innovative revenue models and optimizing processes to lower costs.

First, PDEs facilitate the development of novel revenue models, "*We could generate new income streams by enabling data subjects to share data [and enable data subject data access control], and through data validation*"

(Interview 3). In this case, data providers would enable the data subject to share data by granting data access control, and the data provider could authenticate the validity of the data and get paid for that. Additionally, data providers see granting data access control as an opportunity to develop models where novel data services can be developed on top of data or services they currently offer "W*e can give access to a better API with a longer validity and a better user experience. That way, the company will pay us for extra data provided and a better service." (Interview 2)*. Additionally, data providers could offer added value services on the data generating new incomes "*In our platform, data is stocked in a data vault [enabling data subject data access control], we anonymize the data and offer insights to other companies without including personal data" (Interview 10)*

Furthermore, granting data access control can streamline processes and reduces costs, as data may be available that could make an existing process more efficient: "*Some processes, like sharing official documents with the notary, could be facilitated using data sharing with Solid [by enabling data subject data access control]" (Interview 1)*. Moreover, using certified data in an interoperable PDE ecosystem ensures data validity and reduces administrative processes by minimizing validation steps. "*If you need a driver's license and car attestation for a car insurance, you can just receive a validated document through the PDE. This can* support *existing processes" (Interview 18)*

A high potential for value capturing by developing novel revenue streams and models and by reducing costs streamlining processes positively impacts willingness to grant data access control.

*4.1.2.2. Legal risks.* The legal risk[2] dimension refers to the potential legal compliance costs and associated risks faced by the data provider. This involves the company's assessment of whether granting data access control could impact legal compliance costs related to privacy legislation, potentially posing a financial risk. Eighteen interviewees identified legal risk as a key factor influencing the decision to grant data access control.

Conversely, legal risks could drive the adoption of data access control through PDEs, as they may help ensure compliance with legal requirements if aligned with these regulations. *"European legislations like GDPR and the Data governance act are drivers to look into Solid to simplify the processes and to improve the offering to citizens"* (Interview 11). Companies also perceive granting data access control through a PDE system to reduce legal risk "*As a startup, we cannot guarantee the safety of the data ourselves, and we cannot build systems that are hacker's proof. That is an argument to use a third-party system for personal data*" (Interview 22). Enabling data access control through PDEs may reduce legal risks by minimizing hosted personal data and may lessen data-handling responsibilities, and lower related compliancy costs. "*GDPR is a driver, as the cost to* save *and process data can outsourced to a Solid pod"* (Interview 2).

Granting data access control through a PDE system can mitigate compliance costs and risks, which reduces legal risks, thus positively influencing the decision to grant data access control.

### *4.1.3. Value network*

Turning to the value network dimension, we analyze the impact of the relationship to partners and competitors in the personal data ecosystem. The value network dimension encompasses competition and collaboration. Competition has a negative impact on the willingness to grant data access control, level of collaboration a positive impact. Twenty-three interviewees highlighted the relationship with other organizations in the PDE as a critical consideration, as this determines which company would ultimately gain access to the data.

*4.1.3.1. Collaboration.* The collaboration dimension refers to whether the data providers have a positive or negative collaboration with potential data consumers, such as joined partnerships, allowing data subjects to share their data when granting access control. Eighteen interviewees emphasized that collaboration is a crucial factor in determining the willingness to grant data access control.

As in PDEs data providers grant data access control to data subjects enabling them to share data, the willingness to do so is contingent on the level of partnerships, mutual trust and shared benefits between the companies in the ecosystem. *"Companies will collaborate with each other if they can gain a shared benefit from enabling data subjects to share the data [by enabling data subject data access control*]" *" (Interview 242022)*. Shared strategic goals further facilitate the willingness to enable data exchange by granting data access control, and enable companies to jointly develop services and build a stronger market position: *"Companies can set up strategic partnerships to jointly develop a service and strengthen their market position [by enabling data subject data access control with Solid*]" *" (Interview 15)*.

Collaboration between PDE actors thus has a positive effect on the willingness to grant data access control to data subjects, as data can be shred with (strategic) partners.

*4.1.3.2. Competition.* The competition dimension refers to the level of competition between the data provider and potential data consumers with whom the data subject can share data when granting access control. Twenty-one interviewees noted that competition between data providers and data consumers in the PDE reduces the willingness to grant data access control.

Companies indicated: *"We do not want to strengthen our competitors with our data" (Interview 5)*. They also indicate that there will be limited incentives to share the data with competitors, while it entails significant risks of losing their competitive advantage *"With competitors, we will not share [by enabling data subject data access control] because there will not be a clear business model, and the risk will be too high" (Interview 4)*.

Thus, competition negatively affects the willingness to grant data control to the data subject, as the user can share data with competitors.

### *4.1.4. Value architecture*

Value architecture refers to an organization's core resources and capabilities, which includes the technological infrastructure and organizational infrastructure that allows the provisioning of products and services in addition to information flows. In the case of PDEs, this concerns the personal data they control itself. Therefore, twenty-three respondents consider the competitive nature of the data as a crucial dimension in the decision to grant data access control: "*If data differentiates your business, you will not enable sharing so easily" (Interview 4*). The competitiveness of the data depends on the proximity to the core business and the level of processing.

*4.1.4.1. Coreness.* Coreness refers to how closely data is related to the firm's core operations. For example, transaction data for a bank may be more closely tied to its core business than data on a subject's online behavior. Twenty-one companies noted that if the coreness is high, they may be reluctant to grant access control.

When data is central to the business, companies may be reluctant to grant data access control: "*Some companies have user data on thousands of customers. They use this to offer their services, and they will not easily share this data"* (Interview 16). One of the interviewees also mentioned: *"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). The 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)*.

Data access control is thus less likely to be granted if the data is close

[2] In earlier versions of this work, the dimension now labeled "legal risk" was referred to as "privacy risk," using the same definition. Although "privacy risk" was used in the AHP analysis, the term was revised during the review process to enhance conceptual clarity.

to the core business, as the data is competitive for the company.

*4.1.4.2. Level of processing.* Level of processing refers to the extent to which a company processes data, including the insights generated from it and the level of intellectual property (IP) associated with the processed data. Eighteen interviewees indicated the level of processing as a consideration.

If the company has gathered valuable insights based on the data, they may be reluctant: *"The sensitivity to share [by enabling data subject data access control]" is on the insights we gather on the data"* (Interview 6). Additionally, investments made in data and the development of proprietary algorithms further discourage companies from granting data control*: "If we build in the logic of the data, we will not share this data [by enabling data subject data access control]" because we invested in that" (Interview 9)*. The interviews also revealed that increased data processing leads data providers to regard it as their "'intellectual property"'. For instance, one interviewee emphasized this point, stating, *"It depends on where the IP of the data is [whether we want to enable data subject data access control]. 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)*.

Data access control is thus less likely to be granted if a higher level of processing, as the processed data contains intellectual property, is part of algorithms and if processing investments were high.

### *4.1.5. Proposed business dimensions influencing data access control decision*

As a conclusion to research step one, we propose a set of identified dimensions that influence the willingness to grant data access control, based on expert interviews. Fig. 6 illustrates the business model dimensions that impact data providers' decisions in this regard. The figure also indicates whether each dimension has a positive or negative influence on the decision. The numbers in brackets show how many of the 25 interviewees recognized each dimension as a relevant factor in their decision-making.

## *4.2. Pairwise comparison: data providers preferences to grant data access control in mobility use-cases*

In the following analysis, we assess the significance of various dimensions determined in section 4.1 (as shown in Fig. 6) in determining the willingness to grant data access control. This evaluation is conducted within a mobility PDE use case. We applied the Analytical Hierarchy Process (AHP) method (T. Saaty, 1994) to assign weights to these dimensions, following the step-by-step approach illustrated in the methodology section. The data used in this research can be consulted in the data disclosure section of the publisher's website.

The results of the pairwise comparison, which include the relative weights influencing data providers' decisions within the sample and across groups (as described in Step 5 in Fig. 4), are structured as follows.

- Section 4.2.1 presents the relative weights for the overall sample.
- Section 4.2.2 compares the differing relative weights and rankings between the C-ITS and MAAS sectors.

### *4.2.1. Mobility PDE results*

Table 2 presents the relative weights of data providers' preferences regarding their willingness to grant data access control within the general sample. The table outlines the different business model dimensions and their corresponding relative weights, indicating their importance in the trade-offs data providers consider when making this decision. This is the result of step 5 in Fig. 4, which is calculated by converting into each individual matrix into a sample level matrix. The result matrix of the overall sample can be found in the data disclosure.[3]

The weights are provided for both the sub-dimension level and the dimension levels. A higher percentage reflects a greater perceived importance for that dimension. The general sample consists of 21 respondents, and the results have a consistency ratio of 0,026, well below the 0,1-consistency ratio goal, ensuring reliability. This allows for a clear comparison of the most influential dimensions in the decision-making process, as outlines below.

In the sample, the most decisive business model dimension determining the decision for granting data access control is value finance, explaining 36.35 %. Diving deeper into this dimension, value capturing is the most important sub-dimension overall, accounting for 22.37 %. This concerns the ability of data providers to develop new revenue models and reducing costs when enabling data access control. *"Data access control will be enabled in a mobility ecosystem if value can be captured" (Interview 15b)*. Legal risks influence 13.98 % of the decision, ranked fourth most important sub-dimension, which includes legal compliance costs and data breach risks. *"Being GDPR compliant is crucial to enable users to share in a mobility data ecosystem. Solid could enable that" (Interview 17b)*.

The second most influential dimension concerns the value proposition dimensions, notably impacting the decision with 26 %. End-user value (14.80 %) is the second most important sub-dimension and describes how granting data access control can potentially enhance customer journey and trust. *"Enabling data access control can bring important advantages for the end-user" (Interview 3b)*. This is more influential than ecosystem value (11.15 %, ranked 5th), which involves creating reciprocity and joint data quality within the ecosystem by utilizing a PDE system. *"Even if there would be competition in a mobility ecosystem, enabling the sharing of data would bring a lot of value for the ecosystem" (Interview 11b)*. The mobility ecosystem aims to make data available and enable reciprocity, which is showcased by the emergence of a code of conduct signed by multiple players in the ecosystem which enables a playing level field between MAAS and C-ITS providers *"the code of conduct obliges mobility and MAAS providers to share data about multimodal trip data" (Interview 15b)*.

Third, value architecture contributes 20 % to the decision, which concerns the willingness to grant data access control for data considered competitive. This highlights the reluctance to enable the sharing of data core to the business (14.05 %), which is the third most important consideration of data providers, as "*many players are convinced their data is worth a lot of money. They do not want to share this with others." (Interview 13b)*. In the mobility ecosystem studied, the level of data processing is the least influential of the sub-dimensions, at 5.98 %.

Lastly, the value network dimension influences the decision the least (17.67 %). Data providers in the mobility ecosystem studied show some hesitation in enabling sharing data with competitors (9.49 %), but this is not their primary concern as it is ranked sixth. They place an even lower importance on collaboration (8.18 % ranked 7th) within the mobility ecosystem. This indicates both competition and collaboration do play small a role in mobility ecosystems but are less important than the other sub-dimensions.

### *4.2.2. Mobility use-case comparison*

Table 3 illustrates the sector-based comparison of preference ranking in terms of factors for driving willingness to grant data access control, which involves responses from stakeholders who assessed pairwise comparisons from the perspectives of MAAS (12 participants), compared to C-ITS (8 participants). This is the result of step 5 in Fig. 4, which is calculated by converting into each individual matrix into a MAAS and C-

[3] The disclosed data can be found on the following link https://zenodo.org/records/15004704.

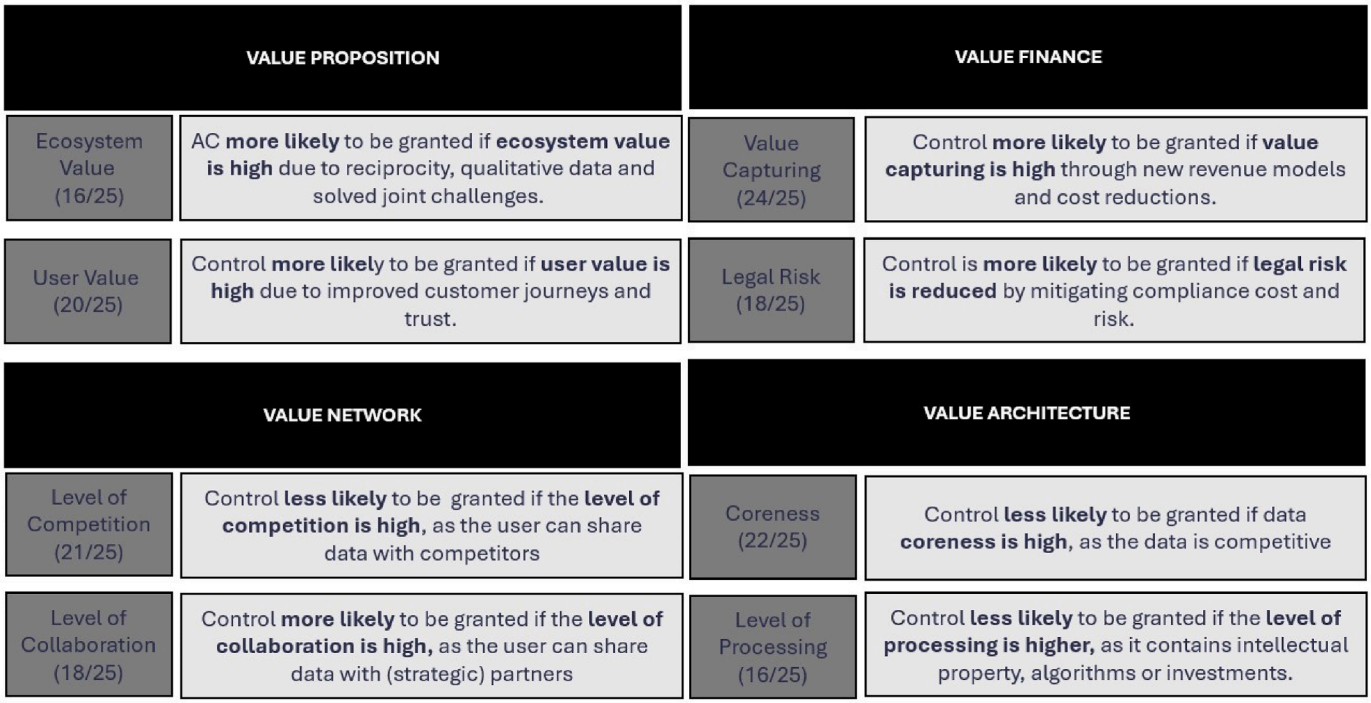



**Fig. 6.** Proposed business dimensions influencing data providers' decisions on granting data access control. The numbers in brackets indicate how many of the 25 interviewees identified each dimension as a factor in their decision-making.

**Table 2**
Aggregated preferences of data to grant access data control (general). The percentages indicate the preferences of the respective business model dimensions and the sub-dimensions. The last column shows the ranking of the sub-dimensions from most important (1) to least important (8). The consistency ratio and number of respondents in the sample are included.

| Data providers' preferences to grant data access control | | | | |
|---|---|---|---|---|
| Value Proposition | 25,95 % | End-User Value | 14,80 % | 2 |
| | | Ecosystem Value | 11,15 % | 5 |
| Value Finance | 36,35 % | Value capturing | 22,37 % | 1 |
| | | Legal Risk | 13,98 % | 4 |
| Value Network | 17,67 % | Competition | 9,49 % | 6 |
| | | Collaboration | 8,18 % | 7 |
| Value Architecture | 20,03 % | Level of Processing Data | 5,98 % | 8 |
| | | Coreness | 14,05 % | 3 |
| Consistency Ratio | 0,026 | | | |
| Respondents | 21 | | | |

**Table 3**
Aggregated preferences of data providers to grant data control in MAAS and C-ITS sectors. The percentages indicate the preferences of the respective dimensions. The consistency ratio and number of respondents in the sample are included.

| Sectoral Comparison of Data providers' preferences to grant data access control | | | | | |
|---|---|---|---|---|---|
| | MAAS | C-ITS | | MAAS | C-ITS |
| Value Proposition | 25,9 % | 24,6 % | Ecosystem Value | 9.8 % | 11.8 % |
| | | | End-User Value | 16.1 % | 12.8 % |
| Value Finance | 35,3 % | 38,8 % | Value Capturing | 21.8 % | 22.1 % |
| | | | Legal Risk | 13.5 % | 16.7 % |
| Value Network | 16,8 % | 18,1 % | Competition | 9.0 % | 10.0 % |
| | | | Collaboration | 7.8 % | 8.1 % |
| Value Architecture | 22 % | 18,6 % | Level of Processing | 4.8 % | 8.2 % |
| | | | Coreness | 17.2 % | 10.4 % |
| Consistency Ratio | 0.050 | 0.045 | | | |
| Respondents | 12 | 8 | | | |

ITS sample level matrix. The result matrix of the MAAS and C-ITS sample can be found in the data disclosure.

Importantly, both groups exhibit consistency ratios below 0.1. Table 4 below illustrates the differences in ranking of the dimensions between the overall-, the MAAS – and C-ITS samples.

Comparing the results from both sectors with the overall sample reveals notable differences in the preferences of data providers for C-ITS and MAAS samples.

The most noteworthy difference is in the salience of the level of value architecture, which is 22 % in the MAAS sample compared to 18.6 % in the C-ITS sample. Diving deeper, the importance of the coreness sub-dimension is strikingly higher in the MAAS group (17.2 % and ranked second) compared to the C-ITS sample (10,4 % and ranked 5th). In a MAAS ecosystem, data is monetized less but is used for the service delivery, thus the willingness to grant data access control depends on the

**Table 4**
Ranking of the dimensions from most important to least important in the overall-, MAAS -, and C-ITS sample. The most significant differences are highlighted in color to emphasize variation between samples. These differences primarily concern end-user value and ecosystem value (light grey), coreness (dark grey) and legal risk (black).

| Overall Sample | | MAAS Sample | | C-ITS Sample | |
|---|---|---|---|---|---|
| Value capturing | 22,37 % | Value Capturing | 21,80 % | Value Capturing | 22,10 % |
| End-user value | 14,80 % | Coreness | 17,20 % | Legal Risk | 16,70 % |
| Coreness | 14,05 % | End-User Value | 16,10 % | End-User Value | 12,80 % |
| Legal Risk | 13,98 % | Legal Risk | 13,50 % | Ecosystem Value | 11,80 % |
| Ecosystem Value | 11,15 % | Ecosystem Value | 9,80 % | Coreness | 10,40 % |
| Competition | 9,49 % | Competition | 9,00 % | Competition | 10,00 % |
| Collaboration | 8,18 % | Collaboration | 7,80 % | Level of Processing | 8,20 % |
| Level of Processing | 5,98 % | Level of Processing | 4,80 % | Collaboration | 8,10 % |

data type based on how core they are to their service delivery *"In MAAS, the sharing of data depends on the data type. If data is more personal, like name, family name or driver's license, users can share it themselves. But sharing data used for the operations of a MAAS operator for ticketing and budgeting will not be enabled. "(Interview 17b)*. On the contrary, in the C-ITS market car manufacturers and location data sellers see data as a revenue generator as they sell data "*Data is close to the core business of the data provider, and thus the willingness to [*grant *data access control] is lower" (Interview 10b)*. Conversely, the level of processing is less important for the MAAS group (4.8 % and ranked last) compared to the C-ITS group (8,2 % and ranked 7th). An interviewee from the C-ITS sample mentioned "*the processed data is our core business. We buy raw free-floating car data and process this data. Thus, we create added value by processing the data and thus do not want to [*grant *data access control] that easily*" *(Interview 9b)*.

Another difference is observed in value proposition dimension (25,9 % in MAAS compared to 24,6 % in C-ITS). However, notable differences occur with the significance of the end-user value (16,1 % ranked 3rd compared to 12,8 % ranked 3rd), while ecosystem value also differs slightly (9,8 % ranked 5th compared to 11,8 % ranked 4th). Thus, end-user value is considered notably more important than ecosystem value in the decision to grant data access control in the MAAS group as *"If a better end-user value is created, more mobility users will make the switch from using cars towards MAAS providers" (Interview 15b)*. In the C-ITS group, this difference between end-user value and ecosystem value is more limited, as *"data providers in C-ITS are not engaging directly with the end-user. They want to create value for other stakeholders in the mobility ecosystem" (Interview 10b)*.

Another notable difference concerns the value finance dimension (35,3 % in MAAS compared to 38,8 % in C-ITS). Value capturing is in both cases the most important factor. Legal risk determines the decision to grant data access control 13.5 % in the MAAS group (ranked fourth) compared to 16 % in the C-ITS group (ranked second), indicating higher risk aversion in the C-ITS group. This is especially the case if data needs to be shared on an individual level as opposed to on an aggregated level *"In the case of C-ITS data, the location data would be shared on an individual level to* e.g. *switch on a traffic light. Sharing data on an individual level would be risky. Usually we work with anonymized, processed car data, in this case legal risk is not such a high concern." (Interview 9b)*.

Concerning value network, no noteworthy differences can be observed.

## 5. Discussion

### 5.1. Business dimensions influencing granting data access control and data sovereignty in PDEs

The link to **research on data sovereignty in PDEs** is centered around adding a business model perspective. The requirement for granting data access control to data subjects in PDEs compel data providers to reassess their business models, balancing the data subject's data sovereignty (Koskinen et al., 2023; Lehtiniemi, 2017) with the need to preserve the company's competitive advantage (Gupta & George, 2016; Kugler & Plank, 2021). By identifying the key dimensions that influence data access control in PDEs (Knaapi-Junnila et al., 2022; Koskinen et al., 2023), it is possible to address the issue of limited data availability in PDEs, which provides insights into challenges literature on PDEs identified (Fallatah et al., 2023; Van Damme et al., 2022).

Whereas partial de jure data sovereignty is enforced through legal frameworks (Solove & Schwartz, 2020), we provide insights into the business dimensions that enable de facto shared data sovereignty in PDEs, which is often complex (Gal & Rubinfeld, 2019; Lam & Liu, 2020; Lauf et al., 2022; Rubinfeld, 2023).This research thus adds insights to PDE research by incorporating a business model perspective highlighting the complex decision-making process for data providers (Al-Debei & Avison, 2010), specifically in a mobility PDE case.

These insights contribute to business model research on data providers, as it show PDEs can enable business models enabling data control in PDEs (Günther et al., 2017; Wiener et al., 2020), and also showcase what business models dimensions data intermediaries can influence to enable data access control (Micheli et al., 2023). These insights further expand on the authors' previously published typology of personal data control configurations in PDEs by introducing a networked business model analytical lens (D'Hauwers & Vandercruysse, 2025). In contrast, their earlier work analyzed these configurations through the resource-based view.

This study adds a data provider perspective by exploring the strategic business model trade-offs in data sovereignty in the context of PDEs. It explores the key dimensions influencing the decision to grant data access control. This provides contributes to data sovereignty literature by expanding on existing research that has identified reference architectures in B2B (Zrenner et al., 2019), B2C settings (Scheider et al., 2023) and data marketplace contexts (Abbas et al., 2024), adding a specific focus on PDEs.

### 5.2. Prioritizing business dimensions affecting granting data access control in a mobility ecosystem

Building on research on data sovereignty in organizational data sharing within mobility ecosystems (Mügge et al., 2023), we highlight that mobility ecosystems require data sovereignty not only for data providers but also for data subjects, extending beyond traditional organizational data sharing frameworks, such as in the context of automotive ecosystems (Jacobs & Singhal, 2020; Rachinger & Müller, 2024). Concretely, we see a shift from physical product ownership to a system of data-driven service use where users keep on contributing data to the service. As such, the part of data exchange that is being taken up by personal data, as opposed to mere manufacturing data (Mügge et al., 2023), can be expected to keep on growing, demanding deeper insight into data provider inclinations with regard to data access control.

Specifically for the **mobility ecosystem**, our research concerns the identification and prioritization of business dimensions determining the willingness to grant data access control. As the progress of mobility ecosystems is hindered by the lack of data sharing between mobility organizations (Pulkkinen et al., 2019; Pütz et al., 2019), this requires data access control by users (Rohunen & Markkula, 2019). By applying the pairwise comparison exercise, we quantified the impact of business model dimensions on the decision of data providers to grant data control to data subjects in a mobility PDE. By quantifying the dimensions identified in RQ1 in the context of mobility, priority levels are given to the trade-off data providers make when granting data access control. In the overall sample, the sub-dimensions value capturing, user value, coreness and legal risk hold the highest importance in the decision for granting data access control, providing insights to how PDE providers need to adapt their business models in a mobility ecosystem by focusing on value creation and legal risk mitigation. By assessing the significance of various dimensions, we identified the key factors that need to be addressed to mitigate limited data sharing between organizations and users in mobility ecosystems, primarily driven by privacy concerns (Kapp et al., 2023; Pulkkinen et al., 2019). These concerns can be managed through data control mechanisms (Hoffmann et al., 2021, pp. 1–6; Rohunen & Markkula, 2019). To the best of the authors' knowledge, this was the first application of AHP to identify business dimensions influencing data access control decisions in PDEs, as well as in the mobility ecosystem.

However, these dimensions hold varying importance in the MAAS and C-ITS sectors, indicating that the preferences differ depending on the sector, especially in the difference between coreness and level of processing, legal risk and user- and ecosystem value. These insights highlight strategies for adapting to increased data use and sharing, which significantly impact how data is used in business models in the mobility ecosystem (Turienzo, 2022; Pépez-Mouré, 2023) with an

important privacy safeguard requirements (Cabanelas, 2023; Constantini, 2017; Armignol et al., 2021).These differences can largely be explained through three differences between the respective business models of actors in the MAAS and C-ITS ecosystems.

First, this is illustrated by the fact that coreness holds much greater salience in the MAAS group (17 %) compared to the C-ITS group (10 %), while the level of processing is more important for the C-ITS group (8 %) than for the MAAS group (4 %). This suggests a different perspective on data management capabilities within the business models of actors in the MAAS and C-ITS sectors, which is a crucial capability within digitalized mobility ecosystems (Turienzo et al., 2023). In MAAS, data sharing depends on the data type. Personal data, like names or driver's license info, can be shared directly, while customer behavior data is closely guarded by providers to protect their competitive advantage (Lukasiewicz et al., 2022). C-ITS involves vast amounts of mobility and service data, with data analytics playing a key role in extracting insights for future applications. Processed data is central to C-ITS providers' business, creating value through data processing. This difference in the types of data perceived as core to their respective business models helps explain the contrasting approaches to data sharing between MAAS and C-ITS.

Second, legal risk was perceived as more significant in the C-ITS group (16.7 %) compared to the MAAS group (13.5 %). MAAS platforms often handle extensive personal data, including users' travel habits and preferences, which requires robust data protection measures to mitigate privacy concerns (Garroussi et al., 2023). C-ITS involves continuous data exchange between vehicles and infrastructure, enabling detailed tracking of individuals' movements. These networks have faced security and privacy attacks (Mahmood et al., 2018), and information exchanged could help adversaries track station behavior (Kountche et al., 2017, pp. 482–486). Consequently, both sectors require secure data collection and privacy measures (Cabanelas, 2023), but in C-ITS systems, this is even more critical than in MAAS ecosystems, apparently making perceived legal risks a more decisive factor for C-ITS.

Third, another key insight is the differing emphasis on end-user value versus ecosystem value between the MaaS and C-ITS sectors. Notable differences arise in the significance placed on end-user value, which is considered more important than ecosystem value in the decision to grant data access control within the MAAS group compared to the C-ITS group. MAAS platforms focus on integrated, user-centric transportation solutions, where data sharing can enhance service personalization and efficiency, inherently prioritizing the user experience (Hensher & Anthony). In contrast, C-ITS solutions are driven by the goal of improving road safety, traffic management, and driver comfort. While user value remains important within C-ITS ecosystems, as indicated by our data, C-ITS is inherently more ecosystem-oriented by nature (Javed et al., 2019; Kang et al., 2023). Both sectors are user- and ecosystem-centric, but their differing focus on user orientation (MAAS) versus ecosystem orientation (C-ITS) likely explains the varying importance of user and ecosystem value in each sector.

These insights suggest that the key dimensions shaping business models for data providers in mobility data ecosystems vary by sector. In MAAS and C-ITS sectors, the most significant differences lie in data processing levels, legal risks, and the emphasis on user versus ecosystem orientation.

## 6. Conclusion

### 6.1. Theoretical contributions

This research enhances the understanding of PDEs and data sovereignty by examining the strategic business dimensions data providers consider when granting data access control to data subjects. The shift toward PDEs presents a trade-off between creating value for data subjects by granting them access control and managing competitive risks, as data subjects may share commercially sensitive information with competitors.

This research addresses the question of what business dimensions influence data providers' willingness to grant data access control to data subjects by integrating a networked business model perspective. By identifying key business dimensions—value proposition (user and ecosystem value), value finance (value capturing and legal risk), value network (collaboration and competition), and value architecture (coreness and data processing level)—this study provides a framework for evaluating data providers' willingness to grant access control.

In the mobility sector, particularly in MAAS and C-ITS, the study highlights sector-specific variations in data-sharing strategies. The findings show that value capturing, end-user value, data coreness, and legal risk are the most influential factors. These differences stem from varying business models, with key distinctions in data processing levels, privacy concerns, and the balance between user-centric and ecosystem-driven approaches. The strategic framework developed in this research offers insights into promoting data sharing by giving users greater control over their data.

### 6.2. Practical implications

This research advances practical knowledge on enabling data sovereignty and strategic decision-making in PDEs, specifically for mobility PDEs.

As earlier IS research highlights the need to further explore how PDEs, with data intermediaries such as PDEs, can sustainably enable digital innovations (Davidson et al., 2023). By identifying the dimensions with the highest leverage for enabling data access control for subjects in PDEs, organizations in PDEs can dynamically shape the ecosystem setup towards granting data access control by influencing value and control dimensions. Regarding value network, the ecosystem constellations and competitor dynamics can be shaped when defining which actors to include in use cases. Value architecture can be managed through data access control mechanisms to mitigate data sensitivity during sharing. Regarding value finance, revenue-sharing models can incentivize grant data access control and promote reciprocity between actors and implementing PDE-based intermediation solutions like Solid can reduce legal risks and compliance costs. Furthermore, the value proposition can be enhanced by introducing new use cases that benefit all stakeholders. Specifically for mobility ecosystems, the analysis indicates that strategies related to value proposition and value finance have the highest leverage in mobility PDEs, followed by measures related to value architecture. Preferences differ across sectors (e.g., C-ITS vs. MAAS), requiring investigating the preferences in distinct ecosystems.

This research can enable data providers to gain insights into their decision to participate in personal data ecosystems and determine whether to grant data access control. The research offers quantifiable business dimensions to assist in strategizing and aligning with company preferences within the (mobility) ecosystem's specific context.

### 6.3. Limitations and further research

A key limitation of this research is the potential restriction on generalizability across different geographies and time periods. This is due to both the exploratory nature of the study and the interview-based methodology, as well as the emerging state of the Solid and mobility ecosystems in Flanders, which involved a limited sample. While the research aimed to provide generalizable insights for data providers considering granting data control, particularly in mobility PDEs, it remained geographically constrained to ensure consistency. The approach focused on participants actively making business decisions about adopting data access control principles adopted in PDEs. Since these principles extend beyond Solid itself, the findings may be relevant to other PDE and/or mobility ecosystems with similar characteristics, particularly those operating under comparable regulatory frameworks,

such as the GDPR. Thus, while the insights are specific to the innovative dynamics of the PDE, Solid and mobility ecosystems in Flanders, they may also apply to other regions with similar legislative and technological conditions. For regions or sectors with different characteristics, this research offers a replicable methodology to generate comparable insights. Additionally, given the early development stage of PDEs, the temporal scope presents another limitation. To address this, future research should replicate the study across various sectors, contexts, and regions. Further studies in Flanders at a later stage would also help assess the long-term evolution of PDEs and their impact.

Second, this study primarily captures the perspectives of data providers, without fully considering the viewpoints of other stakeholders, such as data subjects, data consumers, data intermediaries, and governments. Future studies incorporating multiple stakeholder perspectives would provide a more comprehensive understanding.

Moreover, this study focuses on data sovereignty and access control in PDEs within the mobility sector, specifically in the MAAS and C-ITS sub-sectors. The methodology used to validate the strategic decision-making process for granting data access control can be applied to other sectors and stakeholders. This would help assess the robustness and replicability of these insights in different contexts.

Last, the current conceptual model is static and descriptive, lacking predictive power in guiding strategic decisions for granting data access control. Further research should aim to develop this model into a predictive framework, offering actionable insights. Such a strategic decision framework could validate business models in PDEs and assist in determining strategic fit. Additionally, this research has not examined specific value flows within Solid and PDE ecosystems that enable data access control. Given the high potential influence of the value proposition and value finance dimension, further research should assess the business model impact on existing Solid and PDE initiatives.

## CRediT authorship contribution statement

**Ruben D'Hauwers:** Writing – review & editing, Writing – original draft, Visualization, Software, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Laurens Vandercruysse:** Writing – review & editing, Validation, Supervision, Conceptualization. **Pieter Ballon:** Supervision, Funding acquisition.

## Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author(s) used Chat-GPT 3.5 to enhance the grammar and readability of the text, as well as to assist with programming in R during the data analysis phase. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

## 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).

## Declaration of competing interest

None.

## Annex 1. List of interviewees Solid ecosystem

| Interviewee | Role in Ecosystem | Profile | Date Interview |
|---|---|---|---|
| 1 | Data consumer/provider | Content Expert | 13/06/2022 |
| 2 | Data consumer/provider | C-level | 15/06/2022 |
| 3 | Data consumer/provider | Content Expert | 16/06/2022 |
| 4 | Data consumer/provider | Content Expert | 14/07/2022 |
| 5 | Data consumer/provider | Content Expert | 28/06/2022 |
| 6 | Data consumer/provider | Content Expert | 04/11/2021 |
| 7 | Technology service provider | C-level | 30/06/2021 |
| 8 | Data consumer/provider | Content Expert | 14/10/2021 |
| 9 | Data consumer/provider | Content Expert | 10/11/2021 |
| 10 | Data consumer provider | C-level | 06/07/2022 |
| 11 | Technology service provider | C-level | 07/07/2022 |
| 12 | Ecosystem Level | Content Expert | 12/07/2022 |
| 13 | Technology service provider | Content Expert | 13/07/2022 |
| 14 | Ecosystem Level | C-level | 28/10/2021 |
| 15 | Ecosystem Level | C-level | 15/10/2021 |
| 16 | Data consumer /provider | Content Expert | 08/11/2021 |
| 17 | Data consumer /provider | Content Expert | 27/07/2022 |
| 18 | Technology service provider | C-level | 28/07/2022 |
| 19 | Technology service provider | C-level | 02/08/2022 |
| 20 | Data consumer /provider | Content Expert | 22/10/2022 |
| 21 | Technology service provider | C-level | 04/08/2022 |
| 22 | Data consumer /provider | C-level | 08/08/2022 |
| 23 | Data consumer /provider | Content Expert | 10/08/2022 |
| 24 | Technology service provider | C-level | 11/08/2022 |
| 25 | Technology service provider | C-level | 07/09/2022 |

## Annex 2. List of interviewees AHP analysis

| Interviewee | Sector Perspective | Role Quadruple Helics | Area of Expertise | Date Interview |
|---|---|---|---|---|
| 1b | General | Academic | Data Expert | 07/06/2023 |
| 2b | MAAS | Government | Data Expert | 15/06/2023 |
| 3b | MAAS | Civil Society | Mobility Expert | 15/06/2023 |

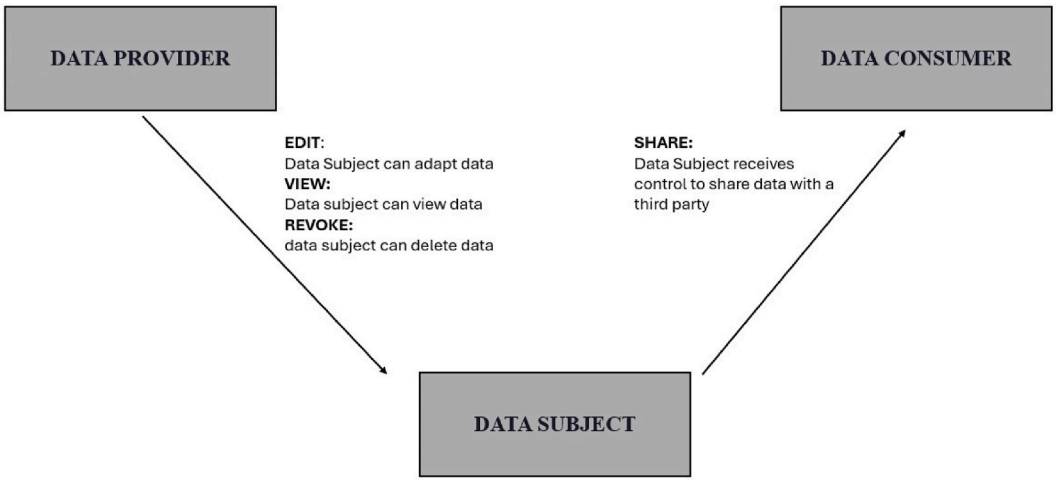
(*continued on next page*)

(*continued*)

| | | | | |
|---|---|---|---|---|
| 4b | MAAS | Government | Mobility Expert | 19/06/2023 |
| 5b | C-ITS | Private company | Mobility Expert | 20/06/2023 |
| 6b | C-ITS | Private company | Mobility Expert | 22/06/2023 |
| 7b | C-ITS | Private company | Mobility Expert | 26/06/2023 |
| 8b | MAAS | Government | Data Expert | 26/06/2023 |
| 9b | C-ITS | Private company | Mobility Expert | 26/06/2023 |
| 10b | C-ITS | Private company | Data Expert | 27/06/2023 |
| 11b | C-ITS | Private company | Data Expert | 27/06/2023 |
| 12b | MAAS | Private company | Data Expert | 28/06/2023 |
| 13b | C-ITS | Private company | Mobility Expert | 28/06/2023 |
| 14b | MAAS | Government | Mobility Expert | 06/07/2023 |
| 15b | MAAS | Private company | Mobility Expert | 06/07/2023 |
| 16b | MAAS | Government | Data Expert | 11/07/2023 |
| 17b | MAAS | Private company | Mobility Expert | 12/07/2023 |
| 18b | C-ITS | Private company | Data Expert | 12/07/2023 |
| 19b | MAAS | Government | Mobility Expert | 20/07/2023 |
| 20b | MAAS | Government | Mobility Expert | 24/07/2023 |
| 21b | MAAS | Private company | Mobility Expert | 02/08/2023 |

## Annex 3. Interview guide interviews Solid Ecosystem

a. What is your role in the company?
b. What are the strategic and contextual drivers for your organization to explore Solid?
c. What role does your company expect to play in the Solid ecosystem?
d. The interviewer explained how Solid can enable granting data access control, by savins data in a pod or vault controlled by the data subject. The data subject would receive editing rights, viewing rights, revoking rights and sharing rights.




e What are drivers and barriers for a company to give editing, viewing, revoking rights to data subjects on their data?
f. For which types of data would a company be willing to give the user editing, viewing and/or revoking rights on their data?
g What are drivers and barriers for a company to receive access to data of third parties of the data subject? What is the top 3 of most valuable data? Would your organization be willing to pay for this data?
h What are drivers and barriers for a company to enable data access control to third parties, so the data subject can choose with whom to share data? Which data with whom would be enabled?

## Data availability

Data has been disclosed

## References

Abbas, A. E., van Velzen, T., Ofe, H., van de Kaa, G., Zuiderwijk, A., & de Reuver, M. (2024). Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. *Electronic Markets, 34*(1), 20. https://doi.org/10.1007/s12525-024-00695-2

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49*, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Adams, W. C. (2015). Conducting semi-structured interviews. In *Handbook of practical program evaluation* (pp. 492–505). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119171386.ch19.

Al-Debei, M. M., & Avison, D. (2010). Developing a unified framework of the business model concept. *European Journal of Information Systems, 19*(3), 359–376. https://doi.org/10.1057/ejis.2010.21

Amponsah, C. T. (2011). Application of multi-criteria decision making process to determine critical factors for procurement of capital projects under public-private

partnerships. *International Journal of the Analytic Hierarchy Process, 3*(2). https://doi.org/10.13033/ijahp.v3i2.121
Andreini, D., Bettinelli, C., Foss, N. J., & Mismetti, M. (2022). Business model innovation: A review of the process-based literature. *Journal of Management & Governance, 26*(4), 1089–1121. https://doi.org/10.1007/s10997-021-09590-w
Anthony, B. (2023). Data enabling digital ecosystem for sustainable shared electric mobility-as-a-service in smart cities-an innovative business model perspective. *Research in Transportation Business & Management, 51*, Article 101043. https://doi.org/10.1016/j.rtbm.2023.101043
Armingol, J. M., Olaverri-Monreal, C., García, F., Milanés, V., & Martín, D. (2018). Cooperative systems for autonomous vehicles. *Journal of Advanced Transportation, 2018*, 1.
Banse, C. (2021). Data sovereignty in the cloud—wishful thinking or reality?. *Proceedings of the 2021 on cloud computing security workshop*. https://doi.org/10.1145/3474123.3486792
Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1041. https://doi.org/10.2307/41409971
Bélanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems, 28*(1), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002
Berg, S. (2006). Snowball sampling—I. In *Encyclopedia of statistical sciences*. John Wiley & Sons, Ltd. https://doi.org/10.1002/0471667196.ess2478.pub2.
Bieker, F. (2022). EU data protection legislation. In F. Bieker (Ed.), *The right to data protection: Individual and structural dimensions of data protection in EU Law* (pp. 13–46). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-503-4_2.
Buyle, R., Taelman, R., Mostaert, K., Joris, G., Mannens, E., Verborgh, R., & Berners-Lee, T. (2020). Streamlining governmental processes by putting citizens in control of their personal data. In A. Chugunov, I. Khodachek, Y. Misnikov, & D. Trutnev (Eds.), *Electronic governance and open society: Challenges in Eurasia* (pp. 346–359). Springer International Publishing. https://doi.org/10.1007/978-3-030-39296-3_26.
Cabanelas, P., Parkhurst, G., Thomopoulos, N., & Lampón, J. F. (2023). A dynamic capability evaluation of emerging business models for new mobility. *Research in Transportation Business & Management, 47*, Article 100964. https://doi.org/10.1016/j.rtbm.2023.100964
Caviglione, L., Podolski, M., Mazurczyk, W., & Ianigro, M. (2016). Covert channels in personal cloud storage services: The case of Dropbox. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2016.2627503, 1–1.
Chen, M. K., & Wang, S.-C. (2010). The critical factors of success for information service industry in developing international market: Using analytic hierarchy process (AHP) approach. *Expert Systems with Applications, 37*(1), 694–704. https://doi.org/10.1016/j.eswa.2009.06.012
Cho, F. (2019). The Saaty AHP and the toy dataset [Computer software] https://cran.r-project.org/web/packages/ahpsurvey/vignettes/my-vignette.html.
Corbin, J., & Strauss, A. (2008). Basics of qualitative research. In *Techniques and procedures for developing grounded theory*. SAGE Publications, Inc. https://doi.org/10.4135/9781452230153
Costantini, F. (2017). *MaaS and GDPR: An overview* (arXiv:1711.02950). *arXiv*. https://doi.org/10.48550/arXiv.1711.02950
Curry, E. (2020). Fundamentals of real-time linked dataspaces. In E. Curry (Ed.), *Real-time linked dataspaces: Enabling data ecosystems for intelligent systems* (pp. 63–80). Springer International Publishing. https://doi.org/10.1007/978-3-030-29665-0_4.
Davidson, E., Wessel, L., Winter, J. S., & Winter, S. (2023). Future directions for scholarship on data governance, digital innovation, and grand challenges. *Information and Organization, 33*(1), Article 100454. https://doi.org/10.1016/j.infoandorg.2023.100454
D'Hauwers, R., & Vandercruysse, L. (2025). Competitive advantage and personal data ecosystems: A typology of personal data control constellations. *Journal of Theoretical and Applied Electronic Commerce Research, 20*(1). https://doi.org/10.3390/jtaer20010008. Article 1.
D'Hauwers, R., Walravens, N., & Ballon, P. (2022). Data ecosystem business models: Value and control in data ecosystems. *Journal of Business Models, 10*(2), 1–30. https://doi.org/10.54337/jbm.v10i2.6946
Digitaal Vlaanderen. (2022). The flemish data utility company. https://www.vlaanderen.be/digitaal-vlaanderen/het-vlaams-datanutsbedrijf/the-flemish-data-utility-company.
Edwards, R., & Holland, J. (2013). *What is qualitative interviewing?* Bloomsbury Academic. https://doi.org/10.5040/9781472545244
Fallatah, K. U., Barhamgi, M., & Perera, C. (2023). Personal data stores (PDS): A review. *Sensors (Basel, Switzerland), 23*(3), 1477. https://doi.org/10.3390/s23031477
Fawcett, S., Osterhaus, Magnan, G., Brau, J., & Mccarter, M. (2007). Information sharing and supply Chain performance: The role of connectivity and willingness. *Supply Chain Management: International Journal, 12*, 358–368. https://doi.org/10.1108/13598540710776935
Fontana, A., & Frey, J. H. (2000). The interview: From structured questions to negotiated text. In *Handbook in qualitative research* (2nd ed., pp. 645–672). Thousand Oaks, CA, London, New Delhi: Sage Publications.
Forman, E., & Peniwati, K. (1998). Aggregating individual judgments and priorities with the analytic hierarchy process. *European Journal of Operational Research, 108*(1), 165–169. https://doi.org/10.1016/S0377-2217(97)00244-0
Fragidis, G. (2017). The user perspective on service ecosystems: Key concepts and models. In L. M. Camarinha-Matos, H. Afsarmanesh, & R. Fornasiero (Eds.), *Collaboration in a data-rich world* (pp. 368–380). Springer International Publishing. https://doi.org/10.1007/978-3-319-65151-4_34.
Frey, R. M. (2017). The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data. *2017 IEEE 16TH International Symposium on network Computing and and applications (NCA), ?(?)*.
Frey, R. M., Bühler, P., Gerdes, A., Hardjono, T., Fuchs, K. L., & Ilic, A. (2017). The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data. *2017 IEEE 16th International Symposium on network computing and applications (NCA)*. https://doi.org/10.1109/NCA.2017.8171385
Gal, M., & Rubinfeld, D. L. (2019). Data standardization (SSRN Scholarly Paper 3326377) https://doi.org/10.2139/ssrn.3326377.
Garroussi, Z., Legrain, A., Gambs, S., Gautrais, V., & Sansò, B. (2023). Data privacy for mobility as a service. *(arXiv:2310.10663). arXiv*. https://doi.org/10.48550/arXiv.2310.10663
Globocnik, D., Faullant, R., & Parastuty, Z. (2020). Bridging strategic planning and business model management – a formal control framework to manage business model portfolios and dynamics. *European Management Journal, 38*(2), 231–243. https://doi.org/10.1016/j.emj.2019.08.005
Gretzel, U., Sigala, M., Xiang, Z., & Koo, C. (2015). Smart tourism: Foundations and developments. *Electronic Markets, 25*(3), 179–188. https://doi.org/10.1007/s12525-015-0196-8
Günther, W. A., Rezazade Mehrizi, M. H., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. *The Journal of Strategic Information Systems, 26*(3), 191–209. https://doi.org/10.1016/j.jsis.2017.07.003
Gupta, M., & George, J. F. (2016). Toward the development of a big data analytics capability. *Information & Management, 53*(8), 1049–1064. https://doi.org/10.1016/j.im.2016.07.004
Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2016). Capturing value from big data – a taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management, 36*(10), 1382–1406. https://doi.org/10.1108/IJOPM-02-2014-0098
Hellmeier, M., & Scherenberg, F. von (2023). *A delimitation of data sovereignty from digital and technological sovereignty. ECIS 2023 Research Papers* (Vol. 18, pp. 1–9). https://aisel.aisnet.org/ecis2023_rp/306.
Hensher, D. A., Mulley, C., & Nelson, J. D. (2021). Mobility as a service (MaaS) – going somewhere or nowhere? *Transport Policy, 111*, 153–156. https://doi.org/10.1016/j.tranpol.2021.07.021
Hoffmann, I., Jensen, N., & Cristescu, A. (2021). Decentralized governance for digital platforms—architecture proposal for the mobility market to enhance data privacy and market diversity. *2021 IEEE 18th Annual consumer Communications & networking Conference (CCNC)*. https://doi.org/10.1109/CCNC49032.2021.9369659
Hummel, P., Braun, M., & Dabrock, P. (2021). Own data? Ethical reflections on data ownership. *Philosophy & Technology, 34*(3), 545–572. https://doi.org/10.1007/s13347-020-00404-9
Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society, 8*(1), Article 2053951720982012. https://doi.org/10.1177/2053951720982012
Iivari, M., Pikkarainen, M., & Koivumäki, T. (2017). How MyData is transforming the business models for health insurance companies. In L. M. Camarinha-Matos, H. Afsarmanesh, & R. Fornasiero (Eds.), *Collaboration in a data-rich world* (pp. 323–332). Springer International Publishing. https://doi.org/10.1007/978-3-319-65151-4_30.
Irion, K. (2012). Government cloud computing and national data sovereignty. *Social Science Research Network*. https://doi.org/10.2139/ssrn.1935859 (SSRN Scholarly Paper 1935859).
Ishizaka, A., & Labib, A. (2011). Review of the main developments in the analytic hierarchy process. *Expert Systems with Applications, 38*(11), 14336–14345. https://doi.org/10.1016/j.eswa.2011.04.143
Jacobs, B. W., & Singhal, V. R. (2020). Shareholder value effects of the volkswagen emissions scandal on the automotive ecosystem. *Production and Operations Management, 29*(10), 2230–2251. https://doi.org/10.1111/poms.13228
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
Javed, M. A., Zeadally, S., & Hamida, E. B. (2019). Data analytics for cooperative intelligent transport systems. *Vehicular Communications, 15*, 63–72. https://doi.org/10.1016/j.vehcom.2018.10.004
Kamargianni, M., & Matyas, M. (2017a). The business ecosystem of mobility-as-a-service. *96th Transportation Research Board Annual Meeting*. https://discovery.ucl.ac.uk/id/eprint/10037890.
Kamargianni, M., & Matyas, M. (2017b). *The business ecosystem of mobility-as-a-service*.
Kang, J., Tak, S., & Park, S. (2023). Analyzing the impact of C-ITS services on driving behavior: A case study of the Daejeon–Sejong C-ITS pilot project in South Korea. *Sustainability (Basel), 15*(16). https://doi.org/10.3390/su151612655. Article 16.
Kapp, A., Nunez von Voigt, S., Mihaljevic, H., & Tschorsch, F. (2023). Towards mobility reports with user-level privacy. *Journal of Location Based Services, 17*(2), 95–121. https://doi.org/10.1080/17489725.2022.2148008
Knaapi-Junnila, S., Rantanen, M. M., & Koskinen, J. (2022). Are you talking to me? – Calling laypersons in the sphere of data economy ecosystems. *Information Technology & People, 35*(8), 292–310. https://doi.org/10.1108/ITP-01-2021-0092
Koskinen, J., Knaapi-Junnila, S., Helin, A., Rantanen, M. M., & Hyrynsalmi, S. (2023). Ethical governance model for the data economy ecosystems. *Digital Policy, Regulation and Governance, 25*(3), 221–235. https://doi.org/10.1108/DPRG-01-2022-0005
Kountche, D. A., Bonnin, J.-M., & Labiod, H. (2017). The problem of privacy in cooperative intelligent transportation systems (C-TIS). *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. https://www.webofscience.com/wos/woscc/full-record/WOS:000418325100082.

Koutroumpis, P., Leiponen, A., & Thomas, L. D. W. (2017). The (unfulfilled) potential of data marketplaces. In *ETLA working papers* (Vol. 53). https://www.etla.fi/wp-content/uploads/etla-working-papers-53.pdf.

Kugler, P., & Plank, T. (2021). Coping with the Double-Edged Sword of Data Sharing in Ecosystems. *Technology Innovation Management Review, 11*(11–12), 5–16. https://doi.org/10.22215/timreview/1470

Lam, W. M. W., & Liu, X. (2020). Does data portability facilitate entry? *International Journal of Industrial Organization, 69*, Article 102564. https://doi.org/10.1016/j.ijindorg.2019.102564

Lauf, F., Scheider, S., Bartsch, J., Herrmann, P., Radic, M., Rebbert, M., … Meister, S.. Linking data sovereignty and data economy: Arising areas of tension. Wirtschaftsinformatik 2022 Proceedings. https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/19/.

Lehtiniemi, T. (2017). Personal data spaces: An intervention in surveillance capitalism? *Surveillance and Society, 15*, 626–639. https://doi.org/10.24908/ss.v15i5.6424

Leidner, D. E., & Tona, O. (2021). The CARE theory of dignity amid personal data digitalization. *MIS Quarterly, 45*(1), 343–370. https://doi.org/10.25300/MISQ/2021/1594

Li, S., & Lin, B. (2006). Accessing information sharing and information quality in supply chain management. *Decision Support Systems, 42*, 1641–1656. https://doi.org/10.1016/j.dss.2006.02.011

Lis, D., & Otto, B. (2020). *Data governance in data ecosystems – insights from organizations*.

Loebbecke, C., van Fenema, P. C., & Powell, P. (2016). Managing inter-organizational knowledge sharing. *The Journal of Strategic Information Systems, 25*(1), 4–14. https://doi.org/10.1016/j.jsis.2015.12.002

Lukasiewicz, A., Sanna, V. S., Diogo, V. L. A. P., & Bernát, A. (2022). Shared mobility: A reflection on sharing economy initiatives in European transportation sectors. In V. Česnuitytė, A. Klimczuk, C. Miguel, & G. Avram (Eds.), *The sharing economy in Europe: Developments, practices, and contradictions* (pp. 89–114). Springer International Publishing. https://doi.org/10.1007/978-3-030-86897-0_5.

Mahmood, A., Zen, H., & Hilles, S. M. S. (2018). *Big data and privacy issues for connected vehicles in intelligent transportation systems* (pp. 1–7). https://doi.org/10.1007/978-3-319-63962-8_234-1

Mehregan, M. (2011). Application of fuzzy analytic hierarchy process in ranking modern educational systems' success criteria. *International Journal of E-Education*. https://doi.org/10.7763/IJEEEE.2011.V1.49. *e-Business, e-Management and e-Learning*.

Micheli, M., Farrell, E., Carballa, S. B., Posada, S. M., Signorelli, S., & Vespe, M. (2023). *Mapping the landscape of data intermediaries*. JRC Publications Repository. https://doi.org/10.2760/261724

Mobilidata. (2023). Gericht rijadvies en intelligente mobiliteit. https://www.mobilidata.be/nl/home.

Moiso, C., & Minerva, R. (2012). Towards a user-centric personal data ecosystem the role of the bank of individuals' data. *2012 16th International Conference on Intelligence in Next generation networks*. https://doi.org/10.1109/ICIN.2012.6376027

Möller, F., Jussen, I., Springer, V., Gieß, A., Schweihoff, J. C., Gelhaar, J., Guggenberger, T., & Otto, B. (2024). Industrial data ecosystems and data spaces. *Electronic Markets, 34*(1), 41. https://doi.org/10.1007/s12525-024-00724-0

Mügge, J., Grosse Erdmann, J., Riedelsheimer, T., Manoury, M. M., Smolka, S.-O., Wichmann, S., & Lindow, K. (2023). Empowering end-of-life vehicle decision making with cross-company data exchange and data sovereignty via Catena-X. *Sustainability (Basel), 15*(9). https://doi.org/10.3390/su15097187. Article 9.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization, 17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Oliveira, S., M, I., Barros Lima, G. de F., & Farias Lóscio, B. (2019). Investigations into data ecosystems: A systematic mapping study. *Knowledge and Information Systems, 61*(2), 589–630. https://doi.org/10.1007/s10115-018-1323-6

Ossadnik, W., Schinke, S., & Kaspar, R. H. (2016). Group aggregation techniques for analytic hierarchy process and analytic network process: A comparative analysis. *Group Decision and Negotiation, 25*(2), 421–457. https://doi.org/10.1007/s10726-015-9448-4

Osterwalder, A., Pigneur, Y., & Tucci, C. L. (2005). Clarifying business models: Origins, present, and future of the concept. *Communications of the Association for Information Systems, 16*(1). https://doi.org/10.17705/1CAIS.01601

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., & Teuscher, S. (2019). *International data spaces association—reference architecture model*. International Data Spaces Association Version 3.0. https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf.

Panian, Z. (2010). Some practical experiences in data governance. https://www.semanticscholar.org/paper/Some-Practical-Experiences-in-Data-Governance-Panian/e908b32d2bf59551f5e322a882aa119ac6ddc44d.

Pérez-Moure, H., Lampón, J. F., Velando-Rodriguez, M.-E., & Rodríguez-Comesaña, L. (2023). Revolutionizing the road: How sustainable, autonomous, and connected vehicles are changing digital mobility business models. *European Research on Management and Business Economics, 29*(3), Article 100230. https://doi.org/10.1016/j.iedeen.2023.100230

Poikola, A., Kuikkaniemi, K., Kuittinen, O., Honki, H., Knuutila, A., & Lähteenoja, V. (2020). MyData – an introduction to human-centric use of personal data, 3rd, Revised edition; p. 57). Mydata.org https://mydata.org/publication/mydata-introduction-to-human-centric-use-of-personal-data/.

Prince, C., Omrani, N., Maalaoui, A., Dabic, M., & Kraus, S. (2023). Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns. *IEEE Transactions on Engineering Management, 70*(10), 3553–3570. https://doi.org/10.1109/TEM.2021.3092702

Pulkkinen, J., Jussila, J., Partanen, A., Trotsk, I., & Laiho, A. (2019). Smart mobility: Services, platforms and ecosystems. *Technology Innovation Management Review, 9*(9), 15–25. https://doi.org/10.22215/timreview/1265

Pütz, F., Murphy, F., Mullins, M., & O'Malley, L. (2019). Connected automated vehicles and insurance: Analysing future market-structure from a business ecosystem perspective. *Technology in Society, 59*, Article 101182. https://doi.org/10.1016/j.techsoc.2019.101182

Rachinger, M., & Müller, J. M. (2024). Investigating a manufacturing ecosystem in transition toward electric vehicles – a business model perspective. *Journal of Manufacturing Technology Management, 35*(9), 24–50. https://doi.org/10.1108/JMTM-07-2023-0279

Ramanathan, R., & Ganesh, L. S. (1995). Energy resource allocation incorporating qualitative and quantitative criteria: An integrated model using goal programming and AHP. *Socio-Economic Planning Sciences, 29*(3), 197–218. https://doi.org/10.1016/0038-0121(95)00013-C

Rantanen, M. M., & Koskinen, J. (2020). Respecting the individuals of data economy ecosystems. In M. Cacace, R. Halonen, H. Li, T. P. Orrensalo, C. Li, G. Widén, & R. Suomi (Eds.), *Well-being in the information society. Fruits of respect* (pp. 185–196). Springer International Publishing. https://doi.org/10.1007/978-3-030-57847-3_13.

Rocca, A. L., & Snehota, I. (2017). Business models in business networks – how do they emerge? *IMP Journal, 11*(3), 398–416. https://doi.org/10.1108/IMP-07-2017-0039

Rohunen, A., & Markkula, J. (2019). On the road – listening to data subjects' personal mobility data privacy concerns. *Behaviour & Information Technology, 38*(5), 486–502. https://doi.org/10.1080/0144929X.2018.1540658

Roloff, J. (2008). Learning from multi-stakeholder networks: Issue-focussed stakeholder management. *Journal of Business Ethics, 82*, 233–250. https://doi.org/10.1007/s10551-007-9573-3

Rubinfeld, D. (2024). Data portability and interoperability: An E.U.-U.S. comparison. *European Journal of Law and Economics, 57*(1), 163–179. https://doi.org/10.1007/s10657-023-09781-w

Saaty, R. W. (1987). The analytic hierarchy process—what it is and how it is used. *Mathematical Modelling, 9*(3), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8

Saaty, T. (1994). How to make a decision—the analytic hierarchy process. *Interfaces, 24*(6), 19–43. https://doi.org/10.1287/inte.24.6.19

Saaty, T. L., & Tran, L. T. (2007). On the invalidity of fuzzifying numerical judgments in the Analytic Hierarchy Process. *Mathematical and Computer Modelling, 46*(7), 962–975. https://doi.org/10.1016/j.mcm.2007.03.022

Sambra, A., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A., & Berners-Lee, T. (2016). Solid: A platform for decentralized social applications based on linked data. https://www.semanticscholar.org/paper/Solid-:-A-Platform-for-Decentralized-Social-Based-Sambra-Mansour/5ac93548fd0628f7ff8ff65b5878d04c79c513c4.

Sanchez-Iborra, R., Bernal-Escobedo, L., & Santa, J. (2020). Eco-efficient mobility in smart city scenarios. *Sustainability (Basel), 12*(20). https://doi.org/10.3390/su12208443. Article 20.

Sarabia-Jácome, D., Lacalle, I., Palau, C. E., & Esteve, M. (2019). Enabling industrial data space architecture for seaport scenario. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 101–106. https://doi.org/10.1109/WF-IoT.2019.8767216

Scerri, S., Tuikka, T., de Vallejo, I. L., & Curry, E. (2022). Common European data spaces: Challenges and opportunities. In E. Curry, S. Scerri, & T. Tuikka (Eds.), *Data spaces: Design, deployment and future directions* (pp. 337–357). Springer International Publishing. https://doi.org/10.1007/978-3-030-98636-0_16.

Scheider, S., Lauf, F., Möller, F., & Otto, B. (2023). A reference system architecture with data sovereignty for human-centric data ecosystems. *Business & Information Systems Engineering, 65*(5), 577–595. https://doi.org/10.1007/s12599-023-00816-9

Schulz, T., Böhm, M., Gewald, H., Celik, Z., & Krcmar, H. (2020). The negative effects of institutional logic multiplicity on service platforms in intermodal mobility ecosystems. *Business & Information Systems Engineering, 62*(5), 417–433. https://doi.org/10.1007/s12599-020-00654-z

Schulz, T., Gewald, H., Krcmar, H., & Wagner, H.-T. (2024). My way, your way, or no way? How mobility-as-a-service ecosystems emerge. *Information Systems and e-Business Management*, 1–44. https://doi.org/10.1007/s10257-024-00691-1

Shahin, A., & Mahbod, M. A. (2007). Prioritization of key performance indicators: An integration of analytical hierarchy process and goal setting. *International Journal of Productivity and Performance Management, 56*(3), 226–240. https://doi.org/10.1108/17410400710731437

Singh, B. C., Carminati, B., & Ferrari, E. (2021). Privacy-aware personal data storage (P-PDS): Learning how to protect user privacy from external applications. *IEEE Transactions on Dependable and Secure Computing, 18*(2), 889–903. https://doi.org/10.1109/TDSC.2019.2903802

Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law* (7th ed. edition). Aspen Publishing.

Spiekermann, M. (2019). Data marketplaces: Trends and monetisation of data goods. *Intereconomics (Baden-Baden), 54*(4), 208–216. https://doi.org/10.1007/s10272-019-0826-z

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K.-L. (2015). The challenges of personal data markets and privacy. *Electronic Markets, 25*(2), 161–167. https://doi.org/10.1007/s12525-015-0191-0

Spiekermann, S., & Novotny, A. (2015). A vision for global privacy bridges: Technical and legal measures for international data markets. *Computer Law & Security Review, 31*(2), 181–200. https://doi.org/10.1016/j.clsr.2015.01.009

Taherdoost, Hamed (2017). Decision Making Using the Analytic Hierarchy Process (AHP); A Step by Step Approach (2017). *International Journal of Economics and Management Systems, 2*. Available at SSRN: https://ssrn.com/abstract=3224206.

Trkman, P., & Desouza, K. C. (2012). Knowledge risks in organizational networks: An exploratory framework. *The Journal of Strategic Information Systems, 21*(1), 1–17. https://doi.org/10.1016/j.jsis.2011.11.001

Tu, Z., Xu, F., Li, Y., Zhang, P., & Jin, D. (2018). A new privacy breach: User trajectory recovery from aggregated mobility data. *IEEE/ACM Transactions on Networking, 26*(3), 1446–1459. https://doi.org/10.1109/TNET.2018.2829173

Turienzo, J., Blanco, A., Lampón, J. F., & Muñoz-Dueñas, M. (2024). Logistics business model evolution: Digital platforms and connected and autonomous vehicles as disruptors. *Review of Managerial Science, 18*(9), 2483–2506. https://doi.org/10.1007/s11846-023-00679-0

Turienzo, J., Cabanelas, P., & Lampón, J. F. (2022). The mobility industry trends through the lens of the social analysis: A multi-level perspective approach. *Sage Open*. https://doi.org/10.1177/21582440211069145

Turienzo, J., Cabanelas, P., & Lampón, J. F. (2023). Business models in times of disruption: The connected and autonomous vehicles (uncertain) domino effect. *Journal of Business Research, 156*, Article 113481. https://doi.org/10.1016/j.jbusres.2022.113481

Van Damme, S., Mechant, P., Vlassenroot, E., Van Compernolle, M., Buyle, R., & Bauwens, D. (2022). Towards a research agenda for personal data spaces: Synthesis of a community driven process. In M. Janssen, C. Csáki, I. Lindgren, E. Loukis, U. Melin, G. Viale Pereira, M. P. Rodríguez Bolívar, & E. Tambouris (Eds.), *Electronic government* (Vol. 13391, pp. 563–577). Springer International Publishing. https://doi.org/10.1007/978-3-031-15086-9_36.

Vandercruysse, L., Dooms, M., & Buts, C. (2021). The DPIA: Clashing stakeholder interests in the smart city?. In D. Hallinan, R. Leenes, & P. De Hert (Eds.), *Data protection and privacy: Enforcing rights in a changing world* (Vol. 14, pp. 245–284) Bloomsbury. http://www.scopus.com/inward/record.url?scp=85186341848&partnerID=8YFLogxK.

Verbrugge, S., Vannieuwenborg, F., Van der Wee, M., Colle, D., Taelman, R., & Verborgh, R. (2021). Towards a personal data vault society: An interplay between technological and business perspectives. *2021 60th FITCE Communication Days Congress for ICT Professionals: Industrial Data – Cloud, Low Latency and Privacy (FITCE), 1–6*. https://doi.org/10.1109/FITCE53297.2021.9588540

Vezyridis, P., & Timmons, S. (2015). On the adoption of personal health records: Some problematic issues for patient empowerment. *Ethics and Information Technology, 17*. https://doi.org/10.1007/s10676-015-9365-x

von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data sovereignty in information systems. *Electronic Markets, 34*(1), 15. https://doi.org/10.1007/s12525-024-00693-4

Walravens, N., & Ballon, P. (2013). Platform business models for smart cities: From control and value to governance and public value. *IEEE Communications Magazine, 51*(6), 72–79. https://doi.org/10.1109/MCOM.2013.6525598. IEEE Communications Magazine.

Weydert, V., Desmet, P., & Lancelot-Miltgen, C. (2019). Convincing consumers to share personal data: Double-edged effect of offering money. *Journal of Consumer Marketing, 37*(1), 1–9. https://doi.org/10.1108/JCM-06-2018-2724

Whittle, A., & Reissner, S. (2025). Making knowledge claims from qualitative interviews: A typology of epistemological modes. *British Journal of Management, 36*(1), 3–16. https://doi.org/10.1111/1467-8551.12845

Wiener, M., Saunders, C., & Marabelli, M. (2020). Big-data business models: A critical literature review and multiperspective research framework. *Journal of Information Technology, 35*(1), 66–91. https://doi.org/10.1177/0268396219896811

Winter, S., Berente, N., Howison, J., & Butler, B. (2014). Beyond the organizational 'container': Conceptualizing 21st century sociotechnical work. *Information and Organization, 24*(4), 250–269. https://doi.org/10.1016/j.infoandorg.2014.10.003

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology, 28*(3), 277–298. https://doi.org/10.1080/13600869.2014.913874

Zhao, J., Zhu, C., Peng, Z., Xu, X., & Liu, Y. (2018). User willingness toward knowledge sharing in social networks. *Sustainability (Basel), 10*(12). https://doi.org/10.3390/su10124680. Article 12.

Zrenner, J., Möller, F. O., 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

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89. https://doi.org/10.1057/jit.2015.5