Designing and Evaluating Control Mechanisms for Sovereign Data Sharing through a Meta-Platform for Data Marketplaces

Abbas, A.E.

DOI
10.4233/uuid:3bc77a9e-7912-4b79-9e86-d0cc3c526785

Publication date
2024

Document Version
Final published version

Citation (APA)
Abbas, A. E. (2024). *Designing and Evaluating Control Mechanisms for Sovereign Data Sharing through a Meta-Platform for Data Marketplaces*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:3bc77a9e-7912-4b79-9e86-d0cc3c526785

Designing and Evaluating Control Mechanisms for Sovereign Data Sharing through a Meta-Platform for Data Marketplaces

Antragama Ewa ABBAS

Designing and Evaluating Control Mechanisms for Sovereign Data Sharing through a Meta-Platform for Data Marketplaces

Dissertation

for the purpose of obtaining the degree of doctor
at Delft University of Technology
by the authority of the Rector Magnificus, Prof.dr.ir. T.H.J.J. van der Hagen,
Chair of the Board for Doctorates
to be defended publicly on
Wednesday 11 September 2024 at 12:30 o’clock

by

Antragama Ewa ABBAS

Master of Science in Information Technology with Business and Management,
University of Sussex, England
born in Banjarmasin, Indonesia

This dissertation has been approved by the promotors.

Composition of the doctoral committee:

Rector Magnificus,	chairperson
Prof.dr.ir. G.A. de Reuver	Delft University of Technology, *promotor*
Dr. A.M.G. Zuiderwijk-van Eijk	Delft University of Technology, *copromotor*

Independent members:

Prof.dr. C. Legner	University of Lausanne
Prof.dr. J. vom Brocke	University of Münster
Prof.mr.dr. J. Wolswinkel	Tilburg University
Prof.mr.dr. J.A. de Bruijn	Delft University of Technology
Prof.dr. Y. Tan	Delft University of Technology

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 871481.

Keywords: Data sharing, Data marketplaces, Meta-platforms, Data sovereignty, Control Mechanisms, Smart contracts, Certifications, Data Economy, Design Science Research

Printed by Gildeprint
Cover by Anni Naimah

ISBN: 978-94-6366-904-7
An electronic version of this dissertation is available at https://repository.tudelft.nl/

Table of contents

List of figures

List of tables

Summary

Imagine you are a credit risk analyst at a bank. Your job is to accept or reject individual credit applications. Your current data-driven credit risk assessment model relies heavily on traditional financial metrics such as credit history, income levels, and existing debts. However, this model has limitations, especially in accurately assessing applicants without extensive credit histories. Consequently, you find yourself rejecting many applications due to this lack of comprehensive insight, resulting in a low approval rate that contributes to low financial inclusion. You realize that improving your credit risk assessment model requires analyzing external data. You could conduct a data sharing partnership with other businesses, such as telecom operators. However, your past experiences remind you that agreeing on technology, contracts, and approaches for data sharing could take twelve to eighteen months, making you hesitant.

But this is an old story. Nowadays, you can simply visit a data marketplace to find the necessary data outside your company. Picture it as an Amazon.com but focused on data products. Here, you can use various types of data products from other businesses. For example, you are now interested in using telecommunication data (e.g., subscription, usage, and billing patterns) to build a better credit risk assessment model. By doing so, your approval rate ends up increasing to 35%, and you are satisfied.

Motivation and relevance

You need other companies to share their data, and you are not alone. The expanding *data economy*, the ecosystem driven by collecting, processing, and sharing data for economic and societal gains, motivates businesses to utilize *data marketplaces* for sharing data products with external parties. Due to the specialized nature of data products, data marketplaces exhibit a high degree of heterogeneity, often focusing on specific countries and industries. This high heterogeneity also indicates substantial variations across multiple aspects of data marketplaces, such as business models, governance arrangements, and technical standards. The heterogeneity increases the transaction costs of data sharing. Additionally, the heterogeneity results in high multi-homing costs, deterring users from joining multiple marketplaces and thus limiting their expansion opportunities. The high degree of heterogeneity will likely persist, limiting the growth of the data economy.

Meta-platforms can reconcile the high degree of heterogeneity in data marketplaces. They are particularly beneficial in reducing transaction and multi-homing costs. Meta-platform is a platform designed to operate atop two or more existing platforms, thereby connecting their respective ecosystems. For example, Trivago serves as a meta-platform in the tourism sector, while Expedia, Booking, and Airbnb act as participating platforms. However, in the data sharing context, a meta-platform for data marketplaces complicates *data sovereignty* (i.e., self-determination of data providers to control data), as data may flow from one data marketplace to another.

To reduce sovereignty concerns, meta-platform operators can implement *control mechanisms* (e.g., smart contracts and certifications) to influence the behavior of data consumers; however, the design of such mechanisms in the complex meta-platform setting is unexplored. If data providers perceive these control mechanisms as less valuable within the meta-platform context, both sovereignty and heterogeneity issues remain unresolved, constraining the growth of the data economy. Taken together, platform operators are unsure how to design control mechanisms for enhancing data sovereignty in a meta-platform for data marketplaces.

Meta-platforms that federate data marketplaces are examined within the intersection of the data sharing and digital platform literature. Considering the data sharing literature, meta-platforms for data marketplaces differ from the conventional ones (e.g., gaming platforms), mainly because data products are a) experience goods whose quality or value cannot be fully evaluated prior to purchase, b) usable by multiple parties at once without diminishing availability, and c) easily duplicable. Consequently, what meta-platforms are in the data marketplace setting remains unclear, especially how they create value *(scientific gap 1).* At the same time, the current digital platform literature has yet to address unique challenges data sharing platforms face, such as data sovereignty. This means there is a lack of clarity about data sovereignty conceptualization, especially in the context of the meta-platform *(scientific gap 2).* The digital platform literature utilizes control mechanisms to tackle platform-related challenges. However, current research mainly concentrates on single and traditional platforms, neglecting the study of data sharing platforms federated by a meta-platform. Furthermore, the literature on digital platforms does not address sovereignty concerns. This leads to a limited understanding of design principles (the "how") and instantiations (the "what") of such mechanisms to address data sovereignty *(scientific gap 3).* Finally, given the ultimate societal relevance to contributing to the growth of the data economy, clarifying sovereignty impacts on the data economy is essential, but such knowledge is scarce *(scientific gap 4).* In all, there is a pressing need to create design knowledge for developing and evaluating control mechanisms in the context of meta-platforms for data marketplaces. Addressing these scientific gaps is crucial for enhancing data sovereignty in meta-platforms for data marketplaces, a vital factor in the growth of the data economy.

Research objective, approach, and questions

This research aims to create design knowledge for developing and evaluating control mechanisms through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy. To achieve the objective, this study employs the Design Science Research (DSR) approach. This study is structured based on the three DSR domains: the problem space, the solution space, and the evaluation space. Each domain has different research questions, which are described below.

- *Problem space*
    - *Research question 1 (Context exploration): How do meta-platforms create value in the data marketplace setting?*
      We investigated how meta-platforms create value in the data marketplace setting, addressing a design knowledge gap of meta-platforms as a context in which the data sovereignty concerns occur (scientific gap 1). Context understanding guided the further exploration of design knowledge across the problem, solution, and evaluation domains. To answer research question 1, we conducted an exploratory qualitative study comprising two steps: 1) conceptual framing and 2) semi-structured interviews. In the first step, we used the holon and holarchy lens to structure meta-platforms. In the second step, we conducted semi-structured interviews to explore meta-platform value creation archetypes.

    - *Research question 2 (Goodness criteria): What are the key facets of data sovereignty in data sharing through meta-platforms for data marketplaces?*
      We examined what data sovereignty is in the complex meta-platform setting. This inquiry is vital due to the prevalent ambiguities surrounding data sovereignty, signifying a design knowledge gap for specifying goodness criteria (scientific gap 2). By exploring the key facets of data sovereignty, this research laid the groundwork in the problem space domain, which then informs the solution and evaluation domains. To address this question, we employed an exploratory qualitative approach comprising 1) conceptual framing and 2) semi-structured interviews. In the first step, we contextualized social contract theory to data sovereignty. In the second step, we conducted semi-structured interviews to examine the substantive aspect of data sovereignty (i.e., the Three PS: Protection, Provision, and Participation).

- *Solution space*
    - *Research question 3 (Design options): What control mechanisms can enhance data sovereignty in data sharing via a meta-platform for data marketplaces?*
      We narratively reviewed control mechanisms to enhance data sovereignty. Currently, a clear overview of such control mechanisms is lacking. Without such an overview, we risk overlooking appropriate mechanisms as design options that can fulfill the goodness criteria of data sovereignty.

    - *Research question 4 (Design principles and a prototype): What do the developed control mechanisms look like in the meta-platform setting?*
      To answer this question, we adapted a common prototyping approach in design science research that consists of four steps: 1) specifying meta-requirements, 2) identifying design principles, 3) developing design features (or interfaces), and 4) evaluating the prototype. Answering this question addressed a design

knowledge gap of design principles (the "how") and instantiations of control mechanisms in meta-platforms (the "what") (scientific gap 3).

- *Evaluation space*
    - *Research question 5 (Solution evaluation): To what extent do data providers perceive that the control mechanisms enhance data sovereignty for data sharing through a meta-platform for data marketplaces?*
      We evaluated the perceived efficacy of control mechanisms (i.e., smart contracts and certifications) to enhance data sovereignty in a meta-platform for data marketplaces. We asked this question to know whether our proposed mechanisms align with the expectations of data providers as the problem owners of sovereignty concerns. Additionally, this evaluation helped us reflect on the design knowledge we formulated in the problem and solution spaces. To address this question, we conducted a between-subject 2x2 factorial experiment based on the presence of smart contracts and certifications.

    - *Research question 6 (Impact evaluation): How does data sovereignty impact the data economy?*
      We evaluated the impacts of data sovereignty on the broader societal context of the data economy. Addressing this research question helps to clarify and explain the presumed necessity of data sovereignty for the data economy's growth (scientific gap 4). By drawing from theories on trust and risk, we employed Partial Least Squares Structural Equation Modelling to establish a nomological network of data sovereignty.

Key findings

We find that data providers have different views on the efficacy of control mechanisms (i.e., smart contracts and certifications) to enhance data sovereignty facets in the context of business data sharing via data marketplace constellations federated by a meta-platform. Our research finds no significant differences in data providers' perception of their ability to *retain ownership* and *maintain control over shared data products* in meta-platforms, regardless of the presence of smart contracts. In addition, our findings suggest that data providers using meta-platforms with certifications feel more confident in *meeting data sharing compliance requirements* compared to those using meta-platforms without certifications. Additionally, these data providers perceive a *clearer division of responsibility* between meta-platform and data marketplace operators. When combined with smart contracts, the responsibility divisions become even clearer. Contrary to our expectations, however, we find no significant difference in the *perceived security* of data providers when sharing data on meta-platforms with certifications compared to those without.

Considering the impacts of data sovereignty on the broader societal context of the data economy, we find that when data providers feel sovereign over their data products, they are more likely to trust both a) meta-platform operators facilitating data sharing and b) data consumers with whom they share data. Surprisingly, we do not identify a correlation between the trust and their willingness to share data. This suggests that when data providers possess data sovereignty, trust in platform operators and data consumers becomes a less important factor for data sharing. In addition, we discover that data providers, feeling sovereign over their data products, perceive lower risks in sharing their data. The reduced perceived risks subsequently increase their willingness to share data through meta-platforms. Therefore, our study emphasizes the significance of data sovereignty in the growth of the data economy by a) promoting trust toward meta-platform operators and data consumers, b) reducing perceived risks, and c) increasing the willingness to share business data through meta-platforms.

Conclusion

Our study contributes to the Information Systems literature, particularly in the intersection between data sharing and digital platform literature. We contribute by being among the first to create design knowledge to develop and evaluate control mechanisms for business data sharing through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy. Specifically, our primary contributions are four-fold: 1) theorizing the potential impact of control mechanisms on data sovereignty, 2) outlining design options and principles as prescriptive knowledge, 3) defining goodness criteria to enhance data sovereignty, and 4) advancing context understanding of a meta-platform as a business data sharing setting. In addition, our secondary contributions are 1) providing evidence on the potential impact of data sovereignty on the broader data economy and 2) extending the applicability of theories employed in this research in the market-based data sharing context.

In conclusion, this study resolves the tensions in the European policy-making agendas that promote a single market for data and interoperable data sharing (e.g., in EU Data strategy, Data Act) while, at the same time, pushing sector-specific data marketplaces to exist (e.g., the eight verticals in the Digital Europe program). Furthermore, policy agendas also emphasize adherence to data sovereignty principles. As data sovereignty is vital for data providers to share their data via meta-platforms, addressing this concern may increase meta-platform adoptions. Hence, we hope a meta-platform can realize its potential to be one distinguished instrument to fulfill what we hope (and are optimistic) for in the data economy: a single European Data Market in 2030.

Samenvatting

Beeld je in dat je een kredietscore-analist bent bij een bank. Het is jouw taak om individuele kredietaanvragen te accepteren of af te wijzen. Het datagedreven beoordelingsmodel voor kredietscores dat je gebruikt is grotendeels gebaseerd op traditionele financiële meeteenheden zoals kredietgeschiedenis, inkomensniveaus en uitstaande schulden. Dit model heeft zijn beperkingen, vooral wanneer aanvragen zonder lange kredietgeschiedenis accuraat beoordeeld moeten worden. Je merkt dat je veel aanvragen afwijst vanwege dit gebrek aan volledige inzichten, resulterend in een laag acceptatiecijfer dat op zichzelf weer bijdraagt aan beperkte financiële inclusie. Je realiseert je dat externe data nodig is om het beoordelingsmodel van kredietscores te verbeteren. Je kunt een samenwerking met andere bedrijven, zoals telecomproviders, opzetten voor het delen van data. Maar je bent terughoudend omdat je uit eerdere ervaringen weet dat het twaalf tot achttien maanden kan duren voordat je overeenstemming bereikt over de technologie, contracten en manieren om data te delen.

Maar dit is een gedateerd verhaal. Tegenwoordig kun je de benodigde, externe data gemakkelijk vinden op een datamarktplaats. Denk aan een soort Amazon.com maar dan voor dataproducten. Je kunt hier verschillende soorten dataproducten van andere bedrijven gebruiken. Je bent bijvoorbeeld geïnteresseerd in telecommunicatiedata (bijv. abonnementen, gebruik en patronen in rekeningen) om het beoordelingsmodel voor kredietscores te verbeteren. Door deze data te gebruiken stijgt het aantal goedkeuringen tot 35 procent en ben je tevreden met het model.

Aanleiding en relevantie

De uitbreidende *dataeconomie,* het ecosysteem dat wordt gedreven door het verzamelen, verwerken en delen van data voor economisch en maatschappelijk nut, stimuleert bedrijven om *datamarktplaatsen* te gebruiken waar data met externe partijen wordt gedeeld. Vanwege het gespecialiseerde karakter van dataproducten vertonen datamarktplaatsen een hoge mate van heterogeniteit, waarbij ze zich vaak richten op specifieke landen en industrieën. Deze grote heterogeniteit duidt ook op substantiële verschillen tussen meerdere aspecten van datamarktplaatsen, zoals bedrijfsmodellen, governanceregelingen en technische standaarden. De heterogeniteit verhoogt de transactiekosten van het delen van data. Bovendien resulteert de heterogeniteit in hoge kosten voor multi-homing, waardoor gebruikers ervan worden weerhouden zich bij meerdere marktplaatsen aan te sluiten en zo hun uitbreidingsmogelijkheden te beperken. De hoge mate van heterogeniteit zal waarschijnlijk blijven bestaan, waardoor de groei van de data-economie wordt beperkt.

Metaplatforms kunnen de hoge mate van heterogeniteit op datamarktplaatsen aanpakken. Ze zijn met name nuttig bij het verlagen van de transactie- en multi-homingkosten. Een metaplatform is een platform ontworpen om boven twee of meer bestaande platformen te opereren, waarmee hun respectievelijke ecosystemen worden verbonden. Trivago, bijvoorbeeld, dient als metaplatform voor de toerismesector, waar Expedia, Booking en Airbnb de deelnemende platformen zijn. Maar in de context van het delen van data compliceert een metaplatform voor datamarktplaatsen *datasoevereiniteit* (d.w.z. zelfbeschikking van data-aanbieders over hun data) omdat data van de ene naar de andere marktplaats kan vloeien.

Om soevereiniteitsbezwaren te verminderen, kunnen metaplatformexploitanten controlemechanismen, zoals smart contracts en certificering, inzetten om het gedrag van datagebruikers te beïnvloeden. Echter, het ontwerp van dit soort mechanismen in de complexe context van metaplatformen is nog niet verkend. Als data-aanbieders deze controlemechanismen minder waardevol vinden in een metaplatformcontext blijven problemen met zowel soevereiniteit als fragmentatie onopgelost, wat de groei van de dataeconomie beperkt. Alles bij elkaar is het voor data-aanbieders onduidelijk hoe ze controlemechanismen voor het versterken van datasoevereiniteit in een metaplatform voor datamarktplaatsen moeten vormgeven.

We hebben metaplatformen die datamarktplaatsen aan elkaar verbinden onderzocht vanuit de intersectie van de literatuur over het delen van data en digitale platformen. Volgens de literatuur over het delen van data verschillen metaplatformen voor datamarktplaatsen vooral van conventionele platformen (bijv. gameplatformen) omdat dataproducten a) ervaringsgoederen zijn waarvan de kwaliteit of de waarde niet volledig kan worden bepaald voorafgaand aan de aankoop, b) door meerdere partijen tegelijk gebruikt kunnen worden zonder dat de beschikbaarheid wordt beperkt en c) gemakkelijk te vermenigvuldigen zijn. Daarom is het onduidelijk wat metaplatformen zijn in de setting van datamarktplaatsen en voornamelijk hoe ze daar waarde creëren (*wetenschappelijke kennislacune 1*). Tegelijkertijd moet de huidige literatuur over digitale platformen de unieke uitdagingen van platformen voor datadeling, zoals datasoevereiniteit, nog adresseren. Dit betekent dat er onduidelijkheid bestaat over de conceptualisering van datasoevereiniteit, voornamelijk als het gaat over metaplatformen (*wetenschappelijke kennislacune 2*). In de literatuur over digitale platformen worden controlemechanismen gebruikt om uitdagingen gerelateerd aan platformen aan te pakken. Het huidige onderzoek concentreert zich echter voornamelijk op traditionele en op zichzelf staande platformen. Daarmee worden platformen voor datadeling die bij elkaar worden gebracht door metaplatformen niet bestudeerd. Daarnaast stelt de literatuur over digitale platformen datasoevereiniteit niet aan de orde. Dit leidt tot beperkt begrip van ontwerpprincipes (het “hoe”) en hun uitwerking (het “wat”) van dit soort mechanismen om datasoevereiniteit te adresseren (*wetenschappelijke kennislacune 3*). Ten slotte, uitgaande van de uiteindelijke maatschappelijke relevantie van bijdragen aan de groei van de dataeconomie, is het essentieel om de effecten van soevereiniteit op de dataeconomie te verhelderen (*wetenschappelijke kennislacune 4*). Alles samengenomen blijkt er behoefte te zijn aan het creëren van ontwerpkennis voor het ontwikkelen en evalueren van controlemechanismen in de context van metaplatformen voor datamarktplaatsen. Het behandelen van deze wetenschappelijke lacunes is cruciaal voor het versterken van datasoevereiniteit in metaplatformen voor datamarktplaatsen, een vitale factor in de groei van de dataeconomie.

Onderzoeksdoel, -aanpak en -vragen

Dit onderzoek richt zich op het creëren van ontwerpkennis voor het ontwikkelen en evalueren van controlemechanismen via metaplatformen voor datamarktplaatsen, met een focus op de doeltreffendheid van deze mechanismen in het versterken van datasoevereiniteit in de maatschappelijke context van de dataeconomie. Om dit doel te bereiken past deze studie een *Design Science Research* (DSR) aanpak toe. De studieopzet is gebaseerd op de drie DSR-domeinen: de probleemruimte, de oplossingsruimte en de evaluatieruimte. Hieronder worden de onderzoeksvragen beschreven die bij elk domein horen.

- <u>*Probleemruimte*</u>
    - *Onderzoeksvraag 1 (Contextverkenning): Hoe creëren metaplatformen waarde in datamarktplaatscontext?*

      We hebben onderzocht hoe metaplatformen waarde creëren in de datamarktplaatscontext. Daarmee pakken we een ontwerpkennislacune over metaplatformen als een context waarin zorgen rondom datasoevereiniteit bestaan aan (wetenschappelijke kennislacune 1). Begrip van de context heeft de verdere verkenning van ontwerpkennis in het probleem-, de oplossings- en de evaluatiedomeinen gestuurd. Om onderzoeksvraag 1 te beantwoorden, hebben we een exploratieve, kwalitatieve studie bestaande uit twee stappen uitgevoerd: 1) conceptuele kaderstelling en 2) semigestructureerde interviews. In de eerste stap hebben we een *holon and holarchy lens* gebruikt om metaplatformen te structureren. In de tweede stap hebben we semigestructureerde interviews uitgevoerd om archetypes van waardecreatie viametaplatformen te verkennen.

    - *Onderzoeksvraag 2 (goodness criteria): Wat zijn de voornaamste facetten van datasoevereiniteit bij het delen van data via metaplatformen voor datamarktplaatsen?*

      We hebben onderzocht wat datasoevereiniteit is in de complexe metaplatformcontext. Dit onderzoek is nodig vanwege de heersende ambiguïteiten rondom datasoevereiniteit die duiden op een ontwerpkennislacune betreffende het specificeren van *goodness* criteria (wetenschappelijke kennislacune 2). Door het verkennen van de voornaamste facetten van datasoevereiniteit heeft dit onderzoek het fundament gelegd in het probleemdomein, wat vervolgens gebruikt wordt in het oplossings- en evaluatiedomein. Om deze onderzoeksvraag te beantwoorden hebben we een exploratieve, kwalitatieve aanpak gebruikt bestaande uit 1) conceptuele inkadering en 2) semigestructureerde interviews. In de eerste stap hebben we sociale contracttheorie toegepast op datasoevereiniteit. In de tweede stap hebben we semigestructureerde interviews uitgevoerd om de inhoudelijke aspecten van datasoevereiniteit (d.w.z. de drie p’s: *protection*, *provision* en *participation*) te onderzoeken.

- *Oplossingsruimte*
    - *Onderzoeksvraag 3 (ontwerpopties): Welke controlemechanismen kunnen datasoevereiniteit bij het delen van data via een metaplatform voor datamarktplaatsen versterken?*
      We hebben controlemechanismen om datasoevereiniteit te versterken beschrijvend beoordeeld. Op dit moment ontbreekt er een duidelijk overzicht van dit soort controlemechanismen. Zonder zo'n overzicht riskeren we geschikte mechanismen als ontwerpopties die *goodness* criteria voor datasoevereiniteit kunnen vervullen, over het hoofd te zien.

    - *Onderzoeksvraag 4 (ontwerpprincipes en een prototype): Hoe zien de ontwikkelde controlemechanismen eruit in een metaplatformcontext?*
      Om deze vraag te beantwoorden hebben we een gebruikelijke aanpak voor prototypering in *Design Science Research* gebruikt die bestaat uit vier stappen: 1) specificeren van metavereisten, 2) identificeren van ontwerpprincipes, 3) ontwikkeling van ontwerpfeatures (of interfaces) en 4) evalueren van het prototype. Met het beantwoorden van deze vraag is een ontwerpkennislacune over ontwerpprincipes (het "hoe") en de uitwerking van controlemechanismen in metaplatformen (het "wat") aangepakt (wetenschappelijke kennislacune 3).

- *Evaluatieruimte*
    - *Onderzoeksvraag 5 (oplossingsevaluatie): In hoeverre ervaren data-aanbieders dat de controlemechanismen hun datasoevereiniteit voor het delen van data via een metaplatform voor datamarktplaatsen versterken?*
      We hebben de bevonden doeltreffendheid van controlemechanismen (d.w.z. smart contracts en certificering) om datasoevereiniteit in een metaplatform voor datamarktplaatsen te vergroten geëvalueerd. We hebben deze vraag gesteld om te begrijpen of de door ons voorgestelde mechanismen overeenkomen met de verwachtingen van data-aanbieders als de probleemeigenaren van de zorgen over soevereiniteit. Bovendien heeft deze evaluatie ons geholpen om te reflecteren op de ontwerpkennis die we hebben geformuleerd in het probleemdomein en het oplossingsdomein. Om deze vraag te beantwoorden hebben we een *between-subject 2x2 factorial experiment* uitgevoerd gebaseerd op de aanwezigheid van smart contracts en certificering.

    - *Onderzoeksvraag 6 (impactevaluatie): Hoe beïnvloedt datasoevereiniteit de dataeconomie?*
      We hebben de effecten van datasoevereiniteit op de bredere maatschappelijke context van de dataeconomie geëvalueerd. Het beantwoorden van deze vraag helpt bij het verduidelijken en uitleggen van de veronderstelde noodzakelijkheid

van datasoevereiniteit voor de groei van de dataeconomie (wetenschappelijke kennislacune 4). Met gebruik van theorieën over vertrouwen en risico hebben we *Partial Least Squares Structural Equation Modelling* gebruikt om een *nomological network* van datasoevereiniteit op te stellen.

Voornaamste bevindingen

Het blijkt dat data-aanbieders verschillende opvattingen hebben over de doeltreffendheid van controlemechanismen (d.w.z. smart contracts en certificering) om datasoevereiniteitfacetten te versterken in de context van het delen van bedrijfsdata via datamarktplaatsconstellaties die worden samengebracht door een metaplatform. Ons onderzoek toont geen significant verschil aan tussen de perceptie van data-aanbieders over hun vermogen om *eigenaarschap te behouden* en over hun vermogen om *controle over gedeelde dataproducten te behouden*, ongeacht de aanwezigheid van smart contracts. Bovendien suggereren onze bevindingen dat data-aanbieders die metaplatformen met certificering gebruiken zekerder zijn van het *behalen van compliance vereisten voor datadelen* vergeleken met aanbieders die metaplatformen zonder certificering gebruiken. Daarbij bemerken deze data-aanbieders een *duidelijkere verdeling van verantwoordelijkheid* tussen metaplatform- en datamarktplaatsexploitanten. Wanneer deze worden gecombineerd met smart contracts, worden deze verdelingen van verantwoordelijkheid zelfs duidelijker. Hoewel we tegengestelde verwachtingen hadden, hebben we geen significante verschillen gevonden in de *ondervonden veiligheid* van data-aanbieders wanneer zij data delen via metaplatformen met of zonder certificering.

Gezien de effecten van datasoevereiniteit op de bredere maatschappelijke context van de dataeconomie zien we dat wanneer data-aanbieders soevereiniteit over hun dataproducten ervaren, zij eerder geneigd zijn om vertrouwen te hebben in zowel a) metaplatformexploitanten die datadelen faciliteren als b) dataconsumenten met wie data wordt gedeeld. Verrassend genoeg hebben we geen correlatie tussen dit vertrouwen en de bereidheid van data-aanbieders om data te delen gevonden. Dit suggereert dat wanneer data-aanbieders soevereiniteit over hun data hebben, het vertrouwen in platformexploitanten en dataconsumenten een minder belangrijke factor wordt voor datadelen. Bovendien hebben we ontdekt dat data-aanbieders, die datasoevereiniteit over hun dataproducten ervaren, minder risico's zien in het delen van hun data. De daling in ervaarde risico's verhoogt vervolgens hun bereidheid om data te delen via metaplatformen. Om die reden benadrukt ons onderzoek het belang van data soevereiniteit in de groei van de dataeconomie van a) het bevorderen van vertrouwen richting metaplatformexploitanten en dataconsumenten, b) het verminderen van ervaarde risico's en c) het verhogen van de bereidheid om bedrijfsdata te delen via metaplatformen.

Conclusie

Onze studie draagt bij aan de *Information Systems* literatuur, voornamelijk daar waar literatuur over datadelen en digitale platformen bij elkaar komt. We zijn een van de eersten die ontwerpkennis tot stand brengen om controlemechanismen voor het delen van bedrijfsdata via metaplatformen voor datamarktplaatsen te ontwikkelen en evalueren met een nadruk op het onderzoeken van hun doelgerichtheid in het versterken van datasoevereiniteit in de maatschappelijke context van de dataeconomie. De voornaamste bevindingen van ons onderzoek zijn als volgt: 1) het theoretiseren van het potentiële effect van controlemechanismen op datasoevereiniteit, 2) het uiteenzetten van ontwerpopties en -principes als prescriptieve kennis, 3) het definiëren van *goodness* criteria voor het versterken van datasoevereiniteit en 4) het bevorderen van begrip van een metaplatform als een context voor het delen van bedrijfsdata. Onze secundaire bijdragen zijn 1) het leveren van bewijs over het potentiële effect van datasoevereiniteit op de bredere dataeconomie en 2) het uitbreiden van de toepasbaarheid van theorieën gebruikt in dit onderzoek naar de context van het op de markt gebaseerde delen van data.

Concluderend neemt deze studie de spanningen weg tussen Europese beleidsagenda's die een enkele mark voor data en het interoperabel delen van data propageren (bijv. in de EU-datastrategie en de Data Act) terwijl deze agenda's op hetzelfde moment zich inspannen om sectorspecifieke datamarktplaatsen te vormen (bijv. de acht verticale pijlers in het Digital Europe programma). Daarnaast benadrukken deze beleidsagenda's ook dat datasoevereiniteitsprincipes nagevolgd moeten worden. Omdat datasoevereiniteit essentieel is voor data-aanbieders om hun data te delen via metaplatformen, kan het aanpakken van zorgen daarover het opzetten van metaplatformen bevorderen. Daarom hopen we dat metaplatformen hun potentieel als eminent instrument kunnen realiseren om zo te vervullen wat we hopen (en waar we optimistisch over zijn) voor de dataeconomie: een single European Data Market in 2030.

PART 1: PROLOGUE

Chapter 1: Introduction[1]

As the data economy is growing, businesses increasingly utilize data marketplaces to share data with external parties. Due to the specialized nature of data products, data marketplaces exhibit a high degree of heterogeneity, often focusing on specific countries and industries. This specialization results in high transaction costs when sharing data in data marketplaces. Additionally, multi-homing costs are high, making it difficult for users to participate in multiple data marketplaces to expand their reach. The existing literature recognizes meta-platforms as a potential measure to reconcile highly heterogeneous digital platforms, thereby reducing transaction and multi-homing costs. Nevertheless, while sharing business data on a data marketplace is already difficult due to data sovereignty concerns, these concerns will likely intensify in a meta-platform setting because data may flow from one data marketplace to another. Control mechanisms can enhance data sovereignty; however, due to the novel and intricate nature of meta-platforms, existing knowledge on designing such mechanisms may not be directly transferable to this complex setting. Therefore, this research aims to create design knowledge for developing and evaluating control mechanisms for data sharing[2] through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy.

1.1 The emergence of data marketplaces in the data economy

In today’s digital era, numerous technologies generate vast amounts of data (Glennon et al., 2023). However, data largely remain underutilized within many businesses (Gantz & Reinsel, 2012; Manyika et al., 2015). Unlocking data potential requires participation in the *data economy*, a global ecosystem driven by collecting, processing, and sharing data (Sestino et al., 2023). In the data economy, companies increasingly share data with external parties (Richter & Slowinski, 2019).

The worldwide data economy is projected to reach a value of €1,025 billion by 2030 (Glennon et al., 2023). Beyond the economic value, the data economy also contributes to societal value by improving critical sectors such as public transportation and healthcare systems (Sestino et al., 2023). The demands from policymakers to unlock the potential of the data economy have urged the development of data marketplaces, a class of digital platforms that facilitate data sharing among businesses (Driessen et al., 2022; Spiekermann, 2019). This trend is especially prominent in Europe, where policy instruments to strengthen the European data economy have accelerated data marketplace proliferation (European Commission, 2020). In such marketplaces, one company grants another company access to its data products (Jussen et

[1] Parts of this chapter are based on the following publication:
Abbas, A. E., Agahari, W., van de Ven, M., Zuiderwijk, A., & de Reuver, M. (2021). Business Data Sharing through Data Marketplaces: A Systematic Literature Review. *Journal of Theoretical and Applied Electronic Commerce Research, 16*(7), 3321-3339. https://doi.org/10.3390/jtaer16070180.

[2] In this research, the term *data sharing* is specifically used to denote the exchange of business-related data, such as data sharing transactions conducted among businesses.

al., 2023), ranging from basic datasets to advanced analytical tools utilizing machine learning (Hasan & Legner, 2023).

Figure 1.1 conceptualizes the interrelations among the primary actors of data marketplaces (Spiekermann, 2019): operators, data providers, data consumers, and third-party providers. *Operators* manage a data marketplace as a business entity. *Data providers* are businesses supplying data products, and *data consumers* are businesses utilizing these products. *Third-party providers* add complementary services to data marketplaces, such as applications or algorithms. To access data products, consumers must compensate providers through monetary or non-monetary incentives (e.g., reciprocal data sharing, service discounts, or collaboration opportunities). Through data marketplaces, for instance, telecommunication operators may share call data insights with banks to increase the precision of credit risk assessments (cf. Óskarsdóttir et al., 2019).

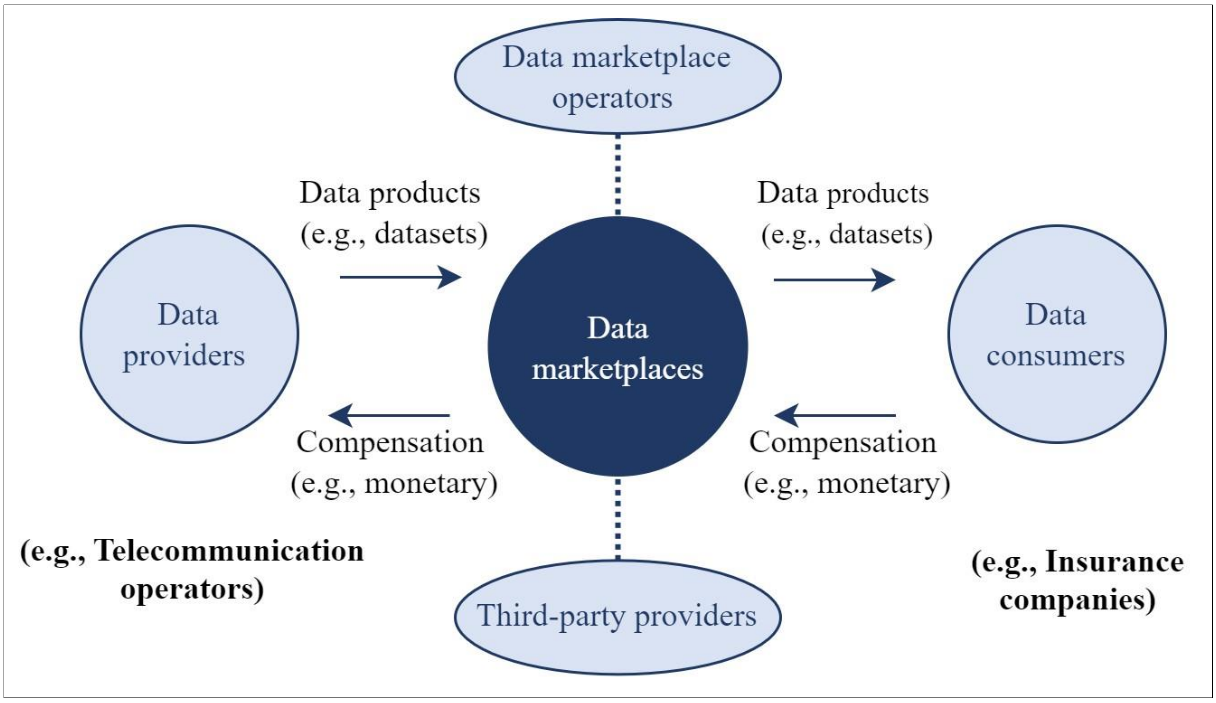

Data marketplace operators
Data products (e.g., datasets)
Data products (e.g., datasets)
Data providers
Data marketplaces
Data consumers
Compensation (e.g., monetary)
Compensation (e.g., monetary)
(e.g., Telecommunication operators)
Third-party providers
(e.g., Insurance companies)

Figure 1.1 Data marketplace conceptualization

Currently, a high degree of heterogeneity exists in data marketplaces (Azcoitia & Laoutaris, 2022). It means that data marketplaces are highly specialized in specific countries (e.g., Mobilithek[3] in Germany) or industries (e.g., Nasdaq Data Link[4] in the financial sector). High heterogeneity also indicates that a substantial number of variations across multiple aspects of data marketplaces exist (e.g., business models, governance arrangements, and technical standards) (Fruhwirth, Rachinger, et al., 2020; Spiekermann, 2019). We argue that a high degree of heterogeneity causes two main barriers to data marketplace adoption often cited in the literature: high transaction costs and multi-homing costs.

[3] https://mobilithek.info/, accessed on 14 February 2024.

[4] https://data.nasdaq.com/, accessed on 14 February 2024.

Transaction costs consist of three elements: searching, contracting, and enforcing (Dahlman, 1979). Searching costs are high because heterogeneity makes it difficult for data providers and consumers to find each other (Zappa et al., 2022). Consider, for example, the many variations of data marketplace business models. The heterogeneity makes data providers struggle to identify suitable marketplaces for their data products. For instance, a telecommunication company may seek out specific telco data marketplaces but still face challenges in finding ones that align with their preferences (e.g., marketplaces that use centralized architecture, fiat currency transactions, and data pricing support). Data consumers encounter similar difficulties due to the context-contingent nature of data (Otto, 2011). Data products must cater to specific contexts or use cases to meet consumer needs, making it challenging for data consumers to identify marketplaces with the desired value propositions. To put it differently, high switching costs prevent data consumers from knowing which providers offer the needed data products in various marketplaces.

High contracting costs arise because each marketplace may use a completely different contracting schema. Consider, for example, one contract element related to pricing mechanisms. Pricing data products is already tricky because data providers often do not know the value of their data products (Stahl & Vossen, 2017). For data consumers, they must access data products to determine their value, yet access is typically granted only after purchase. This is known as Arrow's information paradox (Stahl et al., 2017). With high heterogeneity, pricing data products become even more complex. Some marketplaces use flat pricing, while others adopt dynamic pricing strategies (Abraham et al., 2023). Additionally, payment methods vary; some marketplaces use fiat money, whereas others accept cryptocurrencies (Fruhwirth, Rachinger, et al., 2020). Moreover, data marketplaces already implement various pricing techniques, including volume-based, usage-based, and auction-based methods (Azcoitia & Laoutaris, 2022). Different pricing mechanisms make contracting costs high.

High costs in enforcing occur because data marketplaces operate in different jurisdictions and industry contexts. This means that data providers and consumers need to invest their resources in order to comply with jurisdiction- and industry-specific requirements. Yet, knowing when, where, and which regulations apply, as well as complying with them, are no easy tasks (Scerri et al., 2022). For instance, conducting data sharing in the EU requires adherence to data protection regulations like GDPR, in which the legal terms use broad, aspirational principles. This contrasts with the US, where data protection laws typically use more concrete and specific legal terms (Hoofnagle et al., 2019). Additionally, when users of data marketplaces engage in cross-industry data sharing, they must comply with industry-specific regulations, such as the upcoming European Health Data Space[5] in the health sector.

In addition to high transaction costs, the costs associated with multi-homing are also high. Platform users and third-party providers often multi-home to maximize network effects (Choi, 2010). Multi-homing means allowing them to affiliate with competing platforms (Parker

[5] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en, accessed on 05 July 2024.

& Van Alstyne, 2005). Yet, in the data marketplace setting, the high heterogeneity of data marketplaces makes data providers, data consumers, and third-party providers unable to multi-home to other data marketplaces (Azcoitia & Laoutaris, 2022). This is due, in part, to the extensive technological resources required to participate in data marketplaces, such as using application programming interfaces or installing customized software (Fruhwirth, Rachinger, et al., 2020). Participants may also need to obtain certifications for onboarding (Otto, 2022). These complex and costly technological resources can deter users and third-party providers from multi-homing across different marketplaces.

Multi-homing can also be tricky because it incurs learning costs. These learning costs are especially problematic due to the lack of data skills, such as understanding of data infrastructure (Fassnacht et al., 2023; Scaria et al., 2018). A report from the European Data Market study also highlights the trend of the widening skills gap among data professionals, projecting significant growth from 2023 to 2030 (European Commission, 2024). One reason for these challenges is that many potential users of data marketplaces are Small-Medium Enterprises (SMEs), which make up over 95% of propositions for data providers. Compared to large enterprises, SMEs have fewer resources, including data skills (Duan et al., 2002). They struggle to keep up with the evolving data skill requirements of data sharing as it is not yet a core aspect of their business (Fassnacht et al., 2023).

In response to the current landscape of data marketplaces, European policy agendas advocate for a unified data approach. A published strategy, for instance, outlines a vision for a single Data Market by 2030, enabling data to flow across sectors (European Commission, 2020). New legislation, such as the Data Act[6], allows users to require platform operators to share their data with others. In addition, the Data Governance Act[7] defines what users can expect from a data intermediary like data marketplaces. Collectively, these laws promote easier data sharing, which is currently hindered by the high transaction and multi-homing costs due to significant heterogeneity in data marketplaces.

In summary, the data marketplace landscape exhibits a high degree of heterogeneity due to 1) a high specialization for specific regions or industries and 2) diverse aspects of these marketplaces. This leads to two core challenges: high transaction costs and multi-homing costs. Concurrently, policy agendas aim to facilitate easier data sharing, which is currently obstructed by high transaction and multi-homing costs stemming from significant heterogeneity in data marketplaces.

1.2 Meta-platforms: Reconciling data marketplace heterogeneity

To reconcile heterogeneity, scholars in Information Systems, who investigate the socio-technical aspects of information technology-related phenomena, explore the interconnected platforms (e.g., Alt & Zimmermann, 2019; Kretschmer et al., 2022; Schöbel & Leimeister, 2022). Mosterd et al. (2021) refer to this phenomenon as *Platform-To-Platform Openness*

[6] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3491, accessed on 14 February 2024.

[7] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act, accessed on 05 July 2024.

(PTPO), meaning "the extent to which a platform is interoperable with other platforms" (p. 1). PTPO is helpful in a highly heterogeneous market as it strengthens the network effect required for digital platforms to thrive (Mosterd et al., 2021).

Multiple approaches exist to open a platform to others. Digital platforms can establish *direct* Application Programming Interfaces (APIs) for mutual connectivity (Hodapp & Hanelt, 2022). Alternatively, third parties can *bridge* two platforms by creating an application (Hilbolling et al., 2020) or *fork* a platform by exploiting its core resources (Karhu et al., 2018). Another way is to create a *meta-platform* that is built on top of two or more existing platforms, thereby connecting their respective ecosystems (Zhang & Williamson, 2021).

In this study, we explore meta-platforms because they are especially more appropriate for reducing transaction and multi-homing costs. Considering transaction costs related to searching costs, for example, meta-platforms create value by offering meta-search engines that aggregate and manage information flow from participating platforms (Lanza et al., 2016; Pitt et al., 2021). They provide users with broader, more accurate recommendations (Lanza et al., 2016; Pitt et al., 2021), such as price comparisons (Schöbel & Leimeister, 2023). This offering is often not available in other forms of openness, such as direct APIs, application bridges, and forking. Regarding multi-homing costs, meta-platforms are likely more beneficial because they are not designed for specific partners, allowing for a modular architecture that reduces dependency on individual participating platforms (Mosterd et al., 2021). This allows more participating platforms to join, enabling data providers and consumers to access more data marketplaces.

A few studies have started to explore the role of meta-platforms in enabling data sharing among companies, particularly in highly heterogeneous markets. For example, van der Wielen et al. (2022) investigate how meta-platforms can reduce data sharing bottlenecks in healthcare, thereby facilitating broader access to information and improving the end-user experience. Likewise, Maschewski (2023) explores meta-platforms to improve patient enablement, empowerment, and engagement in healthcare.

Figure 1.2 conceptualizes the structure of meta-platforms for data marketplaces. Compared to the data marketplace conceptualization (see Figure 1.1), *meta-platform operators* emerge as new actors. These operators orchestrate and coordinate different data marketplaces. Hence, meta-platforms cannot exist independently as they need *participating platforms* (Lagutin et al., 2019). For example, Trivago serves as a meta-platform in the tourism sector, while Expedia, Booking, and Airbnb are participating platforms. In the context of data marketplaces, recent initiatives like TRUSTS[8] and i3-Market[9] exemplify the role of meta-platforms. In all, meta-platforms may reconcile heterogeneity while allowing for the specialization of data marketplaces.

[8] https://www.trusts-data.eu/, accessed on 14 February 2024.

[9] https://www.i3-market.eu/, accessed on 14 February 2024.

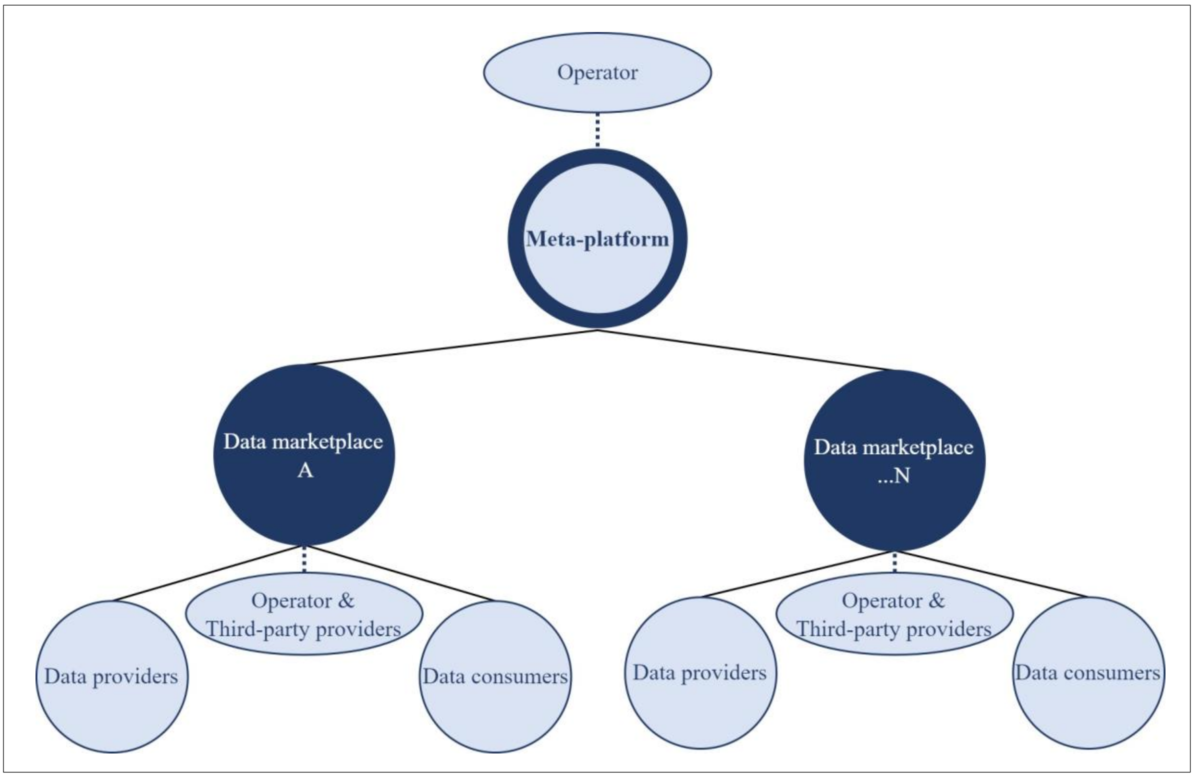


Figure 1.2. A meta-platform conceptualization in the data marketplace setting

Beyond meta-platforms, less complex means also have the potential to reconcile heterogeneity while allowing for the specialization of data marketplaces. These means do not need operators or third-party providers, such as upper ontology and data standardization. Let us consider upper ontology. In brief, upper ontology is a general term that acts as a foundation for more specific terms (Niles & Pease, 2001). For instance, the Basic Formal Ontology classifies entities into two distinct categories: continuants (objects and spatial regions) and occurrents (processes that unfold over time), each with its subclasses and properties (Arp et al., 2015). Another example of an upper ontology is Semantic Data Sharing Architecture in the supply chain domain, which aligns different supply chain ontologies (i.e., mode, cargo, document, and physical infrastructure). This upper ontology allows data sharing between parties using common semantics (Hofman et al., 2024).

Upper ontology may be the most powerful in the data sharing setting with a more well-defined context (e.g., supply chains). In data marketplaces, the nature of data sharing changes due to open and complex interactions with numerous participants and the allowance for third-party development of complementary functionalities that surpass the original plans of marketplace operators (Agahari, 2020). Consequently, data products become even more malleable (Abbasi et al., 2016), context-contingent (Otto, 2011), and can be used in unexpected ways (Susha et al., 2017). Hence, in the data marketplace setting, an upper ontology may be less adaptable, as alignment requires additional data skills to update concepts and properties in lower-level ontologies (Hofman et al., 2024). Moreover, such alignment needs substantial coordination efforts as ontology becomes even more complex (Mohammadi et al., 2020).

Therefore, our research focuses on meta-platforms that provide explicit coordination functions with data marketplace operators (Nickerson et al., 2022; Schöbel & Leimeister, 2023). In fact, meta-platforms often include upper ontology as part of their offerings (Vanderhulst et al., 2009). This way, meta-platforms can help align agreed meta-descriptions required for upper ontology to function in a large-scale setting.

1.3 Data sovereignty concerns in meta-platforms

Meta-platforms can reconcile heterogeneity while allowing for the specialization of data marketplaces. Nevertheless, meta-platforms make *data sovereignty* problematic. The data sharing literature defines data sovereignty as "…self-determination and the capability of a data provider to keep control over their own data assets" (Hellmeier & von Scherenberg, 2023, p. 8). This definition places data providers as the central actors concerned with data sovereignty. Data sovereignty concerns will likely intensify in a meta-platform setting because data may flow from one data marketplace to another, making data providers even harder to exert control over their data products (Zappa et al., 2022).

Data sovereignty concerns bring serious consequences. For example, competitors of data-providing companies may benefit from the shared data in unexpected ways (Gelhaar & Otto, 2020). In all, a lack of sovereignty adversely impacts data providers, constraining their willingness to share data due to reduced trust (Pettenpohl et al., 2022) and heightened risk perceptions (Martin et al., 2021). The lack of sovereignty will eventually reduce the adoption of meta-platforms, implying that a high degree of heterogeneity in data marketplaces will persist.

Control mechanisms may enhance data sovereignty when sharing data products. In the digital platform literature, these mechanisms refer to a portfolio of control instruments implemented by *controllers* to influence *controlees'* behavior to behave according to control goals (Goldbach et al., 2018; Tiwana, 2013). For instance, a platform operator utilizes seller reputation as a control mechanism in a crowdsourcing platform. This mechanism reduces opportunistic behavior among sellers (Zheng et al., 2019). Despite their potential to achieve various control objectives, control mechanisms are unexamined in data sharing literature, particularly for enhancing data sovereignty. Furthermore, given the novel and intricate nature of meta-platforms (e.g., allowing data to flow from one data marketplace to another), it is unknown whether data providers view existing control mechanisms in the digital platform literature as valuable. Overall, we do not know how to design control mechanisms to enhance data sovereignty on meta-platforms. Based on these considerations, we formulate the following practical problem statement.

Practical problem statement

The expanding data economy drives businesses to utilize data marketplaces for sharing data with external parties. Data marketplaces exhibit a high degree of heterogeneity, often focusing on specific countries and industries. This specialization leads to high transaction costs when sharing data. Additionally, multi-homing costs are high, making it difficult for users to participate in multiple marketplaces to expand their reach. Meta-platforms can reconcile high heterogeneity but make data sovereignty problematic. To reduce sovereignty concerns, operators can implement control mechanisms; however, the design of such mechanisms in the complex meta-platform setting is unexplored. If data providers perceive these control mechanisms as less valuable within the meta-platform context, both sovereignty and heterogeneity issues remain unresolved, constraining the growth of the data economy. In all, we are unsure how to design control mechanisms for enhancing data sovereignty in meta-platforms for data marketplaces.

1.4 Scientific problem statement

Given the uncertainty in designing control mechanisms for data sovereignty in meta-platforms, exploring *design knowledge* is critical. Design knowledge consists of two major domains: *the problem space* (e.g., context, goodness criteria) and *the solution space* (e.g., design principles, instantiations) (Bider et al., 2013; Vom Brocke et al., 2020). Nevertheless, design knowledge for developing control mechanisms in these two essential domains remains unclear. We elaborate on scientific gaps based on the following: a) design knowledge domains and b) sovereignty relevance to the data economy (refer to Figure 1.3 for the structure of scientific gaps).

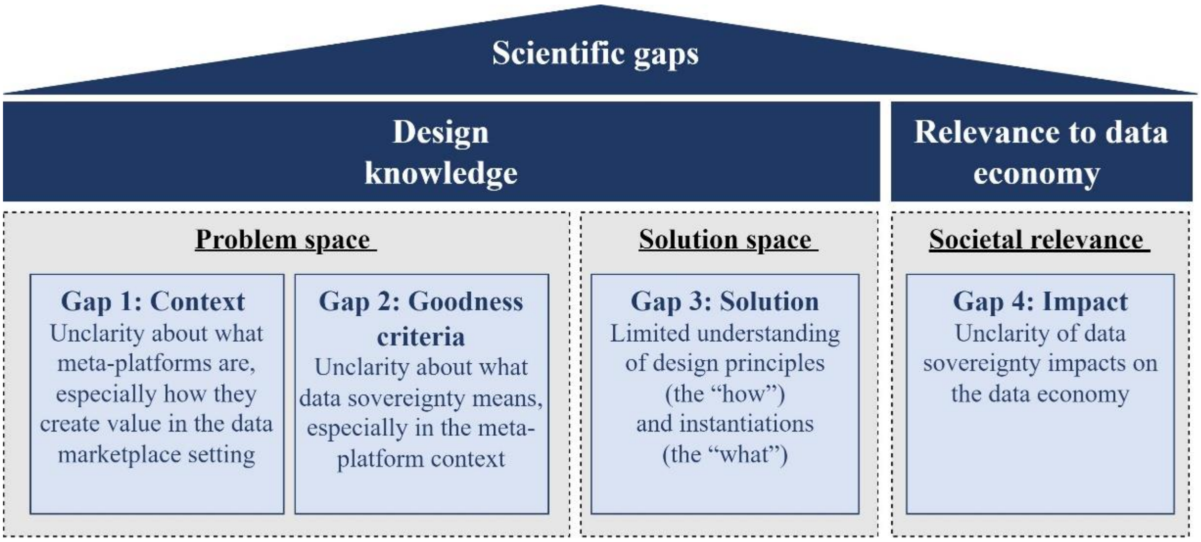

Scientific gaps
Design knowledge
Relevance to data economy
Problem space
Solution space
Societal relevance
Gap 1: Context
Unclarity about what meta-platforms are, especially how they create value in the data marketplace setting
Gap 2: Goodness criteria
Unclarity about what data sovereignty means, especially in the meta-platform context
Gap 3: Solution
Limited understanding of design principles (the "how") and instantiations (the "what")
Gap 4: Impact
Unclarity of data sovereignty impacts on the data economy

Figure 1.3. The structure of scientific gaps

Scientific gap 1 (Problem space—Context): Unclarity about what meta-platforms are, especially how they create value in the data marketplace setting. To create design knowledge in the problem space, we need to understand the context where the problem occurs. Without understanding the context, design interventions will likely be ineffective (Gregor & Hevner, 2013). In this study, we aim to enhance data sovereignty in meta-platforms for data marketplaces. However, we do not know how a meta-platform creates value in the data marketplace setting. Understanding *value creation* is important because it determines the *object* of sovereignty. For example, if meta-platforms create value by merely aggregating metadata from multiple data marketplaces, then the object of sovereignty is the metadata.

Despite being limited, a few studies have started discussing value creation of meta-platforms in the digital platform literature. For example, scholarly discourse explores the value creation mechanisms of meta-platforms in the conventional digital platforms in various domains, including aquaculture (Costabile et al., 2022), automotive (Floetgen, Strauss, et al., 2021; Hein et al., 2019), retail (Reinartz et al., 2019), and finance (Floetgen, Mitterer, et al., 2021; Zhang & Williamson, 2021). Value creation of meta-platforms is also discussed in many contexts, such as social networks (Pitt et al., 2019; Ulrich & Alt, 2021) and metaverse (Nickerson et al., 2022; Schöbel & Leimeister, 2023).

Meta-platforms for data marketplaces differ fundamentally from meta-platforms in traditional digital platforms (e.g., gaming platforms) due to the unique characteristics of data products. The *weak appropriability regime* of data creates challenges in protecting against duplication (Zhu & Madnick, 2009). Additionally, the *non-rival nature* of data allows for simultaneous use by multiple parties without diminishing availability (Koutroumpis et al., 2019). Finally, as *an intangible good*, data’s true value and quality become apparent only through its use (Koutroumpis et al., 2020). These differences imply that meta-platforms employ distinct value creation mechanisms in the data marketplace setting. In the data sharing literature, however, meta-platforms remain unexplored. To our knowledge, we do not identify many studies that discuss value creation of meta-platforms in the data marketplace setting, apart from a study from Lanza et al. (2016) that explores the infrastructure of such meta-platforms.

Scientific gap 2 (Problem space—Goodness criteria): Unclarity about what data sovereignty means, especially in the meta-platform context. Another essential design knowledge in the problem space relates to *goodness criteria,* referring to as “a rigorous set of acceptance criteria for the evaluation of potential design solutions and establishes guidance for the design of both formative and summative evaluation methods” (Vom Brocke et al., 2020, p. 533). However, defining goodness criteria is challenging because of the unclarity of what data sovereignty means, especially in the meta-platform context.

A predominant perspective in the data sharing literature conceptualizes data sovereignty as data providers’ ability to control their shared data (e.g., Hellmeier & von Scherenberg, 2023; Lauf et al., 2022; Scheider et al., 2023). In contrast, some studies align data sovereignty more closely with privacy (e.g., Schmidt et al., 2022) or security (e.g., Winandy, 2012). This variability is not surprising, given the broad interpretation of data sovereignty correlating with many facets (Hummel et al., 2021).

In addition, the complex meta-platform setting complicates our understanding of what data sovereignty means, especially related to data sovereignty facets. For example, the meta-platform setting creates a division of roles between meta-platform and marketplace operators, which complicates setting the responsibilities for providing sovereignty solutions. This is because a meta-platform interconnects heterogeneous data marketplaces, which may each have their own ways of enhancing the sovereignty of data providers. This suggests that responsibility can be a key aspect of data sovereignty in the meta-platform context. To summarize, the lack of clarity about data sovereignty, especially in the complex meta-platform setting, triggers uncertainty about design knowledge to define goodness criteria.

Scientific gap 3 (Solution space): Limited understanding of design principles (the "how") and instantiations (the "what"). Design knowledge in the solution space consists of design principles (the "how") and instantiations (the "what"). Design principles refer to "prescriptive statements that indicate how to do something to achieve a goal" (Gregor et al., 2020, p. 1622), while instantiations refer to contextualized implementations that are based on design principles to operationalize abstract concepts (Vaishnavi et al., 2004). However, we do not understand design principles and instantiations of control mechanisms for enhancing sovereignty in meta-platforms.

A few review papers in the data sharing literature explore mechanisms to enhance sovereignty. For example, Lauf et al. (2022) and Hummel et al. (2018) focus on control mechanisms for personal data sovereignty. Meanwhile, Schmidt et al. (2022) emphasize the privacy and security aspects of data sovereignty. Beyond these reviews, existing studies also investigate a specific mechanism such as certification (Duisberg, 2022; Firdausy et al., 2022), usage control (Jung & Dörr, 2022; Munoz-Arcentales et al., 2019; Zrenner et al., 2019), smart contracts (Precht & Gómez, 2021; Salviotti et al., 2018; Schinle et al., 2021), and privacy-enhancing technologies (Schäfer et al., 2023). However, these discussions only implicitly detail how control mechanisms specifically improve aspects of data sovereignty, particularly from the viewpoint of organizational-level data providers. Hence, a clear overview of such control mechanisms is lacking. As a result, we have limited perspective knowledge (i.e., design principles) on selecting and designing these mechanisms.

Despite not focusing on data sovereignty, several studies in the data sharing and digital platforms literature provide insights into the instantiations of control mechanisms. For example, existing research showcases the instantiation of certification (e.g., Lins & Sunyaev, 2022), usage control (e.g., Park & Sandhu, 2004), smart contracts (e.g., Sharma et al., 2019), privacy-enhancing technologies (e.g., Bauer et al., 2019). However, instantiations of control mechanisms remain underexplored in meta-platform contexts. This gap primarily arises from the lack of clarity on how meta-platforms create value in the data marketplace setting (see scientific gap 1). Without understanding value creation, we cannot accurately instantiate meta-platforms. For instance, without knowing what they offer, it is unclear which features to include in the prototype. Inaccurate instantiations hinder accurate evaluations by causing a mismatch between what is theoretically prescribed in design principles and instantiations.

Scientific gap 4 (Societal relevance): Unclarity of data sovereignty impacts on the data economy. The ultimate societal relevance of this study is to contribute to the growth of the data economy by enhancing data sovereignty. However, sovereignty's influence on the data economy's success remains largely uncharted territory. In the data sharing literature, existing data sovereignty research is technology-oriented (e.g., Falcão et al., 2023; Jarke et al., 2019; Scheider et al., 2023). The strong assumption of data sovereignty's importance to the data economy has been accepted without precise explanation nor little empirical evidence to support it (e.g., Stachon et al., 2023; Lauf et al., 2022; Scheider et al., 2023; Schinle et al., 2021). Therefore, the current conversation and development efforts are driven by the assumed necessity of data sovereignty. Such a perspective risks a potential overinvestment and redirection of resources towards promoting data sovereignty without fully comprehending its real implications, setting the stage for a potential failure akin to, e.g., the Google Glass incident (Kim, 2018; Klein et al., 2020). This overemphasis on an unverified premise calls for a more evidence-based analysis of the impacts of data sovereignty. To sum up, this study focuses on the following scientific problem statement.

Scientific problem statement

As a complex phenomenon, meta-platforms that federate data sharing platforms (i.e., data marketplaces) are examined within the intersection of the data sharing and digital platform literature. According to the data sharing literature, meta-platforms for data sharing platforms differ from the conventional ones, particularly due to characteristics of data products as experience goods, non-rival in nature, and protected by a weak appropriability regime. Consequently, what meta-platforms are in the data marketplace setting remains unclear, especially how they create value (scientific gap 1). In addition, current digital platform literature has yet to address unique challenges data sharing platforms face, such as data sovereignty. It means there is a lack of clarity about data sovereignty, especially in the meta-platform context (scientific gap 2). The digital platform literature utilizes control mechanisms to tackle platform-related challenges. However, existing research primarily focuses on single and conventional platforms (e.g., gaming platforms), leaving data sharing platforms that operate within or are connected through a meta-platform underexplored. Furthermore, the literature on digital platforms does not address sovereignty concerns. This leads to a limited understanding of design principles (the "how") and instantiations (the "what") of such mechanisms to address data sovereignty (scientific gap 3). Finally, given the ultimate societal relevance to contribute to the data economy growth, clarifying sovereignty impacts on the data economy is important, but such knowledge is scarce (scientific gap 4). In all, there is a pressing need to create design knowledge for developing and evaluating control mechanisms in the context of meta-platforms for data sharing platforms. Addressing these scientific gaps is crucial for enhancing data sovereignty in an envisioned single data market, a vital factor of the data economy growth.

1.5 Research objective, approach, and questions

Based on the practical and scientific problem statement, this study's objective is the following.

Research objective

To create design knowledge for developing and evaluating control mechanisms through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy.

To achieve the objective, this study employs the Design Science Research (DSR) approach. DSR aims to develop innovative information system artifacts and explore design knowledge to solve real-world problems (Hevner, 2007). This study is structured based on the three DSR domains: the problem space, the solution space, and the evaluation space. The study organizes each domain to address distinct research questions described below.

Problem space

Research question 1: How do meta-platforms create value in the data marketplace setting?

The first research question explores the value creation of meta-platforms for data marketplaces. This is vital due to a design knowledge gap in understanding what a meta-platform is as a data sharing context. This unclarity arises from different characteristics of data marketplaces and conventional digital platforms (scientific gap 1). Addressing the first research question provides a contextual foundation that guides the subsequent exploration of design knowledge in the problem, solution, and evaluation domains.

Research question 2: What are the key facets of data sovereignty in data sharing through meta-platforms for data marketplaces?

After investigating meta-platforms for data marketplaces, we examine what data sovereignty is within this complex setting. This step is crucial due to existing ambiguities related to data sovereignty, indicating a lack of design knowledge for setting goodness criteria (scientific gap 2). One way to understand data sovereignty is to explore its key facets. Therefore, addressing this second research question establishes foundational design knowledge in the problem space domain, which in turn informs the subsequent solution and evaluation domains.

Solution space

Research question 3: What control mechanisms can enhance data sovereignty in data sharing via a meta-platform for data marketplaces?

After understanding the data sharing context (RQ1) and the problem (RQ2), we review control mechanisms that can enhance data sovereignty in meta-platforms. A clear overview of such control mechanisms is lacking. Without such an overview, we risk overlooking appropriate mechanisms that can fulfill the goodness criteria of data sovereignty. After conducting a review, we prioritize and select a portfolio of control mechanisms that becomes the focus of this study. This step ensures the balance between breadth and depth, allowing for a thorough yet focused examination.

Research question 4: What do the developed control mechanisms look like in the meta-platform setting?

Having selected a portfolio of control mechanisms, we a) derive principles to design such mechanisms and b) instantiate control mechanisms through a prototype of a meta-platform. This step is crucial because we have a limited understanding of design principles (the “how”) and instantiations of control mechanisms in meta-platforms (the “what) (scientific gap 3).

Through this process, we enhance our knowledge of designing control mechanisms and obtain clarity on how such mechanisms look like in the meta-platform setting.

Evaluation space

Research question 5: To what extent do data providers perceive that the control mechanisms enhance data sovereignty for data sharing through a meta-platform for data marketplaces?

Research question 5 evaluates whether the designed control mechanisms fulfill the goodness criteria of enhancing data sovereignty. Without this understanding, we do not know whether our proposed mechanisms align with the expectations of data providers as problem owners. In addition, we cannot reflect on the design knowledge drawn from both the problem and solution space.

Research question 6: How does data sovereignty impact the data economy?

The final research question addresses the unclarity of data sovereignty impacts on the data economy. Addressing this research question helps to clarify and explain the assumed necessity of data sovereignty for the data economy's growth. Through this inquiry, we can assess if the prevailing technology-centric approach to data sovereignty research is the correct trajectory for data sharing communities.

1.6 Dissertation outline

Figure 1.4 presents an overview of the dissertation structure, which comprises ten chapters organized into five parts. The first part, *the prologue*, comprises three chapters. Chapter 1 presents the research background, Chapter 2 discusses the research design, and Chapter 3 elaborates on the research background. The second part, which consists of two chapters, explores *the problem space*. Chapter 4 examines the context in which data sharing occurs by exploring the value creation of meta-platforms in the data marketplace setting. Meanwhile, Chapter 5 discusses data sovereignty facets as goodness criteria. The third part, *the solution space*, proposes mechanisms to enhance data sovereignty. It comprises two chapters: Chapter 6 reviews a portfolio of control mechanisms, and Chapter 7 a) derives design principles for designing the selected control mechanisms and b) instantiates a prototype of a meta-platform that embeds these mechanisms. *The evaluation* part comprises two chapters. Chapter 8 examines the perceived efficacy of control mechanisms, while Chapter 9 evaluates the impact of data sovereignty on the data economy. Finally, *the epilogu*e concludes the dissertation (Chapter 10).

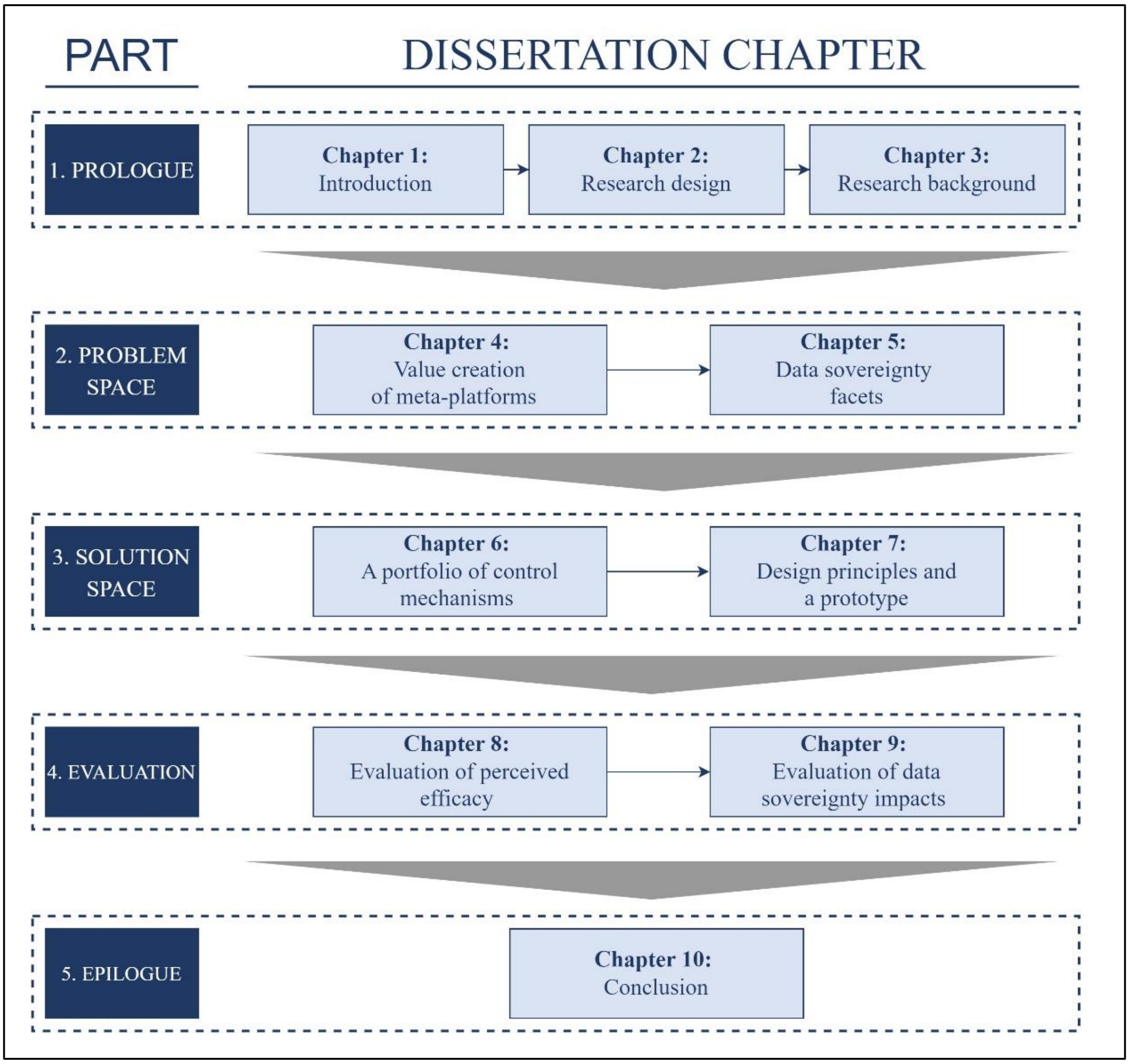

PART
DISSERTATION CHAPTER
1. PROLOGUE
Chapter 1: Introduction
Chapter 2: Research design
Chapter 3: Research background
2. PROBLEM SPACE
Chapter 4: Value creation of meta-platforms
Chapter 5: Data sovereignty facets
3. SOLUTION SPACE
Chapter 6: A portfolio of control mechanisms
Chapter 7: Design principles and a prototype
4. EVALUATION
Chapter 8: Evaluation of perceived efficacy
Chapter 9: Evaluation of data sovereignty impacts
5. EPILOGUE
Chapter 10: Conclusion

Figure 1.4. Dissertation outline

Chapter 2: Research Design[1]

Chapter 1 introduced the objective of this study: to create design knowledge for developing and evaluating control mechanisms for data sharing through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy. This chapter presents the research design employed to achieve the research objective. In Section 2.1, we elaborate on the research philosophy guiding this study. Section 2.2 elaborates on the research approach for addressing the study's objectives and aligns with the selected research philosophy.

2.1 Research philosophy

In the following sections, we explore the philosophical stances in the Information Systems field (Section 2.1.1). We then discuss pragmatism as our guiding research philosophy (Section 2.1.2).

2.1.1 Philosophical stances in Information Systems

Research philosophy informs how researchers create knowledge by clarifying what *reality* is (ontological beliefs), what true knowledge is (epistemological beliefs), and how researchers' value affects the research (axiological beliefs) (Saunders et al., 2019). Understanding research philosophy is key to choosing appropriate research approaches and methods (Crotty, 1998).

Two major research philosophies exist in Information Systems (IS): *positivism* and *interpretivism* (Orlikowski & Baroudi, 1991; Weber, 2004). Another research philosophy, *pragmatism*, evolves as an agnostic response to the traditional dichotomy of positivism and interpretivism in the IS field (Constantinides et al., 2012; Goldkuhl, 2012).

First, in positivism, the ontological belief posits an objective reality, independent of human interpretation. From the epistemological perspective, empirical observation and scientific methodology are crucial to knowledge acquisition (Crotty, 1998). Positivism commonly, but not always, employs quantitative methods that establish causal relationships or test hypotheses (Saunders et al., 2019). Axiologically, this philosophy minimizes the role of researchers' values, aiming for a neutral and unbiased approach to investigation (Stahl, 2007).

Second, interpretivism suggests that reality is not fixed and single but rather socially constructed (Klein & Myers, 1999). From an epistemological standpoint, interpretivism argues that understanding socially constructed reality necessitates interpretative methods, commonly qualitative but not exclusively so (Orlikowski, 1991). Axiologically, interpretivism acknowledges the influence of researchers' values on research processes (Saunders et al., 2019).

Finally, pragmatism holds the ontological perspective that a perfect understanding of reality is unattainable. Pragmatism views reality not as an abstract concept but as practical implications of ideas and actions (Saunders et al., 2019). Epistemologically, knowledge is considered valid when it effectively addresses real-world problems. Axiologically, pragmatism

[1] Parts of this chapter are based on the following publication:
Abbas, A. E. (2021). *Designing Data Governance Mechanisms for Data Marketplace Meta-Platforms.* Proceedings 34th Bled eConference – Digital Support from Crisis to Progressive Change, Online.

emphasizes the role of researchers' values in initiating a reflexive inquiry process, which begins with a sense of doubt and leads to a revised set of beliefs upon problem resolution (Elkjaer & Simpson, 2011). This research employs pragmatism as a research philosophy. The subsequent section justifies our choice of pragmatism as the research philosophy.

2.1.2 Pragmatism as the research philosophy for this study

This study adopts a pragmatic research philosophy for two key reasons. First, the study aims to create design knowledge for developing and evaluating control mechanisms for data sharing through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy (see Chapter 1). Such a focus on societal relevance and theoretical contributions aligns with the pragmatic epistemological assumption that knowledge is only valid if it offers solutions to real-world problems.

Second, this study needs pluralistic methods that accommodate different research domains (i.e., the problem space, the solution space, and the evaluation). In the problem space, understanding design knowledge a) on how meta-platforms create value and b) what data sovereignty is in the meta-platform setting calls for exploratory research, making a qualitative method suitable. In the solution space, the knowledge scarcity concerning design principles and instantiations necessitates design-oriented methods, such as prototyping. Conversely, a quantitative method is suitable to evaluate the perceived efficacy of the developed control mechanisms across a larger data provider population. Given the need to tackle several research domains, pragmatism is a more suitable philosophical stance than positivism or interpretivism. Unlike positivism, which often leans heavily on a quantitative method, or interpretivism, which commonly uses a qualitative method (although not always), pragmatism allows for a mix of both. Pragmatism also accommodates design-oriented methods, such as prototyping. Hence, pragmatism is a well-suited philosophical stance for this study, given its endorsement of pluralistic research methods, as long as they are appropriate to answer research questions.

An essential criticism of pragmatism is an emphasis on solving problems motivated mainly by the researcher's own perspective. This focus limits the ability to look at systemic issues from various angles (Dillon et al., 2000). To address this limitation, we employ a qualitative research method to investigate the problem space from multiple perspectives. Having discussed the rationale for choosing pragmatism, the subsequent section explains the research approach employed in this study: Design science research.

2.2 Research approach: Design science research

The preceding section selected pragmatism as the philosophical stance for this study. In this section, we describe the research approach that is 1) appropriate to achieve the study's objective and 2) aligns with pragmatism: Design Science Research (DSR). A frequently referenced paper defines DSR as follows:

> *"Design science research is a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing*

> *new knowledge to the body of scientific evidence. The designed artifacts are both useful and fundamental in understanding that problem" (Hevner & Chatterjee, 2010, p. 5).*

According to the above definition, DSR is oriented towards practical problem-solving, emphasizing the creation of useful artifacts (e.g., instantiations) while contributing to design knowledge (Hevner, 2007). This focus aligns well with this study's objective to create design knowledge for developing and evaluating control mechanisms for data sharing through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy. To achieve this objective, we create artifacts (i.e., control mechanisms in meta-platforms) and create design knowledge related to context understanding, goodness criteria, design principles, and the impact of data sovereignty on the data economy. Therefore, DSR's dual focus on solving real-world issues and advancing design knowledge is a well-suited approach for this study.

The problem-solving emphasis of DSR aligns with the epistemological and ontological beliefs of pragmatism (Hevner et al., 2004). Epistemologically, pragmatism values knowledge for its utility in problem-solving (Goldkuhl, 2012). Unlike other philosophical stances, such as positivism and interpretivism, which debate the truth of reality, pragmatism focuses on what works in practice (Thapa & Haj-Bolouri, 2023). The epistemological assumptions of pragmatism align closely with DSR, which is inherently focused on developing useful IS artifacts to address real-world challenges.

Ontologically, pragmatism acknowledges the imperfect understanding of reality, a stance distinct from positivism, which asserts a singular reality, and interpretivism, which posits multiple realities (Thapa & Haj-Bolouri, 2023). This ontological perspective of pragmatism aligns with DSR. In DSR, both the organizational problems (i.e., data sovereignty) and the proposed solutions (i.e., control mechanisms in meta-platforms) rapidly evolve. Given these dynamic characteristics, traditional ontological debates on the singularity or multiplicity of reality become less relevant. Instead, by embracing the pragmatist view that reality is imperfectly understood, researchers accommodate dynamic changes and open opportunities for continuous improvement.

In summary, this study employs DSR as the research approach for two primary reasons: 1) its suitability for achieving the study's objective and 2) its alignment with the study's pragmatist philosophical stance.

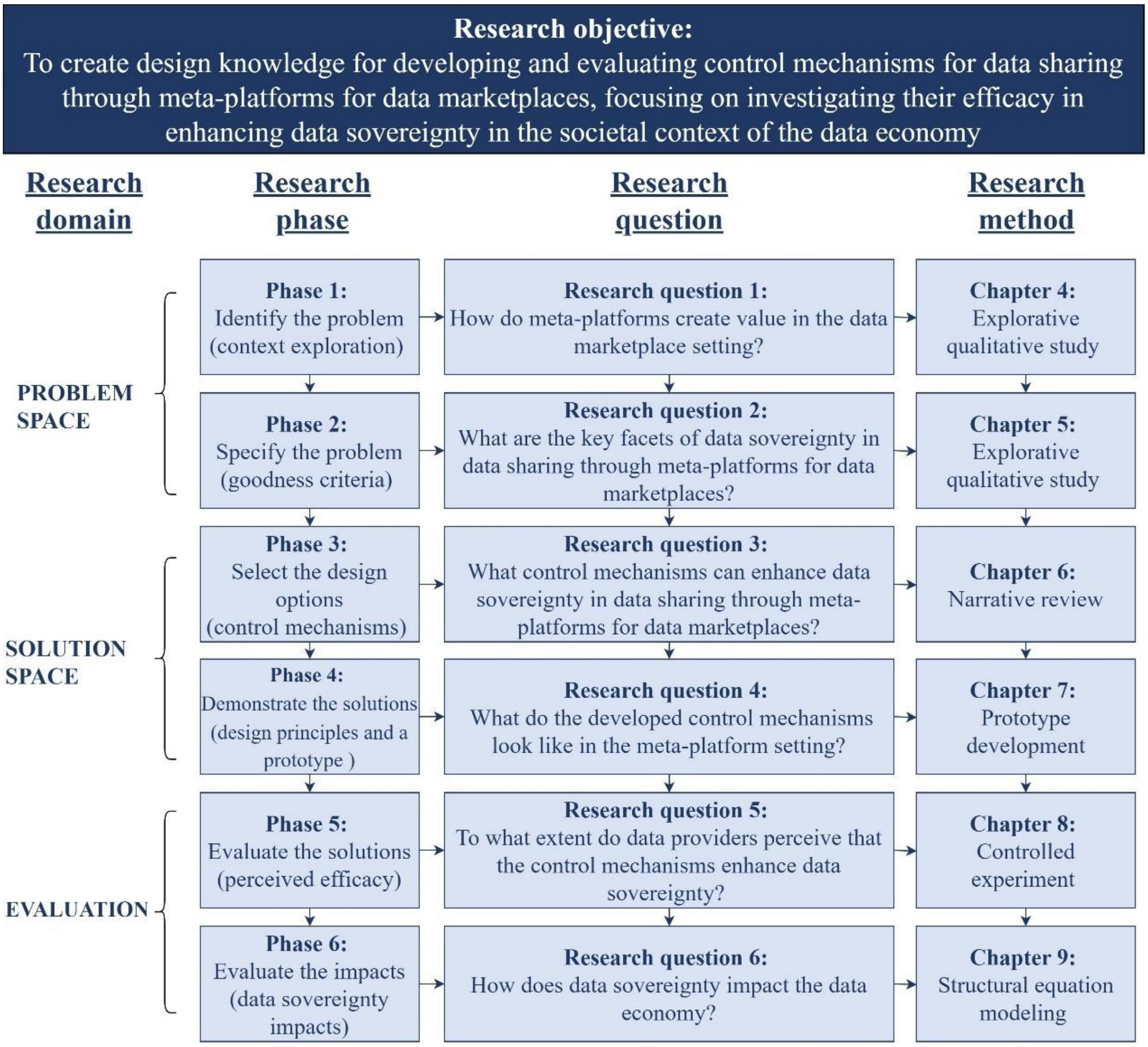
2.2.1 Knowledge in DSR

In Design Science Research (DSR), knowledge is divided into descriptive (Ω) and prescriptive (Λ). Descriptive knowledge, represented by *kernel theories*, "intends to explain or predict phenomena of interest" (Kuechler and Vaishnavi, 2008, p. 489). In contrast, prescriptive knowledge provides action-based guidelines for creating Information Systems (IS) artifacts to achieve desired outcomes. Descriptive knowledge describes *causal and effect relations* of phenomena; meanwhile, prescriptive knowledge describes *means-end relationships* that inform the IS artifact designs.

In the problem space, descriptive knowledge describes the “problem,” the context in which the problem occurs, and goodness criteria (i.e., criteria to measure whether proposed designs solve the problem). In the solution space, descriptive knowledge informs prescriptive knowledge to design artifacts (Venable, 2006; Vom Brocke et al., 2020). In the following section, we elaborate on the research phases of this study.

2.2.2 Research domains, phases, questions, and methods

We adapt the well-known process model of DSR to define the research phases of this study, namely *Design Science Research Methodology (DSRM)* (Peffers et al., 2007). The process model consists of six phases: 1) identifying problems and motivations, 2) defining objectives of solutions, 3) designing solutions, 4) demonstrating solutions, 5) evaluating solutions, and 6) disseminating the DSR project. In this research, we focus on adopting Phases 1-5, as the DSR project dissemination (Phase 6) is addressed through dissertation publications.



Research objective:
To create design knowledge for developing and evaluating control mechanisms for data sharing through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy

Research domain	Research phase	Research question	Research method
PROBLEM SPACE	**Phase 1:** Identify the problem (context exploration)	**Research question 1:** How do meta-platforms create value in the data marketplace setting?	**Chapter 4:** Explorative qualitative study
	Phase 2: Specify the problem (goodness criteria)	**Research question 2:** What are the key facets of data sovereignty in data sharing through meta-platforms for data marketplaces?	**Chapter 5:** Explorative qualitative study
SOLUTION SPACE	**Phase 3:** Select the design options (control mechanisms)	**Research question 3:** What control mechanisms can enhance data sovereignty in data sharing through meta-platforms for data marketplaces?	**Chapter 6:** Narrative review
	Phase 4: Demonstrate the solutions (design principles and a prototype)	**Research question 4:** What do the developed control mechanisms look like in the meta-platform setting?	**Chapter 7:** Prototype development
EVALUATION	**Phase 5:** Evaluate the solutions (perceived efficacy)	**Research question 5:** To what extent do data providers perceive that the control mechanisms enhance data sovereignty?	**Chapter 8:** Controlled experiment
	Phase 6: Evaluate the impacts (data sovereignty impacts)	**Research question 6:** How does data sovereignty impact the data economy?	**Chapter 9:** Structural equation modeling

Figure 2.1. Research design

This study is structured along the DSR domains and DSRM process model. The DSR domains are mapped to specific phases in the DSRM process model. The problem space encompasses Phases 1 and 2, focused on identifying the problems and specifying the problem indicators. The solution space corresponds to Phases 3 and 4, which involve designing and demonstrating solutions. Lastly, the evaluation aligns with Phase 5, where the designed artifacts are evaluated.

Figure 2.1 explains the relationship between DSR domains, phases, questions, and methods used in this research. The following sections provide a general overview of each research phase. Detailed discussions for each phase will be presented in its corresponding chapter.

2.2.2.1 Problem space

This study explores the problem space in two phases. Phase 1 identifies the problem by exploring the context, and Phase 2 specifies the problem indicators by defining goodness criteria.

Phase 1 – Identify the problem (context exploration)

According to Peffers et al. (2007), the initial phase of DSRM requires researchers to identify the problem and highlight its significance. This demands understanding the *application context,* which details the problem's complexity (Vom Brocke et al., 2020). We highlight the importance of addressing data sovereignty concerns in meta-platforms in Chapter 1. Addressing such concerns is pivotal; otherwise, data providers may avoid adopting meta-platforms, preserving the high heterogeneity of data marketplaces and hindering data economy growth. However, design knowledge of meta-platforms as a data sharing setting is lacking, especially on how they create value (scientific gap 1). Without this knowledge, we cannot fully understand what data sovereignty is.

To address this gap, the initial phase of our research explores the context where the data sovereignty problem occurs. We ask, "How do meta-platforms create value in the data marketplace setting?" Due to limited knowledge about meta-platform value creation for data marketplaces, we chose an exploratory qualitative study. Such an approach is often employed when researching novel phenomena (Sekaran & Bougie, 2016).

Our qualitative study in Phase 1 comprises two phases: 1) conceptual framing and 2) empirical analysis. We utilize the holon and holarchy framework in the framing step to explore the meta-platform structure. In doing so, we can identify interaction scenarios between data providers and consumers within a meta-platform for data marketplaces. With a new understanding of the meta-platform structure and interactions, we then engage in empirical analysis, conducting twenty semi-structured interviews. We detail the research approach for Phase 1, including its key findings in Chapter 4.

Phase 2 – Define the problem indicators (goodness criteria)

The second phase of DSRM specifies the problem indicators, which should logically be derived from the problem defined in the previous phase (Peffers et al., 2007). These indicators serve as *goodness criteria,* referring to "a rigorous set of acceptance criteria for the evaluation of potential design solutions and establishes guidance for the design of both formative and summative evaluation methods" (Vom Brocke et al., 2020, p. 533). However, defining goodness criteria is challenging because of the unclarity of what data sovereignty means, especially in the meta-platform context (scientific gap 2). Without goodness criteria, researchers cannot a) evaluate the efficacy of the design artifacts and b) reflect on the identified design knowledge.

To bridge this gap, this phase explores the meaning of data sovereignty within the meta-platform context. One way to understand data sovereignty is to explore its key facets. Hence, we ask: "What are the key facets of data sovereignty in data sharing through meta-platforms for data marketplaces?" Given the limited knowledge of data sovereignty in meta-platforms, we trace the concept of sovereignty to its origins in political science, leading us to adapt the *Social Contract Theory (SCT)*. SCT gives a framework to interpret sovereignty in the context of contemporary data. Given our goal of empirically exploring data sovereignty with SCT, we employ an exploratory qualitative approach. This approach excels in studies that need contextualization and interpretation (Glesne, 2016).

For Phase 2, we utilize the data gathered from the interviews conducted in Phase 1, as these interviews not only covered value creation aspects but also data sovereignty facets. Moreover, we complement our data by incorporating insights from 11 semi-structured interviews conducted by van Velzen (2022).[2] Some parts of these interviews explore data sovereignty concepts within meta-platforms. A detailed overview of the research method and key outcomes for Phase 2 is provided in Chapter 5.

2.2.2.2 Solution space

The solution space of this study is explored through two phases. In Phase 3, we select design options by choosing a portfolio of control mechanisms. Meanwhile, Phase 4 demonstrates the solution through a prototype.

Phase 3 – Select the design options (control mechanisms)

The third phase of DSRM explores design options, considering artifact functionalities that align with goodness criteria (Peffers et al., 2007). This phase is significant as many control mechanism options exist. Therefore, we must select and prioritize those mechanisms to balance breadth and depth, allowing for a thorough yet focused examination. Currently, there is an absence of a clear overview of these control mechanisms to enhance sovereignty. Although some reviews are available, they are fragmented, for example, focusing on the security and privacy facets of sovereignty. With a fragmented overview, we risk overlooking appropriate mechanisms that can fulfill the goodness criteria of data sovereignty.

[2] I served on the committee supervising van Velzen (2022) during his master's thesis at TU Delft, titled *"Business-to-Business data sharing via data marketplace meta-platforms: Exploring governance mechanisms to enhance data sovereignty."*

In Phase 3, we review control mechanisms to provide design options and make informed decisions to prioritize these mechanisms. We ask, “What control mechanisms can enhance data sovereignty in data sharing through meta-platforms for data marketplaces?” To answer this question, we employ a narrative review approach. The narrative review summarizes the prior knowledge within a field without necessarily following strict protocols like the Systematic Literature Review (SLR) does (cf. Okoli, 2015). We opt for this approach because of a) the limited studies directly linking data sovereignty to control mechanisms, complicating the formulation of a precise SLR search string; b) considerations related to research resources, particularly time and effort; and c) the flexibility of the narrative review.

Following Levy and Ellis (2006), our narrative review approach involves 1) collecting relevant literature, 2) analyzing the literature, and 3) writing a review. In selecting and prioritizing the mechanisms, we ground our justification based on the *control theory* perspective. A detailed explanation of the research approach and main findings for Phase 3 are presented in Chapter 6.

Phase 4 – Demonstrate the solutions (design principles and a prototype)

The fourth phase of DSRM involves demonstrating how the proposed solution tackles the identified problem (Peffers et al., 2007). This phase creates an instantiation (the “what”), informed by design principles (the “how”). Yet, design knowledge about these two aspects is limited (scientific gap 3). Without instantiation, data providers cannot evaluate the efficacy of control mechanisms in a realistic setting. Meanwhile, without design principles, we have no guidance in developing control mechanisms.

To address this gap, we ask, “What do the developed control mechanisms look like in the meta-platform setting?” To answer this question, we develop a prototype of a meta-platform incorporating the selected control mechanisms. This approach transforms our prior conceptual ideas (Phases 1-3) into a concrete representation.

Phase 4 develops a prototype based on four steps in DSR: 1) meta-requirement specification, 2) design principle identification, 3) design feature (or interface) development, and 4) prototype evaluation (e.g., Dellermann et al., 2019; Schilling et al., 2019). We derive the meta-requirements from the outcomes of Phase 2, which explore data sovereignty facets. We then propose design principles by drawing from *control* and *signaling theories*. Following this, we develop design interfaces and evaluate their usability. Chapter 7 elaborates on our design principle formulation and prototype design.

2.2.2.3 Evaluation

The evaluation comprises Phases 5 and 6. In Phase 5, we evaluate the perceived efficacy of control mechanisms to enhance data sovereignty in the meta-platform setting. In Phase 6, we evaluate data sovereignty impacts on the data economy.

Phase 5 – Evaluate the solutions (perceived efficacy)

The final phase of the DSRM evaluates the solution by assessing whether the artifacts meet the goodness criteria as defined in Phase 2. After this phase, researchers can either refine the artifacts or disseminate their findings, reserving potential improvements for later (Peffers et al., 2007). Without evaluation, we do not know whether our proposed mechanisms align with the expectations of data providers as problem owners. In addition, we cannot reflect on the design knowledge drawn from the problem and solution spaces.

In Phase 5, we evaluate the perceived efficacy of control mechanisms to enhance data sovereignty in the meta-platform setting. We question, "To what extent do data providers perceive that the control mechanisms enhance data sovereignty?" Instead of a technical appraisal (e.g., whether the control mechanisms can be feasibly developed), we focus on the user perspective (i.e., their *perception*). While objective measures of data sovereignty (e.g., Firdausy et al., 2022) technically exist, they do not always reflect the subjective experience of data providers interacting with control mechanisms. Moreover, our user-centric approach in DSR, especially for evaluation, ensures we assess the desirability of these mechanisms upfront, safeguarding against disproportionate investments in uncertain large-scale deployments.

We evaluate the perceived efficacy of control mechanisms by conducting a controlled experiment. This experiment consists of two steps. In Step 1, we develop a data sovereignty measurement model. In Step 2, we examine the perceived efficacy of control mechanisms using a two-way Analysis of Variance (ANOVA). Chapter 8 provides a more in-depth exploration of this phase.

Phase 6 – Evaluate the impacts (data sovereignty impacts)

Phase 6 of this study evaluates data sovereignty impacts on the data economy by asking, "How does data sovereignty influence the data economy?" Addressing this question helps to clarify and explain the assumed necessity of data sovereignty for the data economy's growth (scientific gap 4). In doing so, we know whether the dominant technology-centric perspective on data sovereignty research aligns with the needs of data-sharing communities.

We incorporate three commonly studied conditions contributing to the data economy: trust, risk, and willingness to share data (Agahari et al., 2022; Reimsbach-Kounatze, 2021; Richter & Slowinski, 2019). To test how data sovereignty influences these three conditions, we employ Partial Least Squares Structural Equation Modelling (Hair et al., 2021). By drawing from *theories on trust and risk*, we establish a nomological network of data sovereignty. Chapter 9 offers a detailed research method and key outcomes of Phase 6.

2.3 Summary of Chapter 2

Chapter 2 discussed the research design of this study, informed by *pragmatism* as the philosophical stance and *Design Science Research (DSR*) as the research approach.

We selected pragmatism for its compatibility with our research objective, which prioritizes societal relevance alongside theoretical contributions. The pragmatism epistemological assumption asserts that knowledge becomes truly valid when addressing real-world issues, which directly ties to our emphasis on societal relevance. Additionally, our study necessitates diverse methods that cater to varying research domains, including the problem space, solution space, and evaluation. Hence, pragmatism is an appropriate philosophical stance for this study, given its endorsement of pluralistic research methods, as long as the methods answer research questions appropriately.

We selected DSR as the research approach for two main reasons. Firstly, DSR is suited for our study's objective, as it emphasizes both social relevance (i.e., resolving real-world problems) and contributes to theories (i.e., formulating design knowledge). Secondly, DSR aligns with pragmatism as the philosophical stance. Epistemologically, while some philosophical stances debate the nature of reality, pragmatism emphasizes the knowledge that works in real situations. This makes pragmatism align with DSR, which aims to formulate design knowledge and develop artifacts that solve actual problems. Ontologically, pragmatism recognizes that our understanding of reality is imperfect, setting it apart from positivism's singular reality and interpretivism's multiple realities. This stance aligns with DSR, where both the challenges faced (i.e., data sovereignty) and the solutions offered (i.e., control mechanisms in meta-platforms) evolve over time. In this context, the traditional debates on the nature of reality become less pressing.

This study is structured along the DSR domains and Design Science Research Methodology (DSRM) process model. The DSR domains are mapped to specific phases in the DSRM process model. The *problem space* encompasses Phase 1–Identify the problem (context exploration) and Phase 2–Specify the problem indicators (goodness criteria). The *solution space* consists of Phase 3–Select the design options (control mechanisms) and Phase 4–Demonstrate the solutions (design principles and a prototype). Finally, the *evaluation* includes Phase 5–Evaluate the solutions (perceived efficacy) and Phase 6–Evaluate the impacts (data sovereignty impacts). Having described the research design, the next chapter will describe the research background for this study.

Chapter 3: Research Background

The previous chapter discussed the research design to achieve the study's objective. In Chapter 3, we examine five key concepts relevant to this study: *data sharing, data marketplaces, meta-platforms, data sovereignty,* and *control mechanisms.* This chapter defines these concepts, clarifies their scope, and positions them with other relevant concepts. Moreover, this chapter briefly discusses relevant theories employed in this study. Defining these concepts and theories is crucial for understanding the descriptive and prescriptive knowledge guiding the creation of design knowledge.

Section 3.1 discusses data sharing modes and justifies the rationale for focusing on market-based data sharing. Section 3.2 examines the business models of data marketplaces and the role of data products as the value unit. Section 3.3 discusses value creation of (conventional) meta-platforms. Section 3.4 discusses data sovereignty, followed by a discussion about theories employed in this study in Section 3.5. We employ the *holon and holarchy* structure to examine meta-platforms (Section 3.5.1) and *social exchange theory* to understand data sovereignty facets (Section 3.5.2). We use *control* (Section 3.5.3) and *signaling theory* (Section 3.5.4) to formulate design principles and *theories on trust and risk* to examine data sovereignty impacts (Section 3.5.5). We conclude Chapter 3 in Section 3.6.

3.1 Data sharing

In this study, we adapted the definition of data sharing by Jussen et al. (2023, p. 3688), which emerged from their systematic literature review study. We adapted the definition by tailoring it explicitly to business rather than personal or governmental data sharing.

Key concept 1: Data sharing

Data sharing is a process, irrespective of domains, where businesses (i.e., data providers) offer others (i.e., data consumers) access to their data products. Data consumers utilize these data products to develop new applications and services. In return, data providers expect rewards, either monetary or other incentives, such as reciprocal data sharing. Conditions for data usage are defined through contracts made between data providers and consumers, potentially including additional stakeholders based on data sharing scenarios.

Business data sharing offers numerous benefits, such as enabling innovative business models (D'Hauwers & Walravens, 2022), generating new revenue streams from data monetization, and enhancing internal processes (Jussen, Schweihoff, & Möller, 2023). We focus on data sharing by businesses because this setting represents a context where data sovereignty is highly challenged due to, for example, issues about losing control over data and ambiguity in data ownership. Losing data control implies data providers' difficulty in maintaining authority and oversight over how their shared data products are used by consumers (Spiekermann, 2019). Meanwhile, unclear data ownership highlights the complexities in determining who has the rights and claims to the data products after sharing (Gelhaar & Otto, 2020). This results in legal and economic liabilities for businesses (Fassnacht et al., 2023). Hence, businesses consider data sovereignty a prerequisite for data sharing (Gil et al., 2020; Pinto et al., 2023).

Considering the data provider perspective, conducting business data sharing typically involves three essential processes: preparation, agreement, and usage (e.g., Bastiaansen et al., 2019; Jussen et al., 2023; Schäfer et al., 2023). In the first phase, data providers prepare their data products for sharing. This phase includes ensuring data quality, defining metadata for their data products, and identifying the desired type of data consumers, such as those with certain certification levels. In the agreement phase, data providers establish terms of use, which encompass usage and access control policies. They also define commercial and legal conditions, followed by negotiating and finalizing the data sharing agreement. In the usage phase, data providers conduct several key activities, such as transferring the data and monitoring the data usage.

Business data sharing operates within three economic modes: hierarchy, network, and market (van den Broek & van Veenstra, 2015, 2018). In the hierarchy mode (e.g., supply chain networks), focal partners orchestrate data sharing through formalized, centralized control. The network mode is characterized by lateral relationships between data ecosystem members, emphasizing social agreements and collaborative approaches (Otto & Jarke, 2019). The market mode has recently gained traction, where data is shared as a commercial good through formal contracts via data marketplaces (Spiekermann, 2019).

The market mode, the focus of our study, presents the most significant challenges concerning data sovereignty. In this setting, data providers and consumers often have no previous partnership experience, leading to mutual unfamiliarity between each other. In addition, precisely defining data sharing terms and conditions is challenging, increasing the risk of misinterpreting data ownership and usage rights (Schomm et al., 2013; Virkar et al., 2019). Due to this condition, data providers lack control over their data products (Spiekermann, 2019). By focusing on the most challenging data sharing mode, we anticipate that data providers regard data sovereignty as a critical concern.

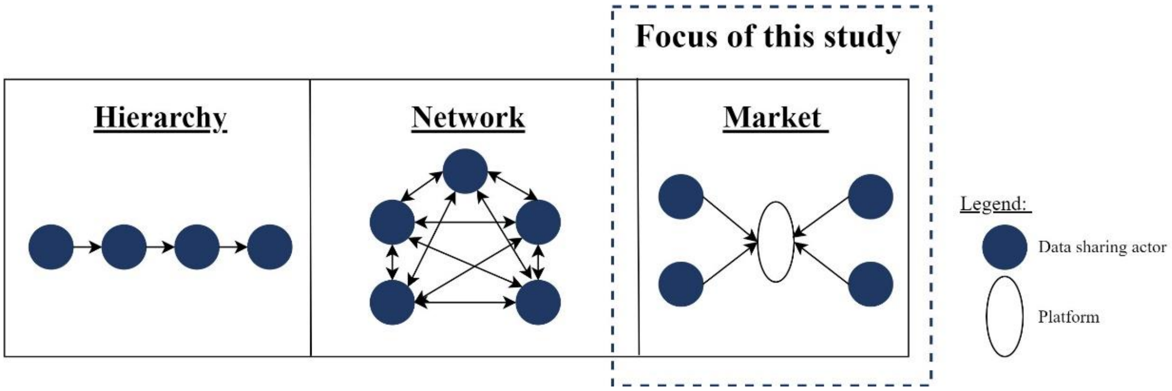


Figure 3.1. Business data sharing modes (adapted from van den Broek and van Veenstra, 2015)

3.2 Data marketplaces[1]

Data marketplaces began receiving attention in 2011, as both practitioners and scholars recognized data as an economic asset in the digital era (Driessen et al., 2022). Schomm et al. (2013) are among the first scholars who explored data marketplaces by identifying their dimensions and categories. The literature stream has since grown, covering topics such as data marketplace trends (Stahl et al., 2014), classification frameworks (Stahl et al., 2016), societal implications (Virkar et al., 2019), and business models (Azcoitia & Laoutaris, 2022; Fruhwirth, Rachinger, et al., 2020). Recent studies explore design options (Driessen et al., 2022) and governance structures (Abraham et al., 2023).

Data marketplaces first appeared in EU policymaking documents around 2017, with a study from the International Data Corporation and Open Evidence spotlighting EU data economy trends.[2] The European Commission continues to update this study on "The European Data Market Monitoring Tool."[3] In another report, "A European Strategy for Data,"[4] the European Commission recognizes data marketplaces as one of the key instruments to accomplish the EU vision to create a single European Data Market by enabling data sharing, thereby releasing the full potential of data flow and use across Europe. Considering the EU investment in data marketplaces and the projected trends in the data economy, research on data marketplaces is also expected to grow.

As a subtype of digital platforms, data marketplaces have inherent platform characteristics. Three core platform characteristics are matching users, facilitating interactions, and maintaining modular architecture. Firstly, platforms connect users, utilizing relevant information to create mutually beneficial connections. Secondly, platforms facilitate interactions by establishing rules that promote constructive exchanges and prevent negative ones. Lastly, a modular architecture is maintained, enabling third-party providers to offer supplementary services (Hein et al., 2020).

Having platform characteristics, data marketplaces match data providers with consumers for the sharing and utilizing data products (Driessen et al., 2022). Providers supply metadata about these products, making them searchable for consumers. Additionally, these marketplaces facilitate interactions with features like contract creation, pre-purchase testing, and review systems (Fruhwirth, Rachinger, et al., 2020). They also can have modular

[1] Some of the material from this section is partly based on the project report below, which the PhD candidate wrote.
Ofe, H., **Abbas, A. E.,** van de Ven, M., Bergman, R., Zuiderwijk, A., Reuver, M. d., Utermark, B., Markopoulos, I., Avgousti, G., Rosam, G., Fribus, M., & Brockob, A. (2021). *D7.1 "Sustainable Business Model for TRUSTS Data Marketplace I"*. https://www.trusts-data.eu/wp-content/uploads/2021/07/TRUSTS_D7.1_Sustainable-Business-Model_Taxonomies.pdf

[2] https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-2015-2020, accessed on 21 January 2024.

[3] https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-update, accessed on 21 January 2024.

[4] https://digital-strategy.ec.europa.eu/en/policies/strategy-data, accessed on 21 January 2024.

architecture, enabling third-party providers to integrate with and enhance the platform's offerings (Spiekermann, 2019). Based on this elaboration, we define data marketplaces as follows.

Key concept 2: Data marketplaces
Data marketplaces are a subtype of digital platforms that create value through a) matching data providers and consumers, b) facilitating interactions to share data products, and c) maintaining modular architecture for third-party providers to add additional offerings and services.

3.2.1 Data marketplace business models

A business model is "a conceptual tool that contains a set of elements and their relationships and allows expressing the business logic of a specific firm" (Osterwalder et al., 2005, p. 10). Discussing business models is vital as they provide a lens to develop a holistic understanding of the inner workings of a phenomenon (Klang et al., 2014).

The literature takes varied focuses on data marketplace business models. For example, Fruhwirth, Rachinger, et al. (2020) categorize business models according to centralized and decentralized architectural models. In the centralized model, providers upload data products to the marketplace infrastructure. In contrast, using technologies such as blockchain, the decentralized model retains data products on the provider's premises. The centralized model prioritizes efficient data sharing by pooling data, while the decentralized one offers on-site data retention but demands a more complex setup. Meanwhile, Azcoitia and Laoutaris (2022) classify data marketplace business models based on their purpose, distinguishing between generic and niche models. Generic marketplaces serve various sectors. In contrast, niche marketplaces target specific segments or industries, tailoring data products to specialized needs. Their pricing strategies differ, too: generic marketplaces use subscription-based pricing, whereas niche ones lean towards volume or usage-based pricing.

The many data marketplace business models open an opportunity to explore how meta-platforms can create value for this specific setting. For example, a meta-platform can create value by identifying and addressing incompatibilities between business models. Consider a scenario where one marketplace employs a centralized architecture while another adopts a decentralized approach; here, interoperability challenges arise. Additionally, a meta-platform can guide users towards marketplaces that align with their specific needs, leveraging the diverse purposes of these marketplaces. Hence, a meta-platform may play a crucial role in harmonizing various data marketplace business models.

3.2.2 Data products as a value unit in data marketplaces

In digital platform literature, the term *value unit* represents the products or services users exchange. For data marketplaces, the value unit is data products. Data products are "…data and analytics used by a service provider to deliver value to a customer or data user (whereas the customer can be internal or external) to solve a customer problem." (Fruhwirth, Breitfuss, et al., 2020, p. 517).

Data products can be categorized into three types: basic, analytical, and advanced analytical. Basic data products are unprocessed, such as raw customer information. Analytical data products derive insights from basic data products, such as visuals on a Power BI dashboard. Advanced analytical products use complex techniques for forecasting and decision-making, such as predictive maintenance tools and machine learning models (Hasan & Legner, 2023).

This research focuses on basic data products as they make data sovereignty problematic. Aaltonen et al. (2021) find that basic data products have key characteristics of *higher editability*, which increase data utility but also risk unforeseen uses that might breach initial agreements. Their *high portability* allows for easy transfers between systems but also presents chances of unplanned utilizations. The *low context* of these products means they have minimal usage constraints, which can lead to utilization outside of the intended initial agreements. Therefore, the distinctive characteristics of basic data products pose significant challenges to data sovereignty by increasing the likelihood of unintended uses and complicating the enforcement of original data agreements. Thus far, the selected focus of our study is as follows.

Study focus:
This research concentrates on business data sharing through data marketplaces, with an emphasis on basic data products as the value unit.

3.3 Meta-platforms

Having elaborated on data sharing and data marketplaces, this section discusses meta-platforms. This study defines meta-platforms as follows (Floetgen, Strauss, et al., 2021; Zhang & Williamson, 2021).

Key concept 3: Meta-platforms
A meta-platform is a platform designed to operate atop of two or more existing platforms, thereby connecting their respective ecosystems.

Chapter 1 outlines various approaches to interconnecting digital platforms: direct interfaces (Hodapp & Hanelt, 2022), application bridges (Hilbolling et al., 2020), platform forking (Karhu et al., 2018), and meta-platforms (Zhang & Williamson, 2021) (see Figure 3.2). We focus on meta-platforms because, unlike others, they are not tailored for specific partners. Consequently, their modular architecture minimizes dependency on individual platform participants, streamlining coordination in complex data marketplaces, which is crucial for lowering transaction and multi-homing costs. Therefore, these characteristics make meta-platforms more scalable and adaptable in a highly heterogeneous data marketplace landscape.

While beneficial, the adaptability and scalability of meta-platforms also increase sovereignty risks. In a meta-platform, data flows from one data marketplace to another. As more marketplaces interconnect, tracking data origins and checking data sharing agreements become increasingly complex. Consequently, data providers face more significant challenges in controlling their data (Zappa et al., 2022). Thus, meta-platforms are an appropriate setting to examine data sovereignty issues.

The following sections examine value creations of conventional meta-platforms (e.g., mobility platforms). Teece (2010) describes value creation as developing products or services that are beneficial to customers. Reviewing value creation in conventional contexts is critical as it lays the groundwork for developing value creation mechanisms in data-focused meta-platforms and contrasting them with conventional ones.

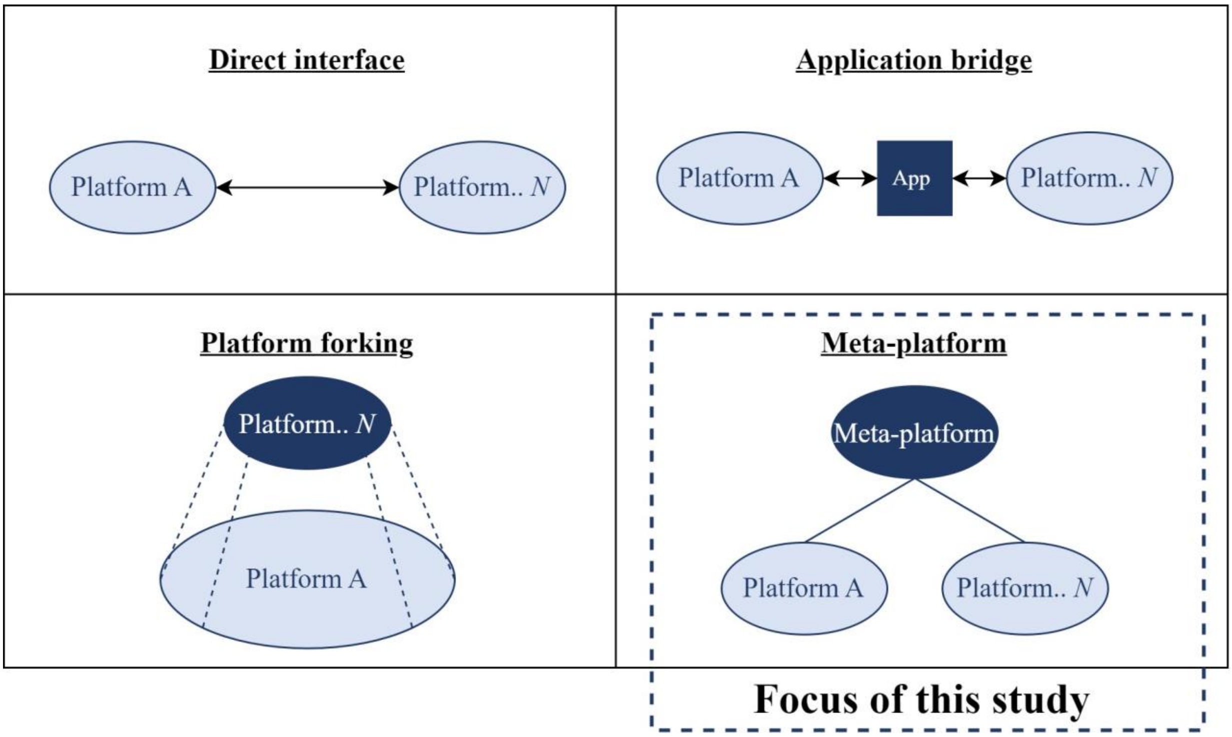


Figure 3.2. Multiple ways to interconnect platforms

Chapter 1 outlines two primary actors of meta-platforms: a) participating platform operators and b) end-users in participating platforms, which include both supply-side users (e.g., providers) and demand-side users (e.g., consumers). We explore value creation of meta-platforms from the perspectives of these actors.

3.3.1 Value creation for participating platform operators

A meta-platform acts as a coordinator or an orchestrator for participating platform operators (Nickerson et al., 2022; Schöbel & Leimeister, 2023). In some cases, meta-platforms are the *center of gravity*, which redirects the strategic direction of participating platforms (Zhang & Williamson, 2021). This happens when a meta-platform acts as a keystone player (e.g., Alipay or WeChat pay). In this case, a meta-platform has a high influence and is even responsible for the growth of participating platforms.

In doing so, meta-platforms create value by standardizing. Meta-platforms provide standardized *infrastructure architecture*, setting a consistent framework adopted by participating platforms (Fontana et al., 2007; Pon et al., 2015). An example is the plug-in architecture (Pitt & Cranefield, 2021; Pitt et al., 2019). This architecture has a core system for general tasks, while plug-ins handle specific tasks. This setup enables new participating platform operators to build new platforms by leveraging the core meta-platform system and selecting relevant plug-ins (Pitt et al., 2021). This idea aligns with shared services, where meta-platforms provide core and minimal offerings, letting new participating platforms build new services. Additionally, meta-platform can offer *integration services* to pre-existing platforms (e.g., Lanza et al., 2016). By doing so, meta-platforms create common interfaces or protocols, facilitating platform-to-platform openness without necessitating significant changes to the internal components of participating platforms. This integration can be facilitated using software development kits and application programming interfaces (Ulrich & Alt, 2021).

Participating platforms gain two benefits by aligning with meta-platforms that standardize infrastructure and provide integration services. First, aligning with a meta-platform increases the *legitimacy* of participating platforms. Legitimacy is “a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions” (Suchman, 1995, p. 574). Aligning with a meta-platform signal that the participating platform’s architecture aligns with broader industry standards (Zhang & Williamson, 2021) and fulfills security and regulation requirements (Mosterd et al., 2021). Second, participating platforms can focus on developing *new value propositions* (Pitt et al., 2021; van der Wielen et al., 2022), meaning meta-platforms enable participating platforms to autonomously tailor themselves to specific consumer segments (Pitt et al., 2019).

3.3.2 Value creation for end-users

Meta-platforms create value to end-users in many ways. Meta-platforms offer meta-search engines to aggregate and manage information flow from participating platforms (Lanza et al., 2016; Pitt et al., 2021). They provide consumer-side users with broader, more accurate recommendations (Lanza et al., 2016; Pitt et al., 2021), such as price comparisons (Schöbel & Leimeister, 2023). By offering meta-search engines, meta-platforms simplify dispatching tasks for providers as their value-unit information becomes accessible to a broader range of consumers in meta-platform ecosystems. Meanwhile, meta-search engines optimize searching tasks for consumers, allowing them to search for value units across multiple platforms. The dispatching and searching value increase user reach and reduce data discovery challenges (Nüesch & Back, 2011). By providing dispatching and searching value, meta-platforms streamline interactions through an integrated user interface, allowing end-users to perform activities through one interface (Floetgen, Strauss, et al., 2021; Reinartz et al., 2019). This simplifies navigation across diverse platform participants (Schöbel & Leimeister, 2023), avoiding lock-in effects (Basaure et al., 2020).

Meta-platforms offer innovative offerings and services. For instance, businesses developed inter-modal routing algorithms on a meta-platform that suggest optimal travel routes, considering social distancing given the COVID-19 situation (Floetgen, Strauss, et al., 2021). Another example is a filter function that enables a mobility platform to be interoperable with a partner (e.g., road safety authorities) (Mosterd et al., 2021). In financial services, Lloyds Bank introduced a meta-platform for subscription management, offering customers enhanced control and adaptability in their financial management during challenging times (e.g., to manage online streaming services they subscribe to) (Floetgen, Mitterer, et al., 2021). The innovating value improves the overall user experience (Djamasbi & Strong, 2019).

In summary, meta-platforms create value for two user groups: a) participating platform operators and b) end-users in participating platforms, encompassing supply-side (such as providers) and demand-side users (such as consumers). For participating platform operators, meta-platforms standardize key technical components such as infrastructure architecture and integration services. This standardization a) increases legitimacy of participating platforms and b) allows operators to develop unique value proposition.

For end-users in participating platforms, especially supply-side users, meta-platforms create value by dispatching metadata, increasing the reachability of their products or services. Meanwhile, for demand-side users, meta-platforms optimize searching tasks, allowing them to search for relevant products and services across multiple platforms. Hence, meta-platforms streamline interactions, granting end-users greater freedom that prevents lock-in effects. Finally, meta-platforms innovate to enhance the overall experience of end-users.

3.4 Data sovereignty

Sovereignty has historically been understood as the ultimate governing power over a political body (Hinsley, 1986). Bodin (1576) relates sovereignty closely to divine-fated monarchic rule for a country. However, the Enlightenment era of the 17th and 18th centuries shifted this understanding. This era, driven by empirical investigation and rational thought, led to new theories about the relationship between a country and its citizens, most notably Social Contract Theory (SCT). This theory is central to understanding data sovereignty and is elaborated in Section 3.5.2.

In the digital era, discussions on sovereignty have been re-focused to encompass individuals, communities, and organizations' control over their data, primarily due to, for example, the rise of cloud computing (De Filippi & McCarthy, 2012) and the Snowden revelations on state-approved surveillance (Lyon, 2014). More recently, data sovereignty has become central to European Union measures to fully leverage the data economy (e.g., European Strategy for Data). This led to initiatives such as the International Data Spaces Association and GAIA-X, both of which highlight the importance of data sovereignty.

To explore the multi-faced nature of data sovereignty (see Chapter 5), we utilize *notions* that correlate with data sovereignty provided by Hummel et al. (2021). Considering the trade-off between the facet richness and the depth of exploration, we focus on the most potentially suitable notions in business data sharing: *control, ownership, security,* and *responsibility* (see Hummel et al., 2021). In addition, we investigate *compliance* as a facet, given its recent legal prominence in contexts such as the European Data Governance Act (Duisberg, 2022).

According to Hummel et al. (2021), control refers to the capability to influence and direct information flows. Ownership refers to data property rights, indicating the privileges over data products. Security, on the other hand, focuses on preventing potential threats and risk mitigation concerning data. Additionally, responsibility delineates roles and expectations, while compliance represents the adherence to relevant legal and regulatory frameworks. To summarize the previous discussion, we use the following definition of data sovereignty for this study.

Key concept 4: Data sovereignty
Data sovereignty represents the self-determination and capability of data providers to claim ownership, exert control, gain security, and comply with relevant regulations, all facilitated by explicit responsibilities of (meta-)platform operators to provision the necessary mechanisms that enable such self-determination and capability.

3.5 Theoretical framework

Section 3.5 presents an overview of the theories employed in this study, each detailed in their respective chapters. Section 3.5.1 introduces the *holon and holarchy* structure, which inform our examination of meta-platform value creation in the data marketplace setting, detailed in Chapter 4. Section 3.5.2 discusses *social contract theory*, which lays the foundation for exploring data sovereignty facets in Chapter 5. Section 3.5.3 explores *control theory*, and Section 3.5.4 explores *signaling theory*; both theories underpin the development of control mechanisms aimed at enhancing data sovereignty, elaborated in Chapters 6 and 7. Lastly, Section 3.5.5 elaborates on *theories on trust and risk*, providing the theoretical framework for evaluating the broader implications of data sovereignty in Chapter 9.

3.5.1 The holon and holarchy structure

Utilizing a conceptual lens is critical to generating innovative insight into emerging phenomena (Jiang et al., 2022). Therefore, we employ a conceptual lens of *holon and holarchy* to examine value creations of meta-platforms in the data marketplace setting.

The holon and holarchy lens structures complex phenomena in Information Systems (IS) literature. Sun et al. (2023) employ this lens to develop a digital innovation model in platform ecosystems, revealing the complex interplay between social and technological resources. Clegg and Shaw (2008) introduce a process-oriented holonic modeling methodology for business process designs. Shanks et al. (2008) apply the holon-holarchy lens to conceptualize modeling grammar. These studies indicate the potential of the holon and holarchy lens in structuring complex IS phenomena.

The term *holon* merges *holos* (whole) and the suffix *on* (part) from Greek. Holon represents an entity as an independent whole and a part of larger systems. For example, while a person is seen as an independent individual with distinct rights and freedoms, they also exist as a member of society, bound by its overarching norms and regulations.

Koestler (1968) introduces *holarchy* to structure holons. Contrasting the traditional understanding of hierarchy as a rigid, top-down structure, a holarchy is a network of independent, self-regulating holons that demonstrate a range of autonomy and self-reliance. Figure 3.3 illustrates a holon structure in a holarchy.

Esbjorn-Hargens and Zimmerman (2011) use an ecological community to explain the holon structure in a holarchy. With its diverse species, this ecological community acts as a holon and fits within a larger ecosystem. On its own, the ecological community appears as a unique and self-sufficient unit. However, as part of the broader ecosystem, it aligns with and is influenced by the larger system's rules. This shows a holon's dual role: an independent entity and a part of a broader system.

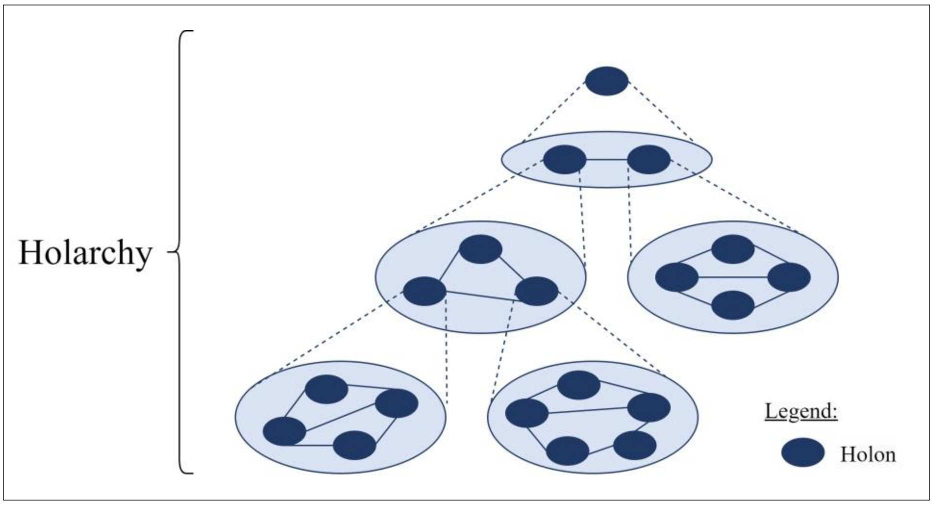


Figure 3.3. A holon structure in a holarchy

Due to the shared generic structure, the holon and holarchy structure is an appropriate lens for examining the value creation of meta-platforms in the data marketplace setting. Generic structure refers to "…the commonality between two domains/input spaces, allowing to see the big picture of the similarities/differences through the mapping of shared conceptual elements" (Jiang et al., 2022, p. 1838). Koestler's (1968) lens of holon and holarchy emphasizes the relationship between individual elements (parts) and their collective systems (wholes). Meta-platforms, comprised of interlinked data marketplaces, represent this part-whole dynamic. In this context, each data marketplace represents a part contributing unique value, yet a meta-platform federates these "parts" into a "whole." Thus, we analyze meta-platform value creation in the data marketplace setting through the holon and holarchy structure (see Chapter 4).

3.5.2 Social contract theory

Social Contract Theory (SCT) posits that individuals sacrifice some freedoms to a governing entity for societal benefits (Friend, 2004). In data sovereignty, data providers agree to certain compromises. For instance, they may adhere to predefined data sharing protocols. In return, they receive benefits offered by platform operators, such as the ability to control their exchanged data. Such trade-offs between freedoms and benefits mirror the principle of SCT. Hence, we consider SCT to be suitable for exploring data sovereignty facets.

To apply SCT as an analytical tool, we must consider its key aspects: spatial, temporal, and substantive (Loewe et al., 2021). The *spatial* aspect of SCT specifies *who* participates and *where* their influence applies in a societal contract. The *who* includes varied parties like governments, societal groups, and individuals. The *where* implies the territorial extent of the agreement, which could span sub-national, national, transnational, or supranational levels (Loewe et al., 2021).

The *temporal* aspect, concerning the *when*, explores the dynamic of social contracts over time. Social contracts can differ significantly in their duration and the timing of their renegotiations. While social contracts aim to provide stability to the relationship between a country and societal groups, they often require renegotiation and adaptation due to changes in power distribution or the perceived failure of countries to meet their obligations (Loewe et al., 2021).

The *substantive* aspect of SCT describes vertical arrangements between a nation and societal groups. These are known as the Three Ps: Protection, Provision, and Participation. The Three Ps explain the *what* of social contracts (Loewe et al., 2021). Protection focuses on recognizing and acknowledging inherent rights that need safeguards (Ellis, 2006; Hickey, 2011). Provision encompasses the various services and resources a country provides to society, including healthcare, education, and infrastructure (e.g., Sobhy, 2021). Participation involves citizens actively engaging in public affairs and interacting with government processes (Loewe et al., 2021). The key facets of SCT form the foundation for contextualizing data sovereignty in Chapter 5.

3.5.3 Control theory

We employ control theory to select control mechanisms we focus on and to explain why design principles for developing such control mechanisms work.

Control theory's exploration in the IS field began in the late 20th century (Cram et al., 2016; Saunders et al., 2020). Recently, control theory has been studied in emerging phenomena, such as data sharing (e.g., Vesselkov et al., 2019), digital platforms (e.g., Tiwana et al., 2010), or data marketplaces (e.g., Agahari, 2020). Building from the fundamental control literature, Tiwana and Keil (2009) define control as "…the process and rules governing controlee actions implemented by the controller to promote desirable controlee behaviors" (p. 12). Control is performed via diverse *control mechanisms* (Tiwana & Keil, 2009), referring to specific actions to achieve control objectives. In this study, we define control mechanisms as follows.

Key concept 5: Control mechanism
Control mechanisms refer to a set of targeted actions implemented by (meta-) platform operators to steer the behavior of data consumers, with the objective to enhance the sovereignty of data providers in data sharing.

Early IS research on control adopted a *cybernetic view*, focusing on adjusting systems to meet predefined controllers' goals. This approach presumed that control goals are fixed, and that behavior can be directed with effective feedback loops. In contrast, contemporary IS control research diverges into two mainstreams. *The functional view* structures control to achieve controllers' goals, acknowledging potential goal conflicts. *The behavioral view* investigates control impacts on controlees, e.g., end-users, examining whether their behaviors align with control goals. This view also explores changes in their participation levels and motivations (Saunders et al., 2020). This research focuses on the behavioral view, as we aim to create design knowledge to design control mechanisms and evaluate their impacts to enhance the data sovereignty of data providers.

Control mechanisms can be classified into formal and informal control modes (Jaworski, 1988; Kirsch, 1996; Kirsch, 1997). *Formal control* is defined by "explicit controller prescriptions," while *informal control* tries "to influence implicit determinants of controlee behaviors" (Wiener et al., 2016, p. 743). Formal control can further be classified into three sub-modes: 1) input, 2) process, 3) and output control.

Input control is measurements implemented by controllers before the beginning of an activity; *process control* is controllers' attempt to influence processes to produce the intended outcome by monitoring controlees' compliance towards prearranged guidelines and rules; *output control* examines delivered outcomes based on predefined goals. Informal control can be distinguished into 1) self and 2) clan control. *Self-control* focuses on intrinsic motivation at the individual-controlee level by defining and monitoring control objectives (Jaworski, 1988). Finally, *clan control* influences peer group behavior by motivating them via shared norms, values, and visions.

Control theory explains the relationship between a (configuration of) control mechanisms to control outcomes. For instance, Goldbach et al. (2018) find that a digital platform benefits when it requires third-party developers to exercise self-control, leading to higher application quality and a stronger commitment to stay on the platform. Zheng et al. (2019) find that in crowdsourcing platforms, both formal controls, such as seller reputation, and social controls, such as the number of fans and members, significantly reduce sellers' chances of engaging in opportunistic behaviors. In summary, control theory is relevant to inform the selection and design of the control mechanisms to enhance data sovereignty in data sharing via meta-platforms, elaborated in Chapters 6 and 7.

3.5.4 Signaling theory

Similar to control theory, we employ signaling theory to explain why design principles for control mechanisms may work. While control mechanisms may technically ensure sovereignty, their efficacy does not necessarily align with the subjective experience of data providers interacting with them. This discrepancy arises due to information asymmetry, a situation where one participant in an exchange possesses more information than the others, leading to less than ideal decision-making (Connelly et al., 2011). In our research, information asymmetry can occur when data providers, the problem owners of data sovereignty concerns, are not fully aware of how those control mechanisms work. To address this limitation, a supplementary theory is required to tackle information asymmetry that informs the design principles for developing control mechanisms. One appropriate theory to deal with information asymmetry is signaling theory.

Information system scholars started to explore signaling theory in the early 2000s, initially focusing on open-source software projects (Hann et al., 2002; Wan et al., 2004) and electronic marketplaces (Huang et al., 2005; Kim et al., 2004; Xu & Kim, 2003). Since then, IS scholars applied signaling theory in various contexts, including online crowdsourcing (Hong & Pavlou, 2012; Xiao et al., 2014), cloud service certifications (Lansing et al., 2013; Lansing & Sunyaev, 2013; Sturm et al., 2014), and emerging areas such as ethical artificial intelligence (Clausen et al., 2022) and blockchain-based innovation (Rammert et al., 2023).

Signaling theory has four elements: signalers, signals, receivers, and feedback (Connelly et al., 2011). *Signalers* are those who send out information; *signals* are observable cues or messages that convey the information; *receivers* are parties that interpret and evaluate the signals; and *feedback* represents the responses from the receivers, providing insight into signal efficacy.

Signaling theory explains the feedback efficacy. For example, Lansing et al. (2019) use signaling theory to examine how cloud service certifications assure businesses, reducing information asymmetry and guiding decision-making in cloud adoption. Zhou et al. (2022) utilize signaling theory to examine the impact of various signals in online mental health care, emphasizing their role in decreasing information asymmetry and drawing in new clients. Wells et al. (2011) employ signaling theory to explore how the quality of a website serves as an indicator of product quality in online retail.

In summary, signaling theory helps understand how meta-platform operators (signalers) develop control mechanisms (signals) that enhance the data sovereignty (feedback) of data providers (receivers), as elaborated in Chapter 7.

3.5.5 Theories on trust and risk

We employ theories on trust and risk as a framework for evaluating the broader implications of data sovereignty in the data economy, elaborated in Chapter 9. Core variables in data sharing within the data economy include trust (Baker, 2021; Van Der Burg et al., 2021), perceived risk (Riss et al., 2022; Sestino et al., 2023), and willingness to share data (Rantanen & Koskinen, 2020b; Richter & Slowinski, 2019). Therefore, theories on trust and risk are appropriate to guide the creation of a nomological network of data sovereignty impacts (cf. Dai & Luo, 2011; McLain & Hackman, 1999).

Theories on trust and risk explain the interplay between trust and perceived risks, examining their combined effect on specific outcomes (McLain & Hackman, 1999). In the IS field, particularly in digital platform literature, theories on trust and risk have been employed across diver settings, such as social media platforms (Wang et al., 2016), e-commerce (Guo et al., 2018; Lăzăroiu et al., 2020; Sun & Li, 2021), sharing economy platforms (Gu et al., 2021; Yan et al., 2018), or fintech (Xia et al., 2023).

We adapt the definition of *trust* as believing “that the trusted party will fulfill its commitment” (Gefen et al. 2003, p. 54). In this study, the trusted parties are meta-platforms and data consumers. Meta-platform operators are responsible for provisioning mechanisms to ensure data sovereignty. Meanwhile, data consumers must use the shared data products that respect the sovereignty of data providers. *Perceived risk* is the uncertainty and potentially harmful outcomes that individuals or organizations anticipate when considering engaging in a specific activity (Featherman, 2001; Featherman & Fuller, 2003). In our context, perceived risks capture the concerns of data providers about the uncertainties and potential pitfalls associated with sharing their data on meta-platforms. Meanwhile, *willingness to share data* is the inclination of data providers to give access to their data products under specific terms.

Existing literature outlines three general mediation models to describe the relationships among trust, risk, and behavioral intentions (Kim & Koo, 2016; Zhai et al., 2022): a) trust influences risk, which then affects behavioral intentions, b) risk influences trust, subsequently impacting behavioral intentions, or c) a bidirectional relationship exists between risk and trust. Employing theories on trust and risk thus offers a foundation to develop a nomological net of data sovereignty impacts, guiding the hypothesis development presented in Chapter 9.

3.6 Summary of Chapter 3

Chapter 3 elaborated on key concepts and theories foundational to this research. We introduced five concepts: data sharing, data marketplaces, meta-platforms, data sovereignty, and control mechanisms.

Data sharing refers to a process, irrespective of domains, where businesses (i.e., data providers) offer others (i.e., data consumers) access to their data products. Data consumers utilize these data products to develop new applications and services. In return, data providers expect rewards, either monetary or other incentives, such as reciprocal data sharing. Conditions for data usage are defined through contracts made between data providers and consumers, potentially including additional stakeholders based on data sharing scenarios. *Data marketplaces* refer to a subtype of digital platforms that create value through a) matching data providers and consumers, b) facilitating interactions to share data products, and c) maintaining modular architecture for third-party providers to add additional offerings and services. This study focuses on basic data products as a value unit of data marketplaces. *Meta-platforms* refer to a platform built on top of two or more existing platforms, thereby connecting their respective ecosystems.

Data sovereignty represents the self-determination and capability of data providers to claim ownership, exert control, gain security, and comply with relevant regulations, all facilitated by explicit responsibilities of (meta-)platform operators to provision the necessary mechanisms that enable such self-determination and capability. *Control mechanisms* refer to a set of targeted actions implemented by (meta-) platform operators to steer the behavior of data consumers, with the objective of enhancing the sovereignty of data providers in data sharing.

We employ five theories in this study (see Figure 3.4). We use the holon and holarchy structure to explore the value creation of meta-platforms for data marketplaces (research question 1). We utilize social contract theory to examine data sovereignty facets (research question 2), informing our evaluation criteria (research question 5). To select and instantiate control mechanisms (research questions 3 and 4), we utilize control and signaling theories as kernel theory. In control theory, control *(Cause)* leads to design behaviors *(Effect).* In signaling theory, signal interventions *(Cause)* reduce information asymmetry *(Effect).* These cause-effect relationships guide the development of control mechanisms *(Mean)* to enhance data sovereignty *(End).* Finally, we employ theories on trust and risk to examine data sovereignty impacts on the data economy (research question 6).

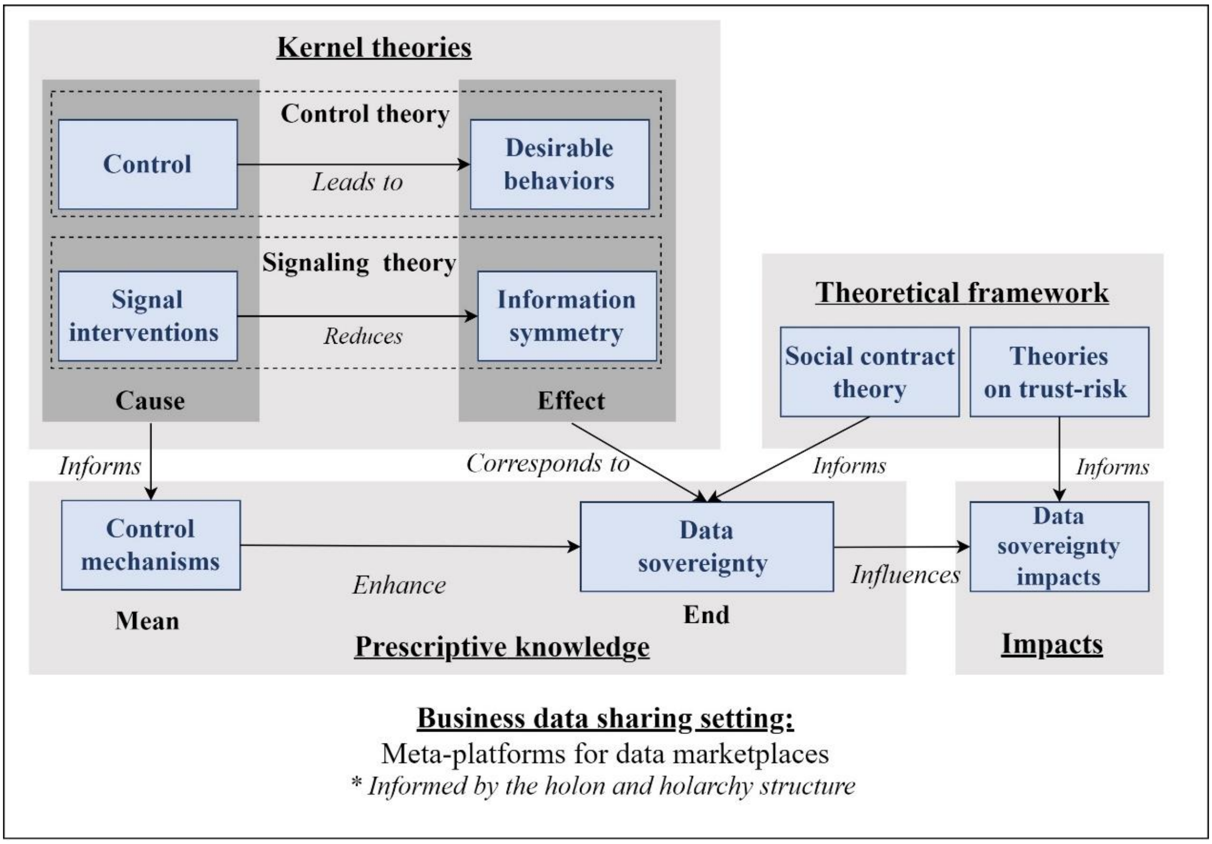


Figure 3.4. The role of theories in this study

Having elaborated on the research background, the next chapter will examine the value creation of meta-platforms in the data marketplace setting to address the first research question.

PART 2: THE PROBLEM SPACE

Chapter 4: Value Creation of Meta-Platforms in the Data Marketplace Setting[1]

The previous chapter discussed key concepts and theories fundamental to this study. We examined five concepts: data sharing, data marketplaces, meta-platforms, data sovereignty, and control mechanisms. Additionally, we explored five theories for understanding the descriptive and prescriptive knowledge guiding the creation of design knowledge: holon and holarchy structure, social contract theory, control theory, signaling theory, and theories on trust and risk.

This chapter explores the value creation of meta-platforms in the data marketplace setting. We address research question 1: *How do meta-platforms create value in the data marketplace setting?* This question arises from a lack of design knowledge about meta-platforms in the data sharing context (scientific gap 1). Meta-platforms in data marketplaces fundamentally differ from those in traditional digital platforms (e.g., gaming platforms), owing to the unique attributes of data products. The *weak appropriability regime* of data complicates protection against duplication (Zhu & Madnick, 2009). The *non-rival nature* of data allows for simultaneous use by multiple parties without diminishing availability (Koutroumpis et al., 2019). As an *intangible good*, the true value and quality of data only emerge through utilization (Koutroumpis et al., 2020). Addressing this research question provides a contextual foundation that guides the subsequent exploration of design knowledge in the problem, solution, and evaluation domains. We address this question by employing a two-step exploratory qualitative study.

Section 4.1 outlines the research approach guiding the exploration of meta-platform[2] value creation. In Section 4.2, we present the results from the two steps of our study: Step 1, which covers the structure and strategic positioning of meta-platforms along with interaction scenarios, and Step 2, which focuses on value creation themes and archetypes. Subsequently, Section 4.3 connects value creation archetypes with meta-platform strategic positioning to further examine the characteristics of each archetype. Section 4.4 selects a value creation archetype of meta-platforms as a data sharing context for this study. Finally, Section 4.5 concludes this chapter.

4.1 Research approach: Explorative qualitative study

We conduct an exploratory qualitative study because very little is currently known about value creation of meta-platforms. This approach is common for researching emerging phenomena (Sekaran & Bougie, 2016). This exploratory study comprises two steps: 1) conceptual framing and 2) semi-structured interviews.

[1] Parts of this chapter are based on the following publication:
Abbas, A. E., Ofe, H., Zuiderwijk, A., & de Reuver, M. (2023). *Toward Business Models for a Meta-Platform: Exploring Value Creation in the Case of Data Marketplaces*. The 56th Hawaii International Conference on System Sciences (HICSS), Honolulu, Hawaii, the United States.

[2] For the remainder of this chapter, the term *meta-platform* always refers to meta-platforms in the data marketplace setting for business data sharing, unless stated otherwise.

In the first step, we used the holon and holarchy lens to structure meta-platforms, which is vital to conceptualizing such meta-platforms in the data marketplace setting (Step 1.1). Without a precise conceptualization, meta-platform interpretations may vary during semi-structured interviews, leading to interviewees discussing disparate ideas under the same terminology. Such inconsistencies can impact the validity of our study. Afterward, we examined the strategic positioning of meta-platforms based on the holon interactions. This analysis informs the examination of value creation archetypes in meta-platforms (Step 1.2). Building on examples from conventional digital platforms, we then explored interaction scenarios explaining how data providers and consumers engage in meta-platforms (Step 1.3). Understanding interaction scenarios is crucial to specific data sharing processes in meta-platforms, informing prototype development.

In the second step, we conducted semi-structured interviews to explore meta-platform value creation archetypes (Step 2). Adapting Piccoli and Pigni (2013), we refer to value creation archetypes as a generalized, high-level blueprint to portray the value creation focus of a meta-platform. An archetype consists of multiple interrelated value creation themes. We developed archetypes because our participants tend to interpret a meta-platform differently. The following sections detail the approach for conducting semi-structured interviews.

4.1.1 Sampling strategy

We utilized the *purposive sampling strategy, s*pecifically *judgment sampling,* to select our interview participants by considering their expertise. This sampling strategy was appropriate as we investigated a novel phenomenon that only a few individuals were knowledgeable about (Etikan et al., 2016; Sekaran & Bougie, 2016); therefore, we selected individuals capable of offering the necessary insights.

We targeted two main groups: business data sharing consultants and meta-platform experts. These consultants promote and engage with business data sharing for their organizations, while the experts participate in interoperable data marketplace projects. As meta-platforms do not exist (yet) for data marketplaces, the industry apparently does not have the incentives to think about creating meta-platforms. Therefore, we interviewed people who were forced to think about meta-platforms because the European Union (EU) incentivizes them to do so in funded projects.

Our participant criteria included: 1) familiarity with meta-platforms and data marketplaces (i.e., knowledge of, experience with, or consideration of), 2) experience in decision-making processes, especially business models, and 3) proficiency in English. Leveraging our networks in EU data sharing projects, we identified twenty interviewees (I-01 to I-20) and stopped once code saturation was achieved. Our participants comprised fourteen (internal or external) business data sharing consultants and six meta-platform experts (Table 4.1). We verified participants' expertise by looking at their public professional profiles (e.g., via LinkedIn) and asked them to share their experience for business data sharing during the interview. Interviews were held online via Microsoft Teams from July to November 2021, averaging 40 minutes each.

Table 4.1. The overview of interviewees

ID	Role	Core relevant experience	Overall work experience (in years)
I-01	Director of innovation	Involved in multiple data sharing projects (e.g., meta-platforms, data marketplaces) and relevant underlying technologies (e.g., privacy-preserving technologies).	28
I-02	Security solution manager	Working on data loss prevention technologies for data sharing.	18
I-03	Product owner	Leading the commercialization of a data sharing platform.	14
I-04	Head of standard business reporting	Leading the implementation of data sharing technologies.	23
I-05	Project manager	Leading multiple projects on the topic of interoperable digital platforms.	10
I-06	Commercial director	Building digital platforms for clients focusing on digital goods.	24
I-07	Chief data officer	Responsible for shaping data policies, including business data sharing with external parties.	12
I-08	Technical innovation manager	Managing a technical lab to explore the newest data sharing technology, such as quantum computing or multi-party computation.	28
I-09	Data protection specialist	Analyzing legal aspects of data sharing.	3
I-10	Head of architecture, innovation, and technology	Exploring the newest technological advancement for data sharing (e.g., blockchain).	16
I-11	Senior strategy manager	Managing the business-to-business stream of a large company, which includes data sharing activities.	32
I-12	Product owner	Leading the commercialization of data analytic platforms.	11
I-13	Risk manager	Conducting risk assessments for data sharing.	5
I-14	Senior consultant	Providing consultancy services in interoperability-related aspects, such as ensuring data portability in digital platforms.	22
I-15	Associate director	Providing consultancy services on information technology outsourcing where business data sharing plays a pivotal role.	24
I-16	Technical researcher	Researching technical aspects of business data sharing, for example, semantic web technologies, metadata management, or vocabulary management.	9
I-17	Deputy studio director	Leading an initiative to explore the interoperability of data marketplaces.	13
I-18	Data science director	Managing a portfolio of data science projects, including business data sharing.	12
I-19	Project manager	Involved in multiple data sharing projects (e.g., meta-platforms, data marketplaces).	19
I-20	Project manager	Developing use cases for business data sharing.	9

Table 4.1 lists our interviewees, who predominantly have mid to senior management roles, with an average work experience of seventeen years. Our sample contains a varied and balanced range of expertise, including strategic roles (e.g., director of innovation, chief data officer, commercial director), technical positions (e.g., technical researcher, technical innovation manager), project management, and legal roles (e.g., data protection specialist, risk manager).

Most of our interviewees are professionals from either the telecommunication or financial sectors.

4.1.2 Interview protocol

We began our interviews with introductory questions about job experience, familiarity with business data sharing, and knowledge of data marketplaces. Then, we presented a meta-platform conceptualization with an interaction scenario between a data provider and a data consumer to ensure a shared conceptual understanding (see Section 4.2.1.3, *Scenario 2 – Supply-side users directly connect to a meta-platform*). We chose this interaction scenario to emphasize the perspectives of the data providers, who are the problem owners of data sovereignty concerns (see the rationale in Section 4.4). To validate our presentation, we conducted two pilot interviews with experts in data sharing projects. However, the presentation approach might introduce bias, as interviewees' responses depend on our explanation of meta-platforms. Thus, we made the explanation consistent across interviews, reducing potential bias. Moreover, discussing meta-platform conceptualization is essential at this exploration stage due to limited known instances in real-life settings.

Following the presentation, we invited interviewees to discuss and clarify the meta-platform conceptualization and scenario, often leading to discussions on value creation and potential challenges. Finally, our main question asked how a meta-platform can create value in the data marketplace context, particularly how it could benefit the three primary stakeholders of a meta-platform: data marketplace operators, data providers, and data consumers. Appendix 1 details the interview protocols.

4.1.3 Data analysis

We analyzed our interview transcripts in two-phase coding (Saldaña, 2016): Open and pattern coding. In open coding, we inductively annotated potential value creation as first-order codes. We analyzed to which stakeholder these first-order codes belong. This step is essential to clarify to whom meta-platforms create value. In pattern coding, we grouped these codes into second-order codes. Afterward, we engaged with digital platform literature to develop value creation archetypes (See Section 4.2.2.2). Finally, we assigned the second-order codes to the most appropriate value creation archetype.

We describe the code procedures in a *data structure* presented in Figure 4.3. To illustrate the coding processes, consider this excerpt from a participant (I-01):

> *"When I have several [data marketplace] options in front of me and have to evaluate the existence, the inclusion of a data marketplace in a meta-platform, it could be a plus to evaluate. If I have to make three to four choices, I would make the choice that has the biggest outlook in the market."*

We coded this excerpt into the first-order code of *finding the data marketplace with the biggest outlook*. This value enables *data providers* to assess and compare data marketplaces by their market potential. We grouped this first-order code with related ones, such as *acting as an advertising agency* and *understanding data demand* to the *promoting* second-order code. This grouping reflects an abstraction of ways to promote data products of data providers appropriately.

We further grouped the second-order code of *promoting* to the value creation archetype of *brokerage*. This grouping differentiates the *brokerage* from other archetypes: *discovery aggregators*, focusing on search and dispatch value, and *one-stop shop*, integrating services within a single interface. Unlike the automated or algorithm-driven processes in other archetypes, the distinct characteristic of the *brokerage* archetype is its reliance on human interaction and expertise based on knowledge in a meta-platform. Therefore, grouping *promoting* to the *brokerage* is appropriate, as it covers personalized data provider needs that demand understanding beyond the capabilities of automated systems.

To enhance the reliability of our analysis, we conducted an intercoder reliability assessment. This process ensured the consistent application of our coding procedures. The first coder was the PhD candidate, while the second was a senior colleague with expertise in digital platform research and qualitative studies. Overall, the coders showed a strong consensus.

4.2 Findings

The previous section outlined the research approach for this chapter, consisting of two steps: 1) conceptual framing and 2) semi-structured interviews. The subsequent sections present the findings for each step.

4.2.1 Findings from the conceptual framing (Step 1)

4.2.1.1 A meta-platform structure

Figure 4.1 illustrates a meta-platform structure based on the holarchy structure discussed in Chapter 3. We adapted this figure from Wang (2021), who uses the holarchy structure to conceptualize digital innovation ecosystems. Our adaptation included adjustments to the holon description to make the figure appropriate in the meta-platform context. This structure is characterized by a network of autonomous, self-regulated holons, each demonstrating varying levels of flexibility and self-sufficiency.

In the meta-platform context, a meta-platform itself functions as a top-level holon. Data marketplaces within a meta-platform represent mid-level holons. These marketplaces maintain operational independence, serving user groups that comply with their specific guidelines. Simultaneously, they align with agreed operation rules with a meta-platform, thereby encapsulating a holon’s dual role: an independent entity and a part of a broader system. On a lower level, data providers, data consumers, and third-party providers are holons within a data marketplace. They retain operational independence yet are influenced by a broader marketplace holon. The atomic-level holons, represented by data products and services, are the foundational elements of the entire meta-platform. This structure strikes a balance between centralized control and localized autonomy.

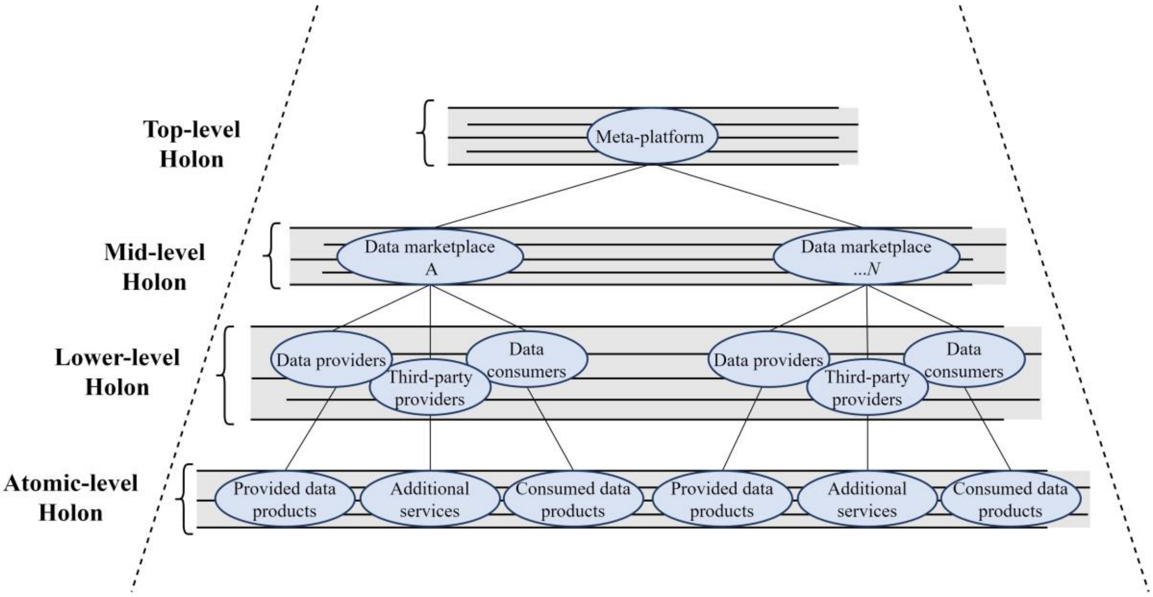


Figure 4.1. Structuring a meta-platform based on the holon and holarchy lens (adapted from Wang, 2021)

4.2.1.2 A spectrum of meta-platform strategic positioning

Strategic positioning involves distinguishing oneself from competitors through unique business model configurations (Casadesus-Masanell & Ricart, 2010; Porter, 2001). Examining strategic positioning helps analyze value creation archetypes, potentially clarifying the focal value proposition (e.g., Dobni, 2010; Husted et al., 2015). To explore strategic positioning, we can examine the interaction between holons. These interactions follow three primary principles: a) exerting *influence* on smaller holons below, b) *integrating* into a broader holon at a higher level, and c) engaging in competitive or collaborative *motives* with other holons on the same level (Velikovsky, 2016). Based on these principles, we describe two opposed strategic positions: *independent cohesion* and *holistic synergy*.

Independent cohesion is a strategic position where a meta-platform exerts *minimal influence*, allowing data marketplaces to largely maintain their autonomy. By nature, this position only requires *low integration* between meta-platforms and participating data marketplaces. With minimal influence and low integration, the focal value proposition of meta-platforms is to provide a *core aggregator service*, facilitating comparisons between various offerings from data marketplaces.

Data marketplace operators' motivation to align with meta-platforms is to capitalize on the inherent *competitiveness* of the data marketplace landscape. They recognize the market's competitive nature and, by joining a meta-platform, choose to participate in this competitive environment rather than avoid or downplay competition.

Trivago, a metasearch engine that gathers information from various hotel booking platforms, illustrates this strategic positioning. As a meta-platform, Trivago focuses on its focal value proposition: providing hotel price comparisons and recommendations. This positioning enables participating hotel booking platforms to remain operationally independent while benefiting from increased exposure.

On the other end of the spectrum of meta-platform strategic positioning is *holistic synergy*, which signifies a strategy where a meta-platform exerts a *high influence*. This strategic positioning requires *a high level of integration* between a meta-platform and data marketplaces because the focal value proposition is to provide *multiple service aggregators.* Thus, the focal value proposition extends beyond the core aggregator service (i.e., comparison). This approach allows end users to utilize a wide range of services without leaving the meta-platform, thereby enriching the user experience.

Table 4.2. A spectrum of meta-platform strategic positioning

Characteristic	**Strategic positioning**	
	Independent cohesion <———>	*Holistic synergy*
Meta-platform's influence	Low	High
Degree of integration	Low	High
Meta-platform's focal value proposition	Core aggregator service	Multiple aggregator services
Participating platforms' motive to align with a meta-platform	Competition between participating platforms	Collaboration between participating platforms
Case example	Trivago[3]	CORE MaaS[4]

Data marketplace operators join meta-platforms motivated by *collaboration*. They share a vision of leveraging collective technological capabilities with other participating marketplaces. For example, the collaboration between Iomob Technology Services[5] and Factual[6] to form "COvid-19 REsilient Mobility as a Service" (CORE MaaS) illustrates this strategic positioning. In response to the COVID-19 crisis, these companies formed a meta-platform that aggregates multiple mobility service providers (Floetgen, Strauss, et al., 2021). This collaboration showcases the effective strategy of high-degree integration by offering a comprehensive, safe, and reliable mobility solution during the crisis. Their success demonstrates how such a cooperative mindset can foster resilience during challenging times. Table 4.2 summarizes the spectrum of meta-platform strategic positioning.

4.2.1.3 Interaction scenarios between data providers and consumers

According to the holon and holarchy lens, the next step after defining the holarchy structure is to examine holon interactions (e.g., Wang, 2021). These interactions clarify the engagement between two critical actors sharing data products: providers and consumers. The interaction scenarios depend on the original registration of the providers or consumers, forming a 2x2 grid (Table 4.3). The following explanation for each scenario is as follows.

1. *Scenario 1 (Dual-sided direct connection via a meta-platform):* a data provider and a data consumer are registered in a meta-platform, enabling them to interact directly with

[3] https://www.trivago.com/, accessed on 22 January 2024.

[4] https://www.polisnetwork.eu/article/urban-mobility-company-core-maas-a-social-distancing-mobility-platform/, accessed on 22 January 2024.

[5] https://www.iomob.net/, accessed on 22 January 2024.

[6] https://factual-consulting.com/, accessed on 22 January 2024.

this meta-platform. In this scenario, the meta-platform serves a dual function: it acts as a federator integrating other marketplaces and simultaneously operates as a data marketplace itself.

2. *Scenario 2 (Supply-side users directly connect to a meta-platform):* Like how a hotel may use a meta-platform (e.g., Mirai[7]) to increase visibility across hotel booking platforms, a data provider joins a meta-platform for greater visibility to numerous data marketplaces at once.
3. *Scenario 3 (Demand-side users directly connect with a meta-platform):* Just as travelers utilize Trivago to search for accommodations across diverse booking platforms, a data consumer joins a meta-platform to search for data products from providers in multiple marketplaces.
4. *Scenario 4 – (Cross marketplace interaction):* a data provider registered in a data marketplace directly shares data products with a consumer registered in another data marketplace (or vice versa). Both parties only engage with their respective marketplaces. This scenario reflects the ability of a meta-platform to facilitate cross-marketplace interactions.

Table 4.3. Four interaction scenarios in a meta-platform

		Data consumers registered in	
		Meta-platform	**Data marketplace**
Data providers registered in	**Meta-platform**	*Scenario 1* *(Dual-sided direct connection via a meta-platform)*	*Scenario 2* *(Supply-side users directly connect to a meta-platform)*
	Data marketplace	*Scenario 3* *(Demand-side users directly connect with a meta-platform)*	*Scenario 4* *(Cross marketplace interaction)*

Figure 4.2 visually represents the four interaction scenarios between data providers and consumers within a meta-platform.

[7] https://www.mirai.com/what-we-do/metasearch-connectivity/, accessed on 15 February 2024.

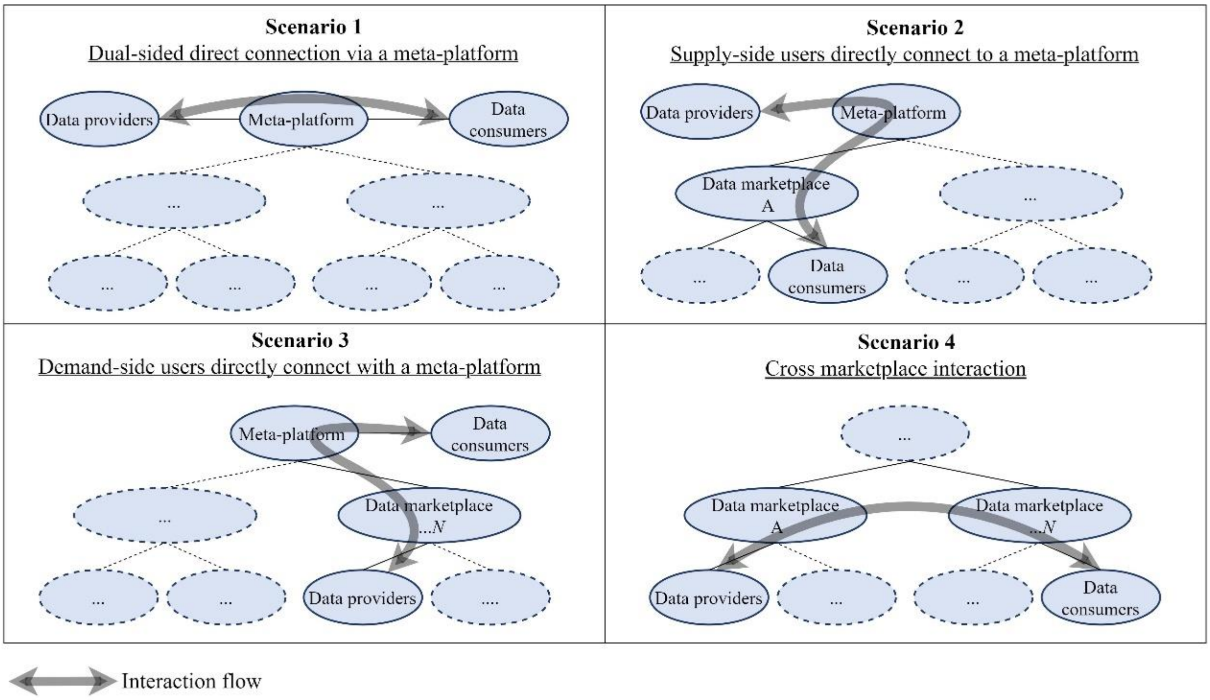


Figure 4.2. Four user interaction scenarios in a meta-platform

4.2.2 Findings from the semi-structured interviews (Step 2)

In Step 1 (conceptual framing), we utilized the holon and holarchy lens to structure meta-platforms (Section 4.2.1.1) and discussed the potential strategic positioning of meta-platforms (Section 4.2.1.2). Moreover, we revealed interaction scenarios between data providers and consumers in meta-platforms (Section 4.2.1.3). These insights enable us to move to Step 2 (semi-structured interviews), examining value creation of meta-platforms. We discover three value creation archetypes of a meta-platform for data marketplaces: *discovery aggregator*, *brokerage*, and *one-stop shop*. We discuss the value creation of each archetype in the following subsections, including the logic of how we derived these archetypes.

4.2.2.1 Value creation themes

Based on the interview findings, this section explores value creation themes for a meta-platform for data marketplaces. The *theme* here refers to the second-order code. In summary, eight value creation themes emerge from the analysis.

The first value creation theme for a meta-platform is searchability. A meta-platform facilitates homogenized *searching data* across multiple marketplaces, creating value for data consumers. One participant (I-19), for instance, illustrated this point:

> *"Searching data between these [data marketplaces] should be homogenized [by a meta-platform]. We need a data naming, for instance, to find a common way to describe the dataset. So, when we search a dataset, we can find the same kind of databases in different data marketplaces [...] At least from my perspective, many different stakeholders could interact, and we should find a universal or common way to name the different datasets. So, everyone interacting in their system could find what they are looking for."*

Another value creation theme is dispatching, where data providers transfer *their metadata descriptions* for greater visibility across multiple marketplaces; as one interviewee (I-17) explained: *"If I understand it correctly, it should be the metadata descriptions that are interoperable. We only show the metadata that other data marketplaces provide but do not necessarily have the datasets or data assets."* Data providers can also *receive requests* from consumers in many data marketplaces. The same participant (I-17) clarified this, noting that: *"Interoperability between other data markets means that we [as a meta-platform] provide interfaces that other data markets can use to exchange data with [an EU data market project], which means that they can upload metadata about their datasets so that users of [an EU data market project] can also see the offers from other data markets."*

A meta-platform can also create value by performing promoting tasks for data providers, such as *acting as an advertising agency.* One participant (I-03) commented: *"So, if you look, for example, from a meta-platform point of view, I would rather see them [meta-platforms] as an advertising agency."* Moreover, a meta-platform should be able to analyze transaction data to *inform data demands* for data providers, as one interviewee put it:

> *"As a provider, you know or have an idea, at least, where your data is residing or know if there are any demands of your data on the different platforms [...] that you have insights in the usage or potential use." (I-10)*

Additionally, the following comment exemplifies how a meta-platform adds promotional value by *showcasing data sharing use cases*, thus demonstrating the tangible benefits of data sharing for both data providers and consumers:

> *"It is a showcase of what [a data provider] can do, and when someone [data consumers] wants to do something with them, they will go directly to [a data provider] or through the marketplace." (I-08)*

A meta-platform can support data providers and consumers, for example, by providing *data pricing assistance* to help them get the most optimum price. Interviewee (I-11) explained: *"If you [data providers] share the data, you do not know what it is worth because you have no idea yet [...] You want to share it at a price that reflects the value to the buyer [...] [If data consumers are interested] you do not know if they make a realistic offer or not. Then, a meta-platform could say, looking at earlier or similar transactions, that this is a realistic price."*

Another potential support relates to *onboarding processes.* As interviewee I-02 described, "*Customers [data providers or consumers] need to register with us [a data marketplace], enroll to our rules, get a contract with us, etc. That could be a bit too much of a hassle, so a meta-platform could significantly ease this process."*

The next identified value theme is standardizing. A meta-platform provides *standardized integration services* for data marketplaces, such as via Application Programming Interfaces (APIs). Participant (I-08) stated: *"You get a meta-platform to find everything and get the standardization of the APIs to eventually get that data."* Furthermore, a participant (I-18) emphasized the importance of including shared services, such as billing schemas, in the meta-platform offering.

> *"Maybe there can also be some interoperability in terms of the pricing. Maybe there can be interoperability in terms of whether you can purchase access to the data set of one platform and you can purchase it through another platform."*

Another value creation theme is regulating, including *self-regulating* endeavors between a meta-platform and data marketplaces. Participant (I-12) elaborated on this, stating:

> *"Sometimes, we see that as a public opinion coming, and we can better organize ourselves for fraud prevention and cyber security [via self-regulating]. We really are looking into it ourselves because criminal activities are quicker than the legislator can exactly tell what we should do about it. So, we try to find out what to do."*

The same participant (I-12) also raised a concern about multiple *membership schemas,* so a meta-platform can create value for data providers and consumers by bridging this gap:

> *"The interesting thing is when you are going to set up a relationship with a data marketplace, you have specific requirements to fulfill. For example, if some customers are connected to data marketplace A, but you want to expose it to as many data marketplaces as possible, you have to comply with the differences of technical or certification requirements."*

Additionally, the regulating theme includes establishing *a central register of data marketplace users* to track violations of the data marketplace code of conduct. This will help data providers and consumers interact with trusted businesses. One participant commented (I-19)*, "Not anybody should interact in such a meta-platform because people who want to share data need to trust who is behind it. For example, it is important to consider the legal aspects and how to check if the company demanding data [data consumers] has no criminal records."*

A meta-platform can also facilitate sharing *features* between data marketplace, for example*, computational resources*. A participant (I-17) illustrated this idea:

> *"Computing resources probably can be exchanged. There is someone who has a lot of computational resources like GPU stuff that they just put it online and then on [a data marketplace] can use. You can rent this infrastructure."*

Finally, we discover another theme: developing *programming ecosystems* (or sandbox environments) for data consumers experimenting with data products. Participant (I-17) said:

> *"A meta-platform can provide a programming ecosystem, maybe a development ecosystem where data experiments are possible."*

In conclusion, we find eight value creation themes for a meta-platform in the data marketplace setting: searching, dispatching, promoting, supporting, standardizing, regulating, sharing, and experimenting.

4.2.2.2 Value creation archetypes of a meta-platform

This section describes the archetypal ways in which meta-platforms create value. We develop archetypes because our participants tend to interpret a meta-platform differently. One interviewee (I-18) indicated*: "I think there are different levels of what [a meta-platform] means. At the moment, we are completely at the beginning of the journey."* Exploring these archetypes is crucial as they determine the object of sovereignty (see Chapter 1 Section 1.4). Therefore, we will select one archetype to focus on as the data sharing context of this study (Section 4.4).

Figure 4.3 connects meta-platform value creation to relevant archetypes: discovery aggregator, brokerage, and one-stop shop. The first value creation archetype for a meta-platform is the *discovery aggregator*. According to digital platform literature, aggregators collect, analyze, and offer insight from multiple data sources (e.g., Garbuio & Lin, 2019). The discovery aggregator archetype is not focused on the role of orchestrating but rather on creating new connections between platforms. Hence, rather than enforcing strict regulations, this archetype allows participating participants to decide their path and niche (Mikołajewska-Zając et al., 2021).

In the context of our study, the discovery aggregator archetype can emphasize searching and dispatching value. Consequently, this archetype can focus on providing metadata interoperability with (and among) data marketplaces. The meta-platform task is finished after redirecting data providers and consumers to relevant data marketplaces. In this regard, data providers (or consumers) must register with relevant data marketplaces (and perform transactions) by themselves. This archetype represents the simplest way a meta-platform can create value. The below comments illustrate:

> *"So, the minimum feature is not far. It is quite close, within reach. And I think it has to do with discovery, definitely." (I-16)*

> *"I think in the very minimum case, you need to transfer the metadata." (I-08)*

The second value creation archetype for meta-platforms is *brokerage*. Unlike the discovery aggregator, the brokerage archetype focuses on managing business relationships (Garbuio & Lin, 2019). With its deep expertise, the brokerage archetype offers consulting services to solve specific clients' problems (Palmié et al., 2021). For example, brokerage can simplify transactions or provide capacity-building activities to improve skills (Komninos et al., 2021).

In our study, the brokerage archetype can focus on promoting and supporting value. This archetype provides value (e.g., pricing supports) to optimize business data sharing based on a) transaction insights (e.g., data demands) and b) meta-platform expertise (e.g., experience in successful use cases). In doing so, this archetype also needs metadata interoperability with participating data marketplace. After finding the desirable data marketplaces, this archetype can provide onboarding support to help users perform transactions.

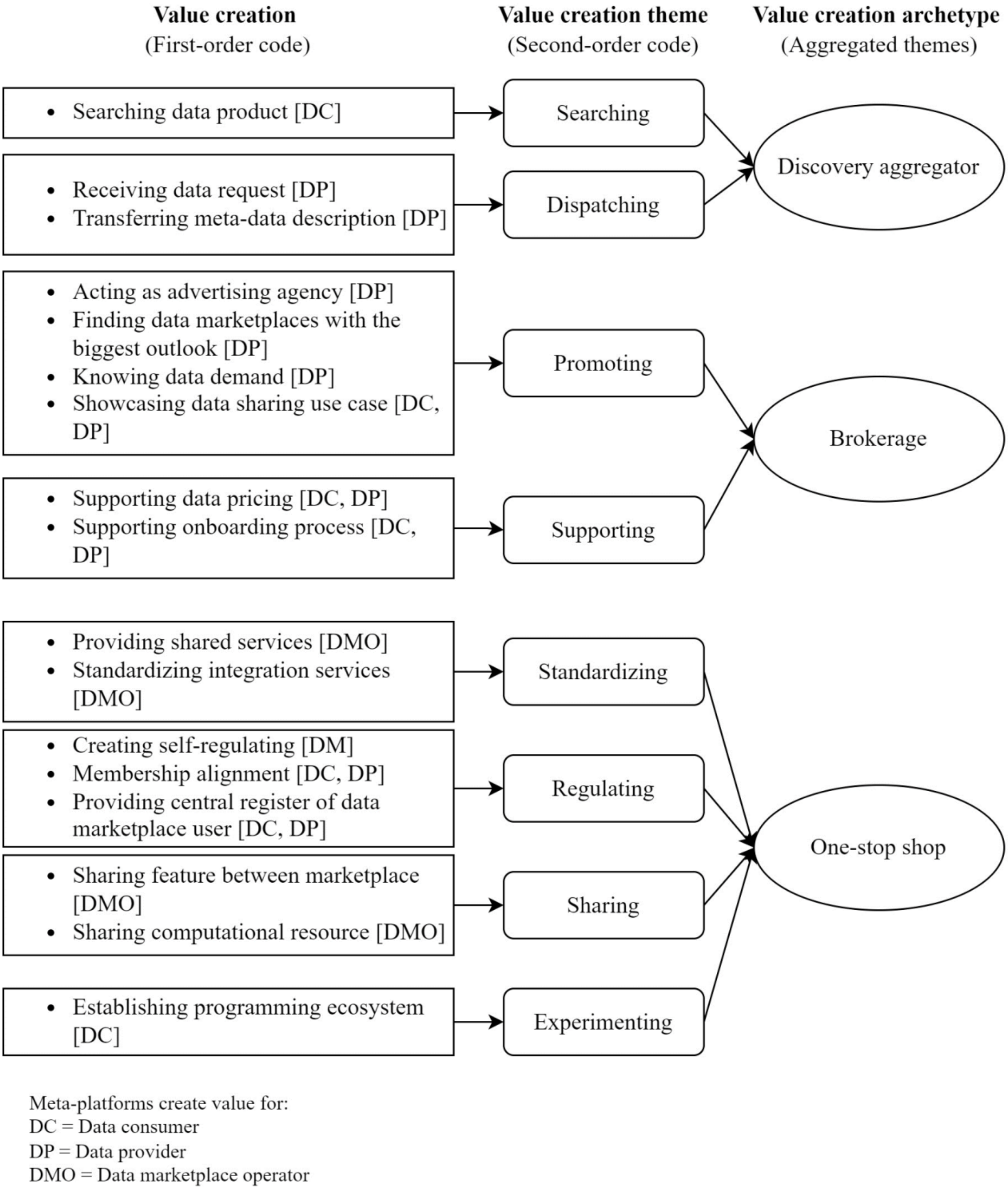

Value creation
(First-order code)
Value creation theme
(Second-order code)
Value creation archetype
(Aggregated themes)
• Searching data product [DC]
• Receiving data request [DP]
• Transferring meta-data description [DP]
• Acting as advertising agency [DP]
• Finding data marketplaces with the biggest outlook [DP]
• Knowing data demand [DP]
• Showcasing data sharing use case [DC, DP]
• Supporting data pricing [DC, DP]
• Supporting onboarding process [DC, DP]
• Providing shared services [DMO]
• Standardizing integration services [DMO]
• Creating self-regulating [DM]
• Membership alignment [DC, DP]
• Providing central register of data marketplace user [DC, DP]
• Sharing feature between marketplace [DMO]
• Sharing computational resource [DMO]
• Establishing programming ecosystem [DC]
Searching
Dispatching
Promoting
Supporting
Standardizing
Regulating
Sharing
Experimenting
Discovery aggregator
Brokerage
One-stop shop
Meta-platforms create value for:
DC = Data consumer
DP = Data provider
DMO = Data marketplace operator

Figure 4.3. Value creation archetypes of a meta-platform

The final value creation archetype of meta-platforms is the *one-stop shop*. This archetype offers fully integrated services, allowing end users to access cross-platform services independently through a standardized portal (Floetgen, Strauss, et al., 2021). Floetgen, Strauss, et al. (2021) reveal that the one-stop shop results from a joint alliance between participating platforms, with a meta-platform orchestrating the integration efforts and participating platforms pooling their resources.

In our study, the one-stop shop creates value in the data marketplace setting by standardizing, sharing, regulating, and experimenting. With a higher level of integration, it is possible to be interoperable beyond the mere metadata, such as the actual data products, along with payment and contract interoperability. In the one-stop shop, data providers and consumers do not have to register with specific marketplaces to conduct transactions. They can perform the actual transaction without leaving a meta-platform or their preferred marketplaces. To sum up, we found three value creation archetypes of meta-platforms in the data marketplace setting: discovery aggregator, brokerage, and one-stop shop.

4.3 Connecting value creation archetypes with meta-platform strategic positioning

Value creation archetypes (Section 4.2.2.2) and strategic positioning (Section 4.2.1.2) can be connected, with each archetype aligning with a specific position on the strategic positioning spectrum (see Figure 4.4). Examining this connection is crucial to linking back the archetype we found in the semi-structured interviews to the conceptual lens of holon and holarchy, which further explain the archetypes' characteristics. We discuss this alignment, focusing on several aspects discussed in Section 4.2.1.2: focal value proposition (core vs. multiple), degree of influence (low vs. high), degree of integration (low vs. high), and data marketplace operators' motives for joining a meta-platform (competition vs. collaboration). We also interpret the object of sovereignty (i.e., the control focus) based on the discussion of this alignment.

This section focuses on aligning the discovery aggregator and one-stop shop archetypes. They are selected due to their positions at opposite ends of the meta-platform strategic spectrum, providing a basis for highlighting the unique characteristics of each value creation archetype. The brokerage archetype then exhibits characteristics that blend independent cohesion and holistic synergy.

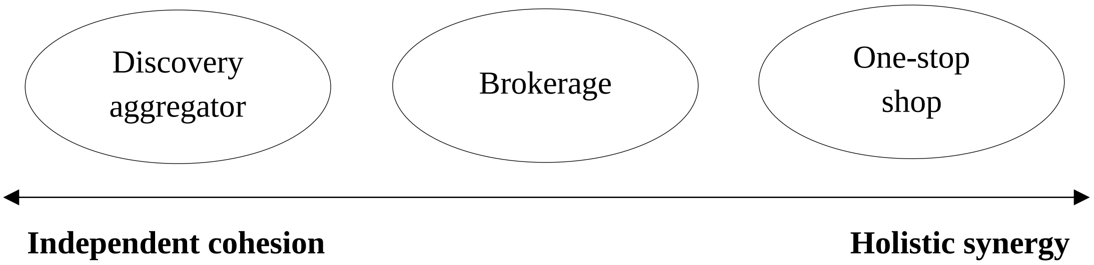


Figure 4.4. The mapping between value creation archetypes with meta-platform strategic positioning

At the left end of the spectrum lies the *discovery aggregator* archetype, corresponding to the *independent cohesion* strategic positioning. This archetype focuses on two key values: searching and dispatching. Searching value allows data consumers to explore data products across various marketplaces while dispatching value enables data providers to spread their metadata descriptions across multiple marketplaces. Hence, this archetype aligns with the independent cohesion strategic positioning, emphasizing its focus on *core aggregator service:* aggregating diverse metadata for participating platforms for product comparison.

Given the *minimal influence* of the meta-platform, data marketplaces aligning with the discovery aggregator largely preserve their autonomy. Alignments between a meta-platform and data marketplaces can be accomplished through *minimal integration*, typically by forming simple partnerships. In such partnerships, simple Application Programming Interfaces (APIs) facilitate bidirectional metadata sharing with data marketplaces, primarily for traffic redirection. If data consumers from a particular marketplace express interest, providers must register with that marketplace to enable a transaction, stepping beyond the meta-platform to interact directly with the marketplace. Adopting this approach facilitates technical feasibility by eliminating the requirement for intricate integrations.

Data marketplace operators align with the discovery aggregator archetype to harness the inherent *competitiveness* of the data marketplace landscape. They recognize the market's competitive nature and, by joining a meta-platform, choose to participate in this competitive environment rather than avoid or downplay competition. This strategic decision is driven by the opportunity to showcase their unique offerings on a meta-platform, thus enhancing their visibility. Since the discovery aggregator focuses on managing metadata disseminated across various data marketplaces, this meta-platform views *metadata* as an object of sovereignty.

The one-stop shop archetype is on the other end of the spectrum, which closely mirrors the *holistic synergy* positioning. The one-stop shop archetype focuses on consolidating various offerings into one unified user experience. This archetype creates value by standardizing (e.g., providing shared services), regulating (e.g., membership alignment), sharing (e.g., computational resources), and experimenting (e.g., establishing a programming ecosystem). Thus, the one-stop shop archetype aligns with the holistic synergy strategic positioning, emphasizing *multiple aggregator services.*

The one-stop shop archetype typically acts as an orchestrator; hence, it has *a high degree* of influence on data marketplaces. A meta-platform and data marketplaces need *a high degree of integration* due to extensive ranges of service alignments. Two main integration methods exist: partnerships with advanced APIs and ownership through adopted infrastructure. In the former case, a meta-platform provides advanced APIs beyond *pulling* metadata for listings and *pushing* updates. Therefore, advanced APIs facilitate direct data sharing across marketplaces, allowing providers and consumers to transact across different marketplaces within their preferred marketplace interfaces or through the meta-platforms themselves. In the latter case, data marketplaces must discontinue their existing systems and fully adopt the new technological infrastructure developed by a meta-platform.

Data marketplaces have *collaboration* motives driven by the shared goal of leveraging combined technological strengths to achieve specific objectives. Given the one-stop shop archetype's ability to facilitate data sharing beyond metadata, these meta-platforms view *data products* as objects of sovereignty. Table 4.4 summarizes the value creation of meta-platforms, focusing on the discovery aggregator and one-stop shop archetypes.

Table 4.4. Value creation for meta-platforms in the data marketplace setting

Characteristic	**Meta-platform archetype**	
	Discovery aggregator	**One-stop shop**
Strategic positioning	▪ Independent cohesion	▪ Holistic synergy
Focal value proposition	▪ Core service aggregator: Value is created by facilitating the searching and dispatching of metadata across multiple marketplaces	▪ Multiple service aggregators: Value is created by providing cross-marketplace services in a unified interface by standardizing, regulating, sharing, and experimenting
Meta-platform's influence	▪ Low	▪ High
Degree of integration	▪ Low: Low partnership–simple APIs to enable basic bidirectional metadata exchange with data marketplaces for traffic redirections	▪ High: High partnership–advanced APIs or ownership–adopted infrastructure ▪ Data marketplaces can both send *(push)* and receive *(pull)* data products from a meta-platform
Motives of data marketplace operators to align with a meta-platform	▪ Competition with other data marketplaces	▪ Collaboration with other data marketplaces
Object of sovereignty	▪ Metadata	▪ Metadata and data products

4.4 Specifying the data sharing context of this study

This study focuses on *the one-stop shop* value creation archetype. First, unlike the discovery aggregator, which primarily deals with metadata, the one-stop shop considers both metadata and data products as objects of sovereignty. This broader scope of data sovereignty is significant, encompassing the descriptive aspects of data (metadata) and the actual data content (data products). For data providers, data products are likely more crucial than metadata, especially as they contain strategic information that, if not properly managed, can diminish competitive advantages. Therefore, it is essential to choose a context where sovereignty issues are highly relevant to avoid underestimating the importance of data sovereignty.

Second, the one-stop shop presents a complex situation in maintaining data sovereignty due to the data provider's interaction with diverse data consumers in various marketplaces. The complexity arises from maintaining sovereignty in two layers: a meta-platform and data marketplaces. Conversely, in the discovery aggregator, data providers typically engage solely at the marketplace layer. This happens because the meta-platform's role concludes with directing them to a specific marketplace, after which data providers must interact directly with their chosen marketplaces. This choice highlights our interest in examining sovereignty in a complex environment like the one-stop shop, potentially leading to more insightful insights.

This study focuses on the one-stop shop within the second interaction scenario outlined in Section 4.2.1.3, where *supply-side users directly connect to a meta-platform.* We chose this focus because it centers on the perspective of data providers, the primary stakeholders in data sovereignty issues. By examining this scenario, we can demonstrate a) how data providers interact with consumers from multiple marketplaces through a meta-platform and b) how data sharing via a meta-platform may amplify data sovereignty concerns. To sum up, Figure 4.5 conceptualizes meta-platforms as the data sharing context of this study.

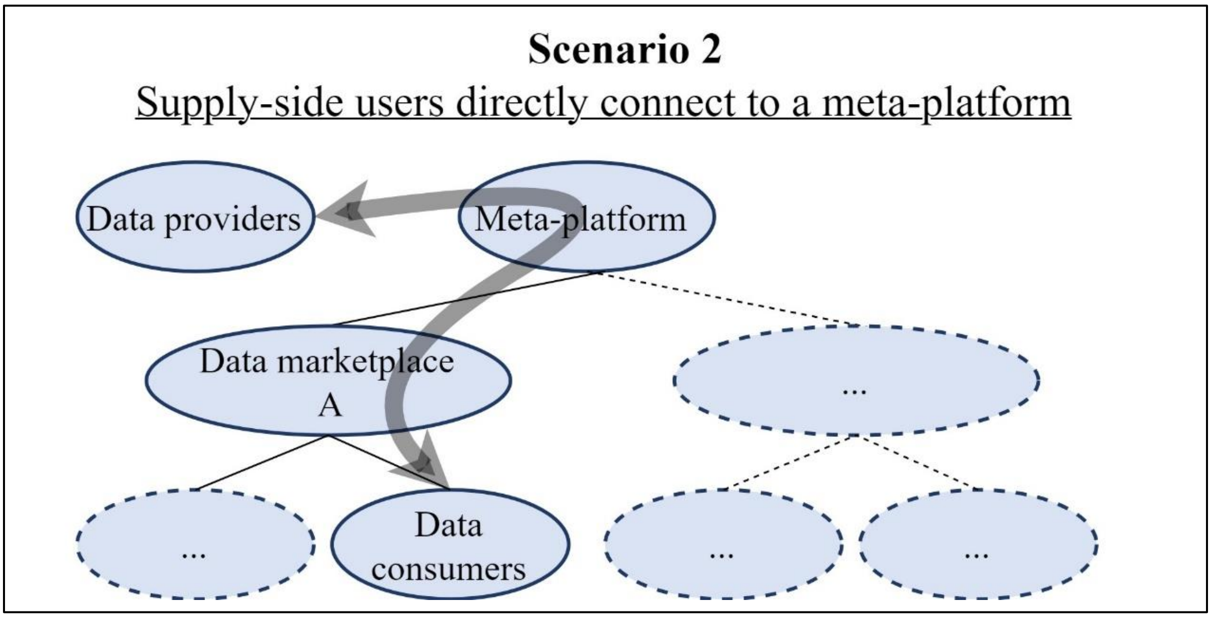


Figure 4.5. Meta-platform conceptualization employed in this study

4.5 Conclusion of Chapter 4

Chapter 4 answered the first research question of this study: *How do meta-platforms create value in the data marketplace setting?* We found three meta-platform value creation archetypes: discovery aggregator, brokerage, and one-stop shop. We then focused on discovery aggregators and one-stop shops, mapping these to the strategic positioning of meta-platforms. We chose these two archetypes because they represent contrasting ends of the strategic spectrum in meta-platforms, enabling a clearer understanding of the distinct characteristics of each value creation archetype. The brokerage archetype exhibits characteristics that blend independent cohesion and holistic synergy.

Discovery aggregators adopt *independent cohesion* in their strategic positioning. These meta-platforms have a focal value proposition of *core service aggregator*, creating value by facilitating the search and dispatch of metadata across various marketplaces. In this positioning, *a meta-platform influence is minimal*, and data marketplaces predominantly maintain their independence. Alignments between a meta-platform and data marketplaces can be accomplished through *minimal integration*, typically by forming simple partnerships and developing simple Application Programming Interfaces (APIs). *Competitive* motives drive the alignment of data marketplaces with these meta-platforms. Confident in their unique offerings, data marketplaces aim to differentiate themselves from the competition. Regarding the object of sovereignty, data providers focus on managing *metadata* disseminated across various data marketplaces.

In contrast, one-stop shops adopt a strategy of *holistic synergy* to deliver their focal value proposition of *multiple service aggregators.* They create value by offering cross-marketplace services through a unified interface involving standardization, regulation, sharing, and experimentation. To realize these services, high integration between the meta-platform and data marketplaces is essential. Two integration methods exist: partnerships with advanced APIs and ownership through adopted infrastructure. Advanced APIs in one-stop shops go beyond basic functions, enabling direct data sharing across marketplaces and allowing transactions within preferred marketplace interfaces or directly through the meta-platform. Alternatively, data marketplaces may need to abandon their existing systems to adopt a new technological framework fully developed by the meta-platform. This approach is driven by *collaborative* motives from data marketplace operators to leverage technological capabilities collectively. The one-stop shop archetype's capacity to extend data sharing beyond metadata positions data products as an object of sovereignty.

The remainder of this study focuses on the one-stop shop value creation archetype as a business data sharing context. Specifically, we focus on the second interaction scenario*: Supply-side users directly connect to a meta-platform.* Moving forward, Chapter 5 will explore data sovereignty facets by considering the context explored in this chapter.

Chapter 5: Data Sovereignty Facets[1]

The previous chapter explored the value creation of meta-platforms in the data marketplace setting. Among various types of value creation archetypes, this dissertation focuses on the one-stop shop meta-platforms, creating value by standardizing (e.g., providing shared services), regulating (e.g., membership alignment), sharing (e.g., computational resources), and experimenting (e.g., establishing a programming ecosystem).

Chapter 5 explores what data sovereignty means in one-stop shop meta-platforms. We address research question 2: *What are the key facets of data sovereignty in business data sharing through meta-platforms for data marketplaces?* This question arises from a lack of clear design knowledge for defining goodness criteria for guiding and evaluating control mechanism designs, primarily due to the ambiguity surrounding the concept of data sovereignty in meta-platforms[2] (scientific gap 2). Addressing the second research question establishes foundational design knowledge in the problem space domain, which in turn informs the subsequent solution and evaluation domains. To address this question, we employ an exploratory qualitative approach comprising conceptual framing and semi-structured interviews.

In Section 5.1, we detail our research approach. Section 5.2 presents findings from Step 1, contextualizing social contract theory in the data sovereignty context. Section 5.3 discusses the results from our semi-structured interviews conducted in Step 2. We focus on two main aspects of data sovereignty. First, Section 5.3.1 explores the substantive elements, which include Protection, Provision, and Participation. Then, Section 5.3.2 examines the spatial aspects, specifically the contextual conditions surrounding data sovereignty. Finally, Section 5.4 concludes this chapter.

5.1 Research approach: Explorative qualitative study

Chapter 5 employs an exploratory qualitative approach. This approach excels in studying emerging phenomena that require contextualization and interpretation (Glesne, 2016). Chapter 5 involves two stages: conceptual framing and semi-structured interview.

In the first step, we contextualized Social Contract Theory (SCT) to data sovereignty. SCT originates from political science, positing that individuals sacrifice some freedoms to a governing entity for societal benefits (Friend, 2004). In data sovereignty, data providers agree to certain compromises. For instance, they adhere to predefined data sharing protocols. In

[1] Parts of this chapter are based on the following publication:
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(20), 1-21. https://doi.org/10.1007/s12525-024-00695-2.
Abbas, A. E., Ofe, H., Zuiderwijk, A., & de Reuver, M. (2022). *Preparing Future Business Data Sharing via a Meta-Platform for Data Marketplaces: Exploring Antecedents and Consequences of Data Sovereignty*. 35th Bled eConference - Digital Restructuring and Human (Re-Action), Bled, Slovenia.

[2] For the remainder of this chapter, the term "meta-platform" always refers to one-stop shop meta-platforms in the data marketplace setting for business data sharing, unless stated otherwise.

return, they receive benefits offered by platform operators, such as the ability to control their shared data. Such trade-offs between freedoms and benefits mirror the principle of SCT. Hence, SCT is an appropriate analytical tool to examine the unexplored facets of data sovereignty in data sharing. Nevertheless, SCT has not been applied in data sovereignty research before, necessitating SCT contextualization for this study.

In the second step, we conducted semi-structured interviews to examine the substantive aspect of data sovereignty. This step was essential, as even after contextualizing SCT to data sovereignty, the substantive aspects remained unclear, warranting further empirical investigation.

5.1.1 Data source

We utilized data from semi-structured interviews in Phase 1 (Chapter 4), which covered not only value creation of meta-platforms but also data sovereignty concerns. To recap, the interview protocol of Phase 1 consisted of three parts. First, we asked about the interviewee's background and knowledge of data marketplaces. Second, we presented the conceptualization of meta-platforms for data marketplaces, specifically with a use case where a data provider is not associated with any marketplaces and then joins a meta-platform to share their data. In doing so, the provider can reach consumers from many participating marketplaces.

Participants were allowed to ask for clarifications after the brief presentation. These clarifications aimed to check that the interviewees' understanding of meta-platforms aligned with ours, which was the case for all interviewees. We then asked about potential value creation related to a meta-platform for data marketplaces. We also inquired about the potential drawbacks of meta-platforms. Often, the interviewees had, at this point, already discussed some aspects related to data sovereignty.

Moreover, we complemented our data by incorporating insights from eleven semi-structured interviews conducted by van Velzen (2022),[3] aiming to capture perspectives not included in our initial interviews. van Velzen (2022) utilized purposive sampling, specifically judgment sampling, to choose interview participants based on their expertise. This method was suitable given the specialized knowledge required for researching data sovereignty within meta-platforms, a topic that only a few individuals were knowledgeable about. To recruit these experts, van Velzen (2022) reached out through direct email invitations, utilized the PhD candidate's network, engaged with contacts from his internship company, and attended the 2022 Hannover Messe fair.

While the interview protocol largely mirrored our previously mentioned approach, these interviews focused on data sovereignty issues in meta-platforms. For instance, following discussions on the potential and drawbacks of meta-platforms, participants were explicitly asked about data sovereignty concerns. This approach encouraged open, unrestricted perspectives, allowing participants to share insights without bias toward expected outcomes.

[3] The PhD candidate was the daily supervisor on the committee for van Velzen's (2022) master thesis at TU Delft, titled *"Business-to-Business data sharing via data marketplace meta-platforms: Exploring governance mechanisms to enhance data sovereignty."*

The interviewer often asked follow-up questions to get detailed elaboration. Hence, we assumed the new interviewees were selected from the same population using a similar approach and instruments, allowing for integration with data from previous interviews. Table 5.1 provides an updated overview of the interviewees (I-1 to I-31), with the new participant IDs (I-21 to I-31) highlighted in bold.

Table 5.1. The updated overview of the interviewees

ID	Role	Core relevant experience	Overall work experience (in years)
I-01	Director of innovation	Involved in multiple data sharing projects (e.g., meta-platforms, data marketplaces) and relevant underlying technologies (e.g., privacy-preserving technologies).	28
I-02	Security solution manager	Working on data loss prevention technologies for data sharing.	18
I-03	Product owner	Leading the commercialization of a data sharing platform.	14
I-04	Head of standard business reporting	Leading the implementation of data sharing technologies.	23
I-05	Project manager	Leading multiple projects on the topic of interoperable digital platforms.	10
I-06	Commercial director	Building digital platforms for clients focusing on digital goods.	24
I-07	Chief data officer	Responsible for shaping data policies, including business data sharing with external parties.	12
I-08	Technical innovation manager	Managing a technical lab to explore the newest data sharing technology, such as quantum computing or multi-party computation.	28
I-09	Data protection specialist	Analyzing legal aspects of data sharing.	3
I-10	Head of architecture, innovation, and technology	Exploring the newest technological advancement for data sharing (e.g., blockchain).	16
I-11	Senior strategy manager	Managing the business-to-business stream of a large company, which includes data sharing activities.	32
I-12	Product owner	Leading the commercialization of data analytic platforms.	11
I-13	Risk manager	Conducting risk assessments for data sharing.	5
I-14	Senior consultant	Providing consultancy services in interoperability-related aspects, such as ensuring data portability in digital platforms.	22
I-15	Associate director	Providing consultancy services on information technology outsourcing where business data sharing plays a pivotal role.	24
I-16	Technical researcher	Researching technical aspects of business data sharing, for example, semantic web technologies, metadata management, or vocabulary management.	9
I-17	Deputy studio director	Leading an initiative to explore the interoperability of data marketplaces.	13
I-18	Data science director	Managing a portfolio of data science projects, including business data sharing.	12
I-19	Project manager	Involved in multiple data sharing projects (e.g., meta-platforms, data marketplaces).	19
I-20	Project manager	Developing use cases for business data sharing.	9
I-21	Consultant	Data sharing and digital identity consultant.	6

ID	Role	Core relevant experience	Overall work experience (in years)
I-22	Project manager	Date e-commerce project manager, experienced professional in the telecommunications and financial industry.	20
I-23	Information technology architect	IT Architect/software developer, data sharing expert.	5
I-24	Project manager	Experienced IT and project professional.	6
I-25	Consultant	Experienced professional in financial services and management consulting.	25
I-26	Senior researcher	Senior researcher specializing in trusted data sharing and business ecosystem architecture.	13
I-27	Director	Director of a pan-European trust and data sovereignty Framework.	15
I-28	Consultant	Board member of a regional collaborative organization specialized in future affairs, including digital and data-related topics.	15
I-29	Data management expert	Data management expert at a global professional services firm.	5
I-30	Researcher	Data expert and research engineer.	5
I-31	Developer	Developer and semantic web expert, data sharing initiatives expert.	6

5.1.2 Data analysis

The coding process employed *a structured categorization matrix* (Assarroudi et al., 2018; Elo & Kyngäs, 2008), incorporating predefined categories based on a theoretical understanding of the substantive aspect of Social Contract Theory (SCT). This matrix comprises four levels: higher-level facets, facets, second-order codes, and first-order codes. The codebook of the structured categorization matrix can be found in Appendix 2. We analyzed each transcript using Atlas.TI 22.4. We chose this software for its superior data visualization capabilities and efficient quotation system, allowing richer data interaction and more intuitive coding than alternatives like NVivo and MAXQDA.[4]

We conducted three coding rounds. In the first round, we inductively coded a relevant block of statements into first-order code by interpreting what the participants said when discussing data sovereignty. In the second coding round, we revised or merged the first-order codes into second-order codes. These second-order codes represented broader, abstract code groupings that emerged from the data. In the third round, we further grouped the second-order code into relevant data sovereignty facets. Furthermore, we interpreted how these facets correlate with the higher-level facets of SCT: the Three Ps (Protection, Provision, and Participation). A senior colleague with expertise in qualitative research examined our coding processes for internal validity.

To illustrate the coding process of analyzing data sovereignty facets, consider the relation between excerpts and the applied coding schema in Table 5.2. During the first coding round, the first excerpt was labeled as *data flow tracking*, the second as *data origin information*, the third as *data access revocation*, and the fourth as *dataset retraction.* In the second coding

[4] https://atlasti.com/research-hub/atlas-ti-alternative-to-other-programs, accessed on 15 February 2024.

round, *data flow tracking* and *data origin information* were categorized into the second-order code of *data provenance*. This was done as they fundamentally discussed the origins and pathways of data, emphasizing the importance of knowing where the data comes from and how it moves. This idea represents data provenance. The first-order codes of *data access revocation* and *dataset retraction* were classified under the second-order code of *data removal* because both emphasize the deliberate actions taken to limit or end access to specific data. The third coding round further categorized the second-order code of *data provenance* and *data removal* into the sovereignty facet of *data control.* This facet represents an overarching theme to ensure data remains under the intended authority and purpose throughout its lifecycle.

Afterward, we mapped *data control* as part of the Provision's higher-level facet. The theoretical underpinning for this mapping is the expectation that data providers desire data control capabilities as a part of their vertical arrangement with meta-platform operators. In return, operators are expected to be responsible for provisioning such control mechanisms. Data control was not categorized under Protection since Protection primarily focuses on recognizing rights, a concept distinct from active provisioning. Likewise, data control was not associated with Participation as its primary objective is not directly fostering engagement from data providers. Instead, it primarily aims to offer capabilities for exerting control over data sharing.

Table 5.2. An illustration of the coding schema

No	Excerpt	Applied coding schema
1	"So, to me, data sovereignty is being in control of your data as much as it is over your meta-data. And that you just have non-repudiation, traceability, that sort of thing. So, what I am actually saying with that is traceability. In order to be able to control it [(meta)-data] at all, you first have to know where it is. You have to have insight into that to be able to enforce anything at all."	▪ First-order: Data flow tracking ▪ Second-order: Data provenance ▪ Data sovereignty facet: Data control ▪ Higher-level facet: Provision
2	"There is a lot of discussion around tagging data contents [to enhance data sovereignty] so you know who the ultimate owner is. And I think that is the answer. So, at the end of the day, you can review where the content comes from. You can say this comes from Data Provider A."	▪ First-order: Data origin information ▪ Second-order: Data provenance ▪ Data sovereignty facet: Data control ▪ Higher-level facet: Provision
3	"I think that [providing technical enforcements for data control] is the main part where the industry has been struggling in the ideal world: You can share data, You have some control over what is done with the data, You can revoke the rights to use the data at any time."	▪ First-order: Data access revocation ▪ Second-order: Data removal ▪ Data sovereignty facet: Data control ▪ Higher-level facet: Provision
4	"Data sovereignty is basically the ability of the data provider, for instance, to withdraw the datasets from a particular marketplace at the time of their choosing. That is one example of exercising data sovereignty. My dataset is being traded somewhere. If I no longer want to do it, I can remove the dataset."	▪ First-order: Dataset retraction ▪ Second-order: Data removal ▪ Data sovereignty facet: Data control ▪ Higher-level facet: Provision

5.2 Findings from the conceptual framing (Step 1): Social contract theory contextualization to data sovereignty

Step 1 contextualizes Social Contract Theory (SCT) to data sovereignty. To contextualize SCT, we must define the spatial, temporal, and substantive aspects that shape social contracts (e.g., Furness & Trautner, 2020; Loewe et al., 2021) (refer to Table 5.3).

As discussed in Chapter 3, the spatial aspect of SCT specifies *who* participates and *where* their influence applies in social contracts. The temporal aspect, concerning the *when*, explores the dynamic of social contracts over time. The substantive aspect of SCT describes vertical arrangements between a nation and societal groups (e.g., labor unions). These are the Three Ps: Protection, Provision, and Participation. The Three Ps explain the *what* of social contracts. Protection focuses on recognizing and acknowledging inherent rights that need safeguards (Ellis, 2006; Hickey, 2011). Provision encompasses the various services and resources a country provides to society, including healthcare, education, and infrastructure (e.g., Sobhy, 2021). Participation involves citizens actively engaging in public affairs and interacting with government processes (Furness & Trautner, 2020; Loewe et al., 2021).

Table 5.3. The mapping between social contract theory and data sovereignty in this study

	Social contract theory	**Data sovereignty**
Spatial aspect	Actors (who)	(Meta-platform and data marketplace) operators, data providers, and data consumers
	Territorial settlement (where)	Meta-platform ecosystems, including data marketplaces they federate
Temporal aspect	Duration and timing (when)	Focusing on post-2018 as this time shows significant regulatory changes in the data economy
Substantive aspect	Vertical arrangements (Three Ps: Protection, Provision, Participation)	*Underexplored*

In *the spatial aspect*, the main actors participating in business data include sovereign entities, such as (meta-platform and data marketplace) operators, and societal groups, such as data providers and data consumers (cf. Azcoitia & Laoutaris, 2022). The social contract of data sovereignty is applicable within the scope of the meta-platform, covering the data marketplaces they federate.

Considering *the temporal aspect*, we direct attention to the period post-2018. Within the European Union, which is the sociopolitical area for our study, this time signifies a crucial regulatory evolution in the data economy. Notable legislation arose, such as the Data Governance Act, setting a vision for a Single European Data Market. Concurrently, these rules emphasized the importance of data sovereignty. This period is, thus, appropriate for studying the effects of regulatory influences on social contracts within the meta-platform territory.

The *substantive aspect* of SCT is represented by vertical arrangements, the Three Ps (Protection, Provision, and Participation). However, the existing understanding of the Three PS, initially explored within the context of the relationship between citizens and countries, cannot be directly transferred to the context of data sovereignty in business data sharing. This is due to the fundamentally different characteristics of these contexts. In the former case, the relationship revolves around well-established societal structures and tangible resources; in the latter case, data sovereignty resides within the more abstract and fluid scope of data sharing. Hence, it is unclear how the Three Ps manifest in data sovereignty.

To explore the Three Ps, we utilize notions that correlate with data sovereignty provided by Hummel et al. (2021) (discussed in Chapter 3). As a starting point, we focus on the most potentially suitable data sharing notions: *control, ownership, security,* and *responsibility* (Hummel et al., 2021). In addition, we investigate *compliance* as a facet, given its recent legal prominence in contexts such as the European Data Governance Act (Duisberg, 2022). Here, control refers to the capability to influence and direct information flows. Ownership refers to data property rights, indicating the privileges over data resources. Security, on the other hand, focuses on preventing potential threats and risk mitigation concerning data. Additionally, responsibility delineates roles and expectations, while compliance represents the adherence to relevant legal and regulatory frameworks.

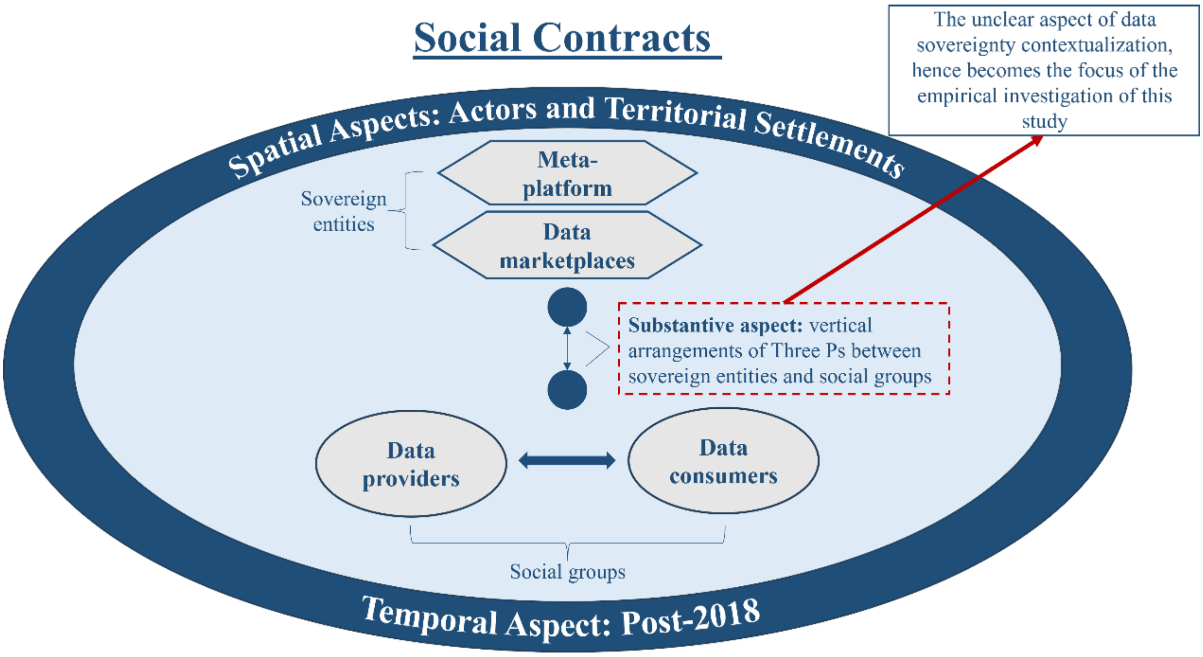

Social Contracts
The unclear aspect of data sovereignty contextualization, hence becomes the focus of the empirical investigation of this study
Spatial Aspects: Actors and Territorial Settlements
Sovereign entities
Meta-platform
Data marketplaces
Substantive aspect: vertical arrangements of Three Ps between sovereign entities and social groups
Data providers
Data consumers
Social groups
Temporal Aspect: Post-2018

Figure 5.1. Contextualizing the social contract theory to data sovereignty (adapted from Furness & Trautner, 2020)

In summary, Figure 5.1 illustrates how this study contextualizes SCT to data sovereignty, highlighting the Three Ps as the primary focus of the empirical investigation. This figure is adapted from Furness and Trautner (2020), who apply SCT to the relationship between societal groups and countries. We tailor this figure by specifying SCT aspects to the data sovereignty context, as shown in Table 5.3. This figure is used as a frame of reference in our subsequent analysis.

5.3 Findings from the semi-structured interviews (Step 2)[5]

Section 5.3 presents the research findings from the semi-structured interviews. Section 5.3.1 delves into the substantive aspect of data sovereignty, highlighting the Three Ps: Protection, Provision, and Participation. Facets and their interrelationships are emphasized using *italics* and underscores, respectively. Section 5.3.2 examines the spatial aspect, exploring how contextual conditions impact the difficulty in realizing data sovereignty facets. Participants are referenced using the identifier (I-X) from Table 4.1.

5.3.1 The substantive aspect of data sovereignty: Protection, Provision, and Participation

5.3.1.1 Protection of data ownership

Data ownership is a critical facet of data sovereignty, which can be interpreted as part of Protection. One interviewee (I-21) stated that data ownership is correlated with data sovereignty: "I think data sovereignty means control over data ownership." Data ownership is associated with possession (I-28), meaning data providers can retain intellectual property rights for their data products (I-01). One participant stated, "… data ownership should always remain with the provider, and that should be clear through whatever kind of licensing they do" (I-25). However, claiming ownership is not straightforward, with some participants questioning whether data ownership can be as transferrable as physical products (I-06, I-10). With this complexity, defining terms of uses becomes pivotal (I-01), as it defines how data products are used, specifies monetary incentives (I-05), and decides data storage locations (I-22). One participant (I-24) illustrated this in detail: "[Data ownership means] I can define my policies and be sure that no one accesses my data without my consent, I can define how long the access is granted, I can define who is getting access. I have a data contract to define how to use this data for which purposes."

Empirical evidence shows that participants emphasize the importance of data possession and term of use definition, demonstrating *safeguarding* needs. Thus, we classify the data ownership facet within the broader Protection facet. This interpretation aligns with the perspective of Interviewee (I-01), who emphasized the connection between ownership and protection, explicitly stating the need to "…have strong protection mechanisms for the ownership of the data." With this interpretation, Protection encapsulates the baseline rights inherently held by data providers (i.e., data ownership), which are recognized as societal norms. These rights are pre-existing conditions *before* data sharing transactions occur, setting a baseline for subsequent data sharing processes. Data ownership does not fall under Provision, as Provision primarily concentrates on service delivery. Similarly, the data ownership facet is distinct from Participation, measures taken to improve the active engagement of data providers.

[5] Several direct quotations in this section are sourced from van Velzen's (2022) master thesis at TU Delft. The PhD candidate was the daily supervisor of this master thesis.

5.3.1.2 Provision of control, security, and compliance mechanisms

The discussion with participants transitioned to the sovereignty facet of Provisioning control, security, and compliance mechanisms. With the foundational rights of ownership in place, data providers require mechanisms for *data control* to protect these rights. This makes data control a crucial facet of data sovereignty. Participant (I-18) illustrated the connection between control and sovereignty: “One can imagine data sovereignty is basically the ability of the data owner, for instance, to withdraw the data set from a particular marketplace at the time of their choosing. That is one example of exercising data sovereignty.”

The ownership facet defines the control facet because control over data is exercised based on the agreed-upon terms of use, which are formalized through contracts signed by consumers (I-18). These contracts are technically enforced to ensure control (I-16). I-24 exemplifies this with the case of technical enforcement using a *connector:*

> *“In the connector world, they [researchers and practitioners] often talk about fully enforced policies. In your data source, you have a connector. You have another connector in your data sink. And you have your offer, you agree on the contract, and then you have all the terms, conditions, and policies. After that, the data gets transferred from the data source to the sink. Technically, we could build this.”*

Having the agreement technically enforced, data control enables data provenance to track data usage history for data monitoring (I-10). In all, data control helps retain ownership of data products.

Besides data control, *security* is also a data sovereignty facet. Security safeguards ownership of providers; as one interviewee (I-26) highlighted, “Looking at data sovereignty, security is also important because you do not want everything to be put out in the open.” According to the interviewees, security means preventing unauthorized parties from accessing the data (I-12), making sure transactions cannot be denied (non-repudiation) (I-05), and ensuring “… availability of data, and then you can use it in a certain application. That is where the added value [of a meta-platform] lies” (I-21). Security entails providing cutting-edge security protections for data sharing (I-05), such as watermarking (I-16), certification (I-19), and smart contracts (I-23), to name a few.

Compliance also emerges as a vital facet of data sovereignty, branching into two areas: external and internal compliance. Firstly, data providers must respect external compliance, encompassing legal and regulatory mandates. For example, (I-27) illustrated compliance in the context of the Data Governance Act:

> *“Let’s say we have a particular data space around this specific service, and these datasets serve an interest. With that interest, everyone agrees it is a good idea to start sharing data as long as they keep control [over data] in line with the Data Governance Act.”*

Given legal intricacies, several participants voiced the need for guidance. I-07 expressed, “It will be great if data stewardship is established. So, when somebody is unsure about this data point, they can immediately contact data stewardships for further explanation.”

Internal compliance involves data providers aligning with the technical aspects enforced by meta-platform operators. I-11 emphasized the technical nature of this compliance, stating, “I believe compliance also has a technical facet, given that your data should be standardized or normalized.” To simplify this compliance process, operators should introduce easy-to-follow mechanisms, such as clear certifications (I-19) or the adoption of a widely recognized reference architecture, like those from the International Data Sharing Association (I-24) or Gaia-X (I-23).

Like control and security, compliance mechanisms serve as tools to safeguard the ownership of data products. I-09 stressed the significance of compliance mechanisms:

> *“We have technical and organizational protection. In my words, you must have some technical and legal skills ... People in security will be looking for some security aspects from a technical point of view. From a contractual point and a legal point, we will try to find some stipulations that do not align with the GDPR or the national law. For example, you can have a contract between two data controllers. One of the obligations is to inform your data subjects about data processing. I can put in a contract that another data controller is obliged to inform my clients about my data processing. This is possible in contracts. So, you can protect your clients.”*

In summary, we infer that Provision in data sovereignty encapsulates data control, security, and compliance mechanisms. Data control via technical enforcement provides mechanisms for ongoing monitoring post-transaction to check whether data is shared according to terms and conditions. Security mechanisms, such as encryption and watermarking, aim to safeguard against unauthorized access, even after sharing data. Compliance extends beyond legal frameworks, necessitating consistent alignment with meta-platform technical specifications. The findings indicate two types of Provisions: *control-based*, which facilitates horizontal interactions among societal actors like data providers and consumers, ensuring adherence with established terms for data sharing, and *defense-based*, which involves security and compliance, countering breaches from malicious actors (e.g., cybercriminals, unauthorized third-party organizations) and ensuring territorial regulations to avoid negative consequences, respectively. In all, Provision highlights intentional actions by meta-platforms to safeguard ownership *during* and *post-data transactions*. Hence, Provision differs from Protection, primarily concerned with recognizing and establishing data providers’ rights rather than actively implementing technical and compliance measures that characterize Provision. Furthermore, they are distinct from Participation, which aims for the active engagement and involvement of data providers in meta-platforms.

5.3.1.3 Participation through clear responsibility division

The connection between data sovereignty, participation, and *responsibility* was frequently discussed in the interviews. Participation represents the opportunities available to diverse societal groups, especially data providers, to articulate concerns, contribute feedback, steer decisions, and participate in meaningful interactions. From the perspective of data providers, Participation extends beyond mere outcomes like willingness to share data. For example, participatory engagements mean that providers (and other actors) use meta-platforms in standardized, mutually agreed upon, and approved ways (I-29). Another example is active oversight of other societal groups (I-27).

Yet, in the interviews, concerns emerged about meta-platforms potentially turning monopolistic and non-democratic. I-29 articulated, "[…] what makes me doubtful is such a meta-platform will always be coupled to commercial aspects and capitalistic systems which are inherently non-democratic." Echoing this, concerns about dominant platforms emerged, with the dilemma of high participation costs on platforms like hotel booking services highlighted by (I-26): "[...] participating comes at a steep cost, sometimes as much as around 20% in charges." Further, concerns about platforms potentially exploiting participants were evident, as (I-21) pointed out: "I can well imagine that a [meta-]platform will be created that organizes it very well from a technological perspective, but then starts to exploit participants."

To ensure constructive and meaningful Participation, delineating responsibility among sovereign entities and societal groups is crucial. I-23 asked, "[…] who is going to write the software, and who is just going to install it?" This view resonates with I-28's statement:

> *"Who should provide the infrastructure [for sovereignty]? It could be a meta-platform, but it could also be a marketplace. But the governance, from my perspective, has to be some cooperative model—an association or a foundation or any other form. If you want to maintain trust, because that is ultimately what this is about, because you will only participate in it if you know that this is reliable, then it must also be reflected in the way in which you organize it together."*

Nevertheless, responsibility division is not straightforward, especially in the context of meta-platforms where the governance structure between a meta-platform and data marketplace participants remains unclear. One interviewee (I-12) said:

> *"So, for example, if a meta-platform and a data marketplace gets data products from you and then sells it to data consumers, and then that data marketplace has security issues or goes down, or the data is corrupted, and then the question is, who is responsible for that? Is it the data marketplace itself? Is it the meta-platform?"*

To conclude, our findings highlight the criticality of defining clear responsibilities between meta-platform and data marketplace operators. This clarity is essential to foster active Participation among all data sharing actors. Such well-defined responsibilities are pivotal for facilitating the Provision of data sovereignty measures, which are crucial for safeguarding the fundamental rights of data providers and subjects. Thus, the responsibility facet of data sovereignty belongs to Participation rather than Provision, which concentrates on delivering mechanisms supporting data sharing rights, or Protection, which focuses on recognizing these rights.

5.3.1.4 *Data sovereignty conceptual framework: Interactions between data sovereignty facets*

This section summarizes the previous findings about data sovereignty facets and their interactions. Figure 5.2 shows the relationships between higher-level facets (i.e., Participation, Provision, and Protection). Participation *steers* how meta-platform and data marketplace operators divide responsibilities for developing Provision mechanisms, which are either control or defense-based. Control-based provision facilitates horizontal interactions among actors such as data providers and consumers to ensure sovereignty. Meanwhile, defense-based provision consists of security and compliance mechanisms, safeguarding against breaches (e.g., by cybercriminals) and ensuring adherence to territorial regulations, respectively. Meta-platforms develop these mechanisms to support the foundational rights that need Protection: data ownership of providers. Every data sharing should start with providers describing data ownership, thus *defining* the data control facet. Control over data is exercised based on terms of use formalized through contracts, aiding ownership *retention*.

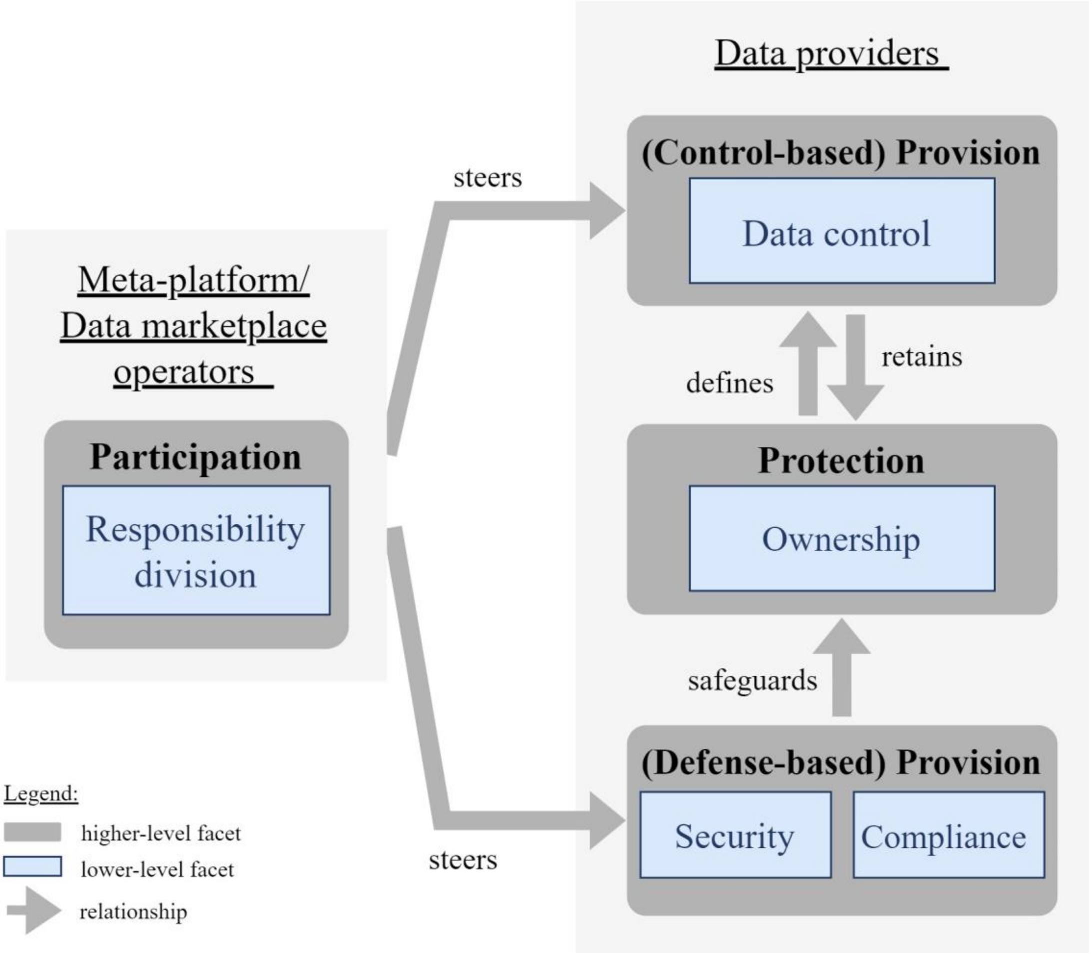


Figure 5.2. A conceptual framework of data sovereignty

The relationship between (higher-level) facets and specific actors becomes evident within the conceptual framework. For instance, the *responsibility division* facet belongs to the operator perspective. Meanwhile, the other facets belong to data providers. Figure 5.2 also shows that each facet interrelates with multiple other facets rather than simply exhibiting one-on-one interrelationships like mutual interdependence. At the same time, it is also not the case that all facets are connected to everything else. Instead, the facets interrelate in various ways, with each facet redefining and enabling subsets of the other facets.

5.3.2 The spatial aspect of data sovereignty: Contextual conditions

The spatial aspect of SCT identifies conditions that shape the substantive aspect, the Three Ps: Protection, Provision, and Participation. In this study, the spatial aspects of SCT can be interpreted as contextual conditions, as they influence the difficulty of realizing data sovereignty facets. To explore this further, the following sections examine three contextual conditions: data type, data sharing setting, and organizational size.

5.3.2.1 Data type

Diversities of *data type formats* complicate *control*. Some data consumers prefer single dataset purchases (I-03), while others seek continuous streams (I-05) with potential time constraints (I-03). Data products, especially when transformed into machine learning models (I-18), make control even more challenging. Given these varying needs for different data formats, providing suitable control mechanisms to safeguard all data formats presents a formidable challenge.

Data origin, particularly the *industry* it originated from, plays a pivotal role in the complexities of *compliance* and *ownership*. Unique characteristics across industrial sectors necessitate tailored regulations. This necessitates (meta-)platform operators to guide data providers in adapting ownership definitions according to pertinent policies (I-31). Furthermore, regulatory and law requirements exhibit considerable discrepancies across various industries. For example, I-07 argued about "… over-regulation of the banking industry. So, there are a lot of regulations on the table" compared to the telecommunication industry. I-10 from a finance industry mentioned, "If you just looked through our IT portfolio … there you see the part of legal is increasing every year. Now, we have European regulation; we have European bank law; we have our national regulators." This highlights the expansion of regulations in certain sectors, spotlighting the role of industry-specific data in shaping compliance and data ownership paradigms.

Certain characteristics of *industry-specific* data influence the complexities associated with data *ownership* and *control*. Consider the data sharing practices prevalent in the capital markets industry as an illustrative example. This sector's maturity in data practices and regulations has led to a sophisticated understanding and effective management of data sharing. I-25 stated, "The capital markets as a data provider area are fairly mature ... And what is also interesting is that the financial and capital markets industry is highly regulated. So, they are mature in compliance practices." Therefore, the nature of industry-specific data influences industry practices, regulations, and awareness around data sharing. This, in turn, fosters an increased level of data literacy, thereby supporting data providers in defining ownership and meta-platforms in provisioning control measures.

5.3.2.2 Business data sharing setting

Data sovereignty complexities intensify in the *meta-platform setting*, mainly due to ambiguous governance between meta-platforms and data marketplaces. Section 5.3.1.3 highlights the challenge of pinpointing *responsibility* in meta-platforms, especially during security breaches or system failures. Furthermore, meta-platform operators are responsible for selecting trustworthy data marketplace participants, which adds another layer of complexity given the diverse operation rules and security standards across platforms. Data providers are suspicious if specific marketplaces are disreputable intermediaries (I-04). One interviewee (I-01) said: "If a channel [a data marketplace], for instance, is ruled by mafias, you will try to avoid it." Evaluating such marketplaces is problematic because each has unique operation rules (I-01). For example, while some marketplaces have decent security, others do not (I-12). These challenges highlight the importance of defining clear responsibilities to enforce data sovereignty measures effectively.

The meta-platform context also increases *control* complexity. While achieving complete control is feasible, technical hindrances persist (I-02, I-03). For example, exchanging data via a meta-platform raises concerns related to data provenance. Meta-platforms allow providers to share their business data with multiple data marketplaces. Hence, data lineage from providers to consumers becomes more complex. An interviewee (I-12) asked: "Who is responsible for providing the lineage from supplier to buyer if you have two stops, which are two separate entities? ... We have two parts in the chain." Therefore, there is a possibility of having blind spots in the data lineage, making data tracing difficult (I-7). In addition, data providers may need to withdraw data for specific reasons. Nevertheless, retrieving shared data is difficult: data providers must identify which data marketplace shares their data (and to which data consumers) (I-09).

The meta-platform setting raises difficulties in providing *compliance mechanisms*. A meta-platform commonly aims to be interoperable across data marketplaces in different countries or industries. Nevertheless, different work rules depend on specific areas (I-01), and translating diverse legal instruments between countries is difficult (I-02, I-08). For example, in extreme cases where a meta-platform is interoperable with data marketplaces outside the European Union, some regulations like GDPR may not be applicable (I-01). Hence, meta-platforms may not help data providers understand what they can (and cannot) do with the data (I-13).

5.3.2.3 Organizational size

Organizational size is pivotal in data providers' capacity to define *ownership*. Larger entities are often more prepared to share data. As I-26 put it, "But I do not think Small-Medium Enterprises (SMEs) will share raw data on such a marketplace." Typically, bigger organizations have enhanced capabilities for ownership definition (I-21). In contrast, smaller providers face challenges due to inadequate data skills and awareness. I-10 voiced a concern, asking: "What happens to the ownership of the data?" For SMEs lacking data skills, a solution is to outsource processes and draw insights from external parties. I-21 suggested, "Larger organizations have those [data sharing] capabilities. The smaller ones can rely on external parties, for instance, for data storage."

Organizational size is essential when addressing *non-compliance data sharing cases*, especially regarding legal consequences. Given their substantial market presence, larger organizations often experience the implications more intensely. I-13 noted, “It is the bigger player in the market that is always going to bear the brunt of it.” I-20, who shared a personal experience of a security breach at a small enterprise, further agreed with this view. Although this incident occurred in a small-scale context, it caused considerable distress: “We were careless, and it happened. So, these security breaches were very painful for us even though we are a small business. For a big business, I think it is even more painful.”

Nevertheless, large organizations that handle extensive datasets are often more ready to conduct data sharing due to their rigorous liability measures. They are more vigilant about potential infringements, thereby minimizing risks. I-27 illustrated this point, noting, “Because with that, you also have the liability taken seriously. The chances of violation are smaller than with many small players.” Hence, collaborating with larger companies often signifies a more secure data sharing than partnering with multiple smaller firms with potentially inadequate data practices. Table 5.4 summarizes how contextual conditions influence the complexity of realizing data sovereignty facets.

Table 5.4. Contextual conditions affecting data sovereignty facets

Contextual conditions	Influence on data sovereignty facets
Data type (format variations)	• Data format variations raise technical challenges for provisioning *control* mechanisms.
Data type (industry-specific data)	• The diversity in industry-specific laws and regulations mandates (meta-) platform operators to provision *compliance* mechanisms for data providers in tailoring data *ownership* definitions following applicable policies. • In some industrial types, such as capital markets, data providers and consumers generally know about business data sharing practices, increasing the overall data skills and awareness to define *ownership* and exercise *control*.
Business data sharing setting	• An unclear governance structure between meta-platform and data marketplace operators amplifies complexity in realizing clear *responsibility division*. • Meta-platform architecture raises technical challenges in realizing *control* mechanisms. • The meta-platform setting raises difficulties in adhering to *compliance*, primarily due to aiming for cross-industry and cross-border data sharing.
Organizational size	• SMEs lack data skills and awareness to define *data ownership*. • Larger enterprises are more liable to the *consequences of non-compliance*.

5.3.2.4 Implications of contextual conditions for this study

Contextual conditions serve as boundary conditions, specifying the contexts or limitations where a (design) theory holds true (Foss & Saebi, 2017). Hence, we need to select the conditions that make data sovereignty contextually significant and challenging to achieve; otherwise, data sovereignty may be incorrectly deemed unimportant. Therefore, the findings confirm our decision to focus on meta-platforms as a business data sharing setting (as outlined in Chapter 1), mainly due to the issues related to a) responsibility division with data marketplace operators and b) difficulty in realizing control and compliance mechanisms.

Other contextual conditions, such as data types (including format variations and industry-specific data) and organizational size, are not the focus of our study and thus are controlled. For data types, we concentrate on basic data products like datasets (refer to Chapter 3). We primarily examine the telecommunications and banking sectors for industry scope, presuming they possess the necessary expertise to assert control and define ownership. We limit our geographical focus to the EU, focusing on European regulations. Regarding organizational size, we target larger enterprises, assuming they have the requisite skills and knowledge. These organizations are also more likely to face sovereignty consequences, underscoring the importance of data sovereignty.

5.4 Conclusion of Chapter 5

This chapter answered the second research question: *What are the key facets of data sovereignty in business data sharing through meta-platforms for data marketplaces?* Building on SCT, we identified three higher-level facets of data sovereignty. First, the protection higher-level facet encompasses the baseline rights inherently held by data providers for data ownership. These rights stand as a pre-existing condition before any data sharing transactions occur. Second, the provision higher-level facet encapsulates data control, security, and compliance mechanisms. These mechanisms are provided by meta-platforms to safeguard ownership during and post-data sharing transactions. Third, the participation higher-level facet requires clear responsibility division between sovereign entities (e.g., meta-platforms and participating data marketplaces) to ensure active engagements of societal groups (e.g., data providers). Our conceptual framework (see Figure 5.2) shows the interrelation between higher-level facets of sovereignty. The higher-level facet of participation determines how (and by whom) the provision mechanisms are provided, which, in turn, ensures baseline rights protections. We will develop a data sovereignty measurement model using the lower-level facets. This model serves as indicators to assess the perceived effectiveness of control mechanisms (Chapter 8) and the impact of data sovereignty on the broader data economy (Chapter 9).

We found three contextual conditions determining the difficulty in realizing sovereignty facets: data type, business data sharing setting, and organizational size. Different data types, like structured and live-streamed data, present technical challenges for control mechanisms, while industry-specific data intensifies compliance complexity. The meta-platform setting raises ambiguity in determining the responsibility between such a meta-platform and data marketplace operators. Moreover, aligning multiple architectures of data marketplaces raises technical challenges in provisioning control mechanisms. Furthermore, meta-platform settings aiming for cross-border data sharing complicate compliance mechanisms. Finally, small to medium-sized enterprises struggle to define ownership and maintain control, often due to resource and expertise constraints. We will control these factors to ensure our examination of data sovereignty is contextually relevant. This involves focusing on fundamental data products in the telecommunications and banking industries, using meta-platforms as the business data sharing setting, and targeting large enterprises.

The next chapter will identify and select control mechanisms to enhance data sovereignty by considering data sovereignty facets. We will conduct a narrative review to investigate the state-of-the-art of control mechanisms to enhance data sovereignty in the Information Systems literature.

PART 3: THE SOLUTION SPACE

Chapter 6: A Portfolio of Control Mechanisms

The previous chapter identified five data sovereignty facets: data ownership, data control, compliance, security, and responsibility. Data ownership refers to the rights and privileges over data products. Data control is the ability to manage the flow of these data products. Compliance is defined as mechanisms to follow legal and regulatory standards for sharing data products. Security emphasizes provision against threats and managing risks associated with business data sharing, and responsibility defines roles and expectations for meta-platform and data marketplace operators. These facets serve as goodness criteria that guide control mechanism design and evaluation.

This chapter explores the design options of control mechanisms for enhancing data sovereignty. In doing so, we answer the third research question: *"What control mechanisms can enhance data sovereignty in business data exchange via a meta-platform for data marketplaces?"* This question arises because a clear overview of such control mechanisms is lacking. As a result, we have limited perspective knowledge on selecting and designing these mechanisms (scientific gap 3).

This chapter consists of four sections. Section 6.1 discusses the research approach, specifically the narrative review approach. Section 6.2 reviews control mechanisms identified in the literature to enhance data sovereignty. This section defines these control mechanisms and discusses their applicability in the data sharing processes. We also categorize these mechanisms into appropriate control modes, explore how they can enhance data sovereignty, and discuss their limitations. Section 6.3 selects the control mechanisms that are the most relevant in the context of this study by considering the control theory perspective. Finally, Section 6.4 concludes this chapter.

6.1 Research approach: Narrative review

This chapter employs the literature review approach to investigate the state-of-the-art of control mechanisms to enhance data sovereignty in the Information Systems (IS) literature. In doing so, we can identify which mechanisms are beneficial in enhancing specific facets of data sovereignty. Specifically, this chapter employs the narrative review approach. The narrative review summarizes the prior knowledge within a field without necessarily following strict protocols like the Systematic Literature Review (SLR) does (Paré et al., 2015). Our motivation to use a narrative review over an SLR is three-fold.

Firstly, the limited research directly linking data sovereignty and control mechanisms as part of control theory creates a challenge in defining the search string for an SLR. Initial attempts using a search string that combined "data sovereignty" and control-related keywords ("control theory," "control mechanism," "control mode") yielded no relevant articles. Consequently, we decided to change our approach by identifying key literature on data sovereignty and conducting snowballing from this starting point.

Secondly, we had to consider resource allocation, specifically time and effort. To identify key literature, we leveraged the bibliographies of recently published SLR studies that focus on delineating the concept of data sovereignty (see Hellmeier & von Scherenberg, 2023).

By using the selected literature from Hellmeier and von Scherenberg (2023), we optimized our resources by focusing on the analysis rather than recollecting relevant literature.

Thirdly, the flexibility of narrative reviews influenced our decision. Unlike SLR, which requires adherence to a pre-set protocol, narrative reviews allow the inclusion of new sources during the review process. This adaptable approach allowed us to refine our literature list as the review progressed, thereby ensuring the consideration of the most recent and relevant studies (Paré et al., 2015).

While narrative reviews are sometimes criticized for their potential subjectivity and lack of methodological transparency, we aimed to minimize these issues by following Levy and Ellis (2006) framework. This framework includes three steps: (1) collecting relevant literature, (2) analyzing the literature, and (3) writing a review. The subsequent sections discuss each of the steps.

6.1.1 Step 1: Collecting relevant literature

The first phase of a narrative review involves gathering key literature through a literature screening strategy (Levy & Ellis, 2006). Figure 6.1 illustrates this screening strategy.

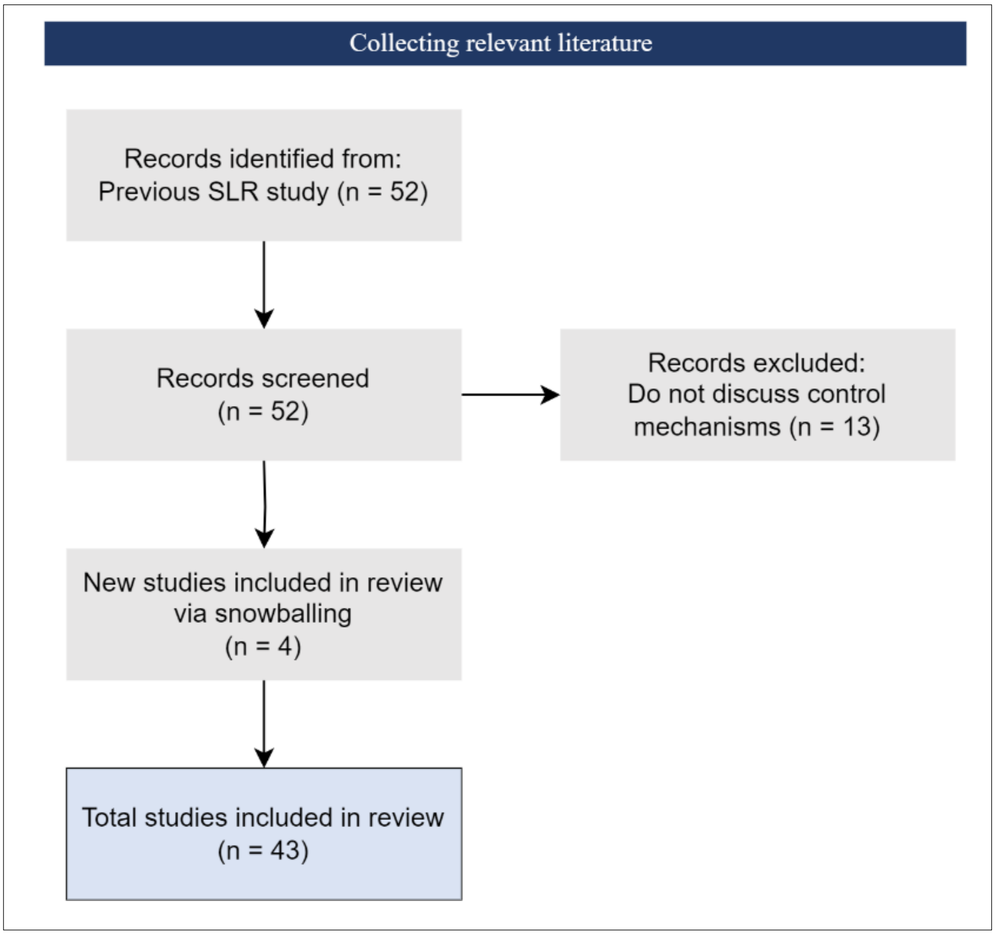

Collecting relevant literature
Records identified from: Previous SLR study (n = 52)
Records screened (n = 52)
Records excluded: Do not discuss control mechanisms (n = 13)
New studies included in review via snowballing (n = 4)
Total studies included in review (n = 43)

Figure 6.1. The PRISMA diagram for collecting relevant literature (adapted from Haddaway et al., 2022)

We collected 52 relevant articles on data sovereignty in the Information Systems field, drawing from the bibliographies of Hellmeier and von Scherenberg (2023). We reviewed the title, abstract, introduction, and conclusion of each article to assess its relevance. Subsequently, we excluded 13 articles that did not specifically address control mechanisms for enhancing data sovereignty. For instance, Rainie et al. (2019) discuss indigenous communities and their prerogative to retain their cultural legacy, traditional wisdom, and intellectual assets, while Taylor (2020) explores the concept of data localization, i.e., the requirement for data to be stored and processed in its country of origin.

Following the screening process, we retained 38 articles. These include studies on various topics, such as data sovereignty solutions (Lauf et al., 2022), a reference architecture for sovereign data sharing (Scheider, Lauf, Möller, et al., 2023), and usage control (Zrenner et al., 2019).

We employed a snowballing approach to help uncover key literature that might not have been identified in the existing list. This involved backward snowballing (adding articles cited in our sources) and forward snowballing (including articles that cited our sources). This process led to the addition of four articles (Schäfer et al., 2023; Scheider, Lauf, & Geller, 2023; Scheider, Lauf, Möller, et al., 2023; Schmidt et al., 2022). Our sample now consists of 43 key literatures. The complete list is available in Online Appendix 1.[1]

6.1.2 Step 2: Analyzing the literature

The second step for a narrative review is literature analysis. To do so, we read the literature to identify control mechanisms provisioned by controllers (e.g., platform operators) to control controlees (e.g., data consumers), which help data providers enhance their data sovereignty. We defined these mechanisms and demonstrated their application relative to the data sharing processes from the data provider perspective, which consists of preparation (e.g., describing metadata), agreement (e.g., creating a contract), and usage (e.g., monitoring data usage) (see Section 3 for the detailed elaboration of these processes). We then categorized the control mechanisms by control mode, analyzed their contribution to enhancing data sovereignty, and discussed their limitations. Afterward, we elaborated on their contribution to data sovereignty facets and discussed their challenges.

6.1.3 Step 3: Writing a review

The last step is to write the review by crafting a logical chain of argumentations (Levy & Ellis, 2006). Our review was guided by the analysis we performed in Step 2. Informed by control theory, we then selected the most relevant control mechanisms for the context of this study: smart contracts and certifications. This selective approach was crucial to maintaining a balance between the breadth and the depth of our investigation.

6.2 Control mechanisms to enhance data sovereignty

This section presents seven control mechanisms to enhance data sovereignty.

[1] Link: https://doi.org/10.4121/785dfc19-d82b-4e46-a6d4-8a714569557b

6.2.1 Certifications

Definition: Certifications set technical and organizational prerequisites for business data sharing (Menz, Resetko, & Winkel, 2019). Certification coverage varies, extending from overall technical infrastructure (Lauf et al., 2022) to specific components (Cuno et al., 2019; Otto & Burmann, 2021; Ruparelia, 2016; Sarabia-Jácome et al., 2019; Zrenner et al., 2019) such as identity management and third-party modules (Nagel & Lycklama, 2021). Other certification coverages include encryption techniques (Esposito et al., 2019; Plateaux et al., 2013; Ruparelia, 2016), algorithmic logic (Mawere & Van Stam, 2020), and data processing approaches (Lauf et al., 2022). Certifications often incorporate risk assessments as part of certification procedures, and certified entities receive seals as proof of compliance (Ethikrat, 2017).

Applicability in the data sharing processes: Certifications are relevant in the *agreement* phase of data sharing processes. It signals fulfillment with pre-conditions, which can be a decision factor for data sharing actors to select their counterparts for establishing data sharing agreements (Melero & Navarro-Molina, 2020).

Control mode: Certifications ensure conformity with data sharing pre-conditions (Biegel et al., 2020). From the control theory perspective, certification is an *input control* (Adam et al., 2022), functioning as a gatekeeper by verifying that all essential criteria are met at the beginning of the process.

Contribution to enhance data sovereignty: Certifications may contribute to data sovereignty facts of *compliance, security,* and *responsibility*. In terms of compliance, for instance, certifying employees enhances adherence to regulatory requirements, as it involves training and knowledge testing, raising awareness about compliance requirements (Abdullah et al., 2010; Panitz et al., 2011). Hence, this approach may also apply to data sharing actors, helping them become familiar with data sharing regulations.

Certifications also enhance the security facet of sovereignty. For example, obtaining certifications from the International Data Space for data sharing signifies compliance with globally accepted standards, such as ISO/IEC 27001 for information security management (Nagel & Lycklama, 2021). It implies that holding such certifications strengthens businesses' defenses against cyber threats for data sharing. Considering the facet of responsibility, certifications can generally distinguish actors' roles and responsibilities. This is because certifications establish well-defined processes and clarify expectations with each actor (Lansing et al., 2018). Hence, certifications ensure increased responsibility awareness among all actors. In our study context, data sharing certification may enhance the division of responsibilities between meta-platform and data marketplace operators.

Challenges: Certifications have limitations. For instance, earning certifications are costly (Irion, 2012). Moreover, businesses get certifications for promotion purposes without fully integrating the best practices into their organizational routines (Danylak et al., 2022). Furthermore, certification requirements often struggle to stay up to date in rapidly evolving technological environments. This results in varying certification outcomes, both positive and negative (Lansing et al., 2018).

6.2.2 Usage control

Definition: Usage control is a technology that manages access to and use of digital resources (Lazouski et al., 2010; Park & Sandhu, 2004). Usage control plays a crucial role in data sharing by technically enforcing agreements between providers and consumers (Munoz-Arcentales et al., 2019; Nagel & Lycklama, 2021; Schäfer et al., 2023). As a key design principle in designing data sharing platforms (Scheider, Lauf, & Geller, 2023), the primary advantage of usage control is data traceability (Sarabia-Jácome et al., 2019). With this capability, data providers no longer rely merely on trust in platform providers and data consumers (Zrenner et al., 2019).

Usage control improves traditional access control with four key characteristics (Park & Sandhu, 2004): authorizations, obligations, conditions, and ongoing controls. Authorizations permit users to access specific resources. Obligations specify users' responsibilities. Conditions ensure compliance with environmental or system requirements. Ongoing controls involve continuous monitoring of access, including immediate revocation.

Control mode: From the control theory perspective, usage control is a form of *process control*. Usage control ensures digital resource usage obeys the necessary authorizations, obligations, and conditions during the lifecycle. Hence, this approach aligns with process control principles, where controllers steer processes to achieve desired outcomes by constantly monitoring and enforcing adherence to predefined rules.

Applicability in the data sharing processes: Usage control covers all data sharing processes, including *preparation* (e.g., data usage specification), *agreement* (data usage negotiation), and *usage* (e.g., data usage monitoring) (Jung & Dörr, 2022).

Contribution to enhance data sovereignty: Usage control primarily contributes to the sovereignty facet of *ownership* and *control* (Hellmeier & von Scherenberg, 2023; Jarke et al., 2019; Munoz-Arcentales et al., 2019; Schmidt et al., 2022). Regarding ownership, usage control helps maintain rights and privileges over data products. Data providers can specify terms of uses of data products during the preparation and agreement stages. Regarding data control, usage control enables providers to steer the flow of data products according to the agreed-use terms. For instance, it allows for the deletion of data products if issues arise (Lauf et al., 2022; Nast et al., 2020).

Challenges: Usage control in data sharing is promising but challenging, necessitating more research (Munoz-Arcentales et al., 2019; Otto & Burmann, 2021). These challenges include a trade-off between achieving a high degree of sovereignty and the effort required for implementation. Architectures that offer maximum data sovereignty for data providers demand significant implementation effort from data consumers (Zrenner et al., 2019). Furthermore, usability issues arise due to usage control complexities, leading to the exploration of human-centric approaches (Scheider, Lauf, Möller, et al., 2023).

6.2.3 Self-sovereign identity

Definition: Self-Sovereign Identity (SSI) allows individuals or organizations to manage their digital identities independently, free from third-party intervention (Nagel & Lycklama, 2021). SSI uses decentralized identifiers stored in a decentralized registry, verifiable through cryptography (Mühle et al., 2018). To illustrate how Self-Sovereign Identity (SSI) functions, consider the following example from the education sector, where graduates could manage their academic credentials. With SSI, graduates can directly provide verifiable proof of their academic credentials to employers, bypassing the administrative process of obtaining verified transcripts or diplomas (Koukoularis et al., 2023).

Applicability in the data sharing processes: SSI is applicable in the *agreement* phase of data sharing, primarily aiding in identity verification. This means that data-sharing agreements are grounded in verified identities. This ensures businesses can share data with confidence, knowing their counterparts are authenticated and authorized.

Control mode: SSI primarily serves as *process control,* regulating the verification of identity information in blockchain-based systems. SSI involves three key actors: the issuer, the holder, and the verifier (Mühle et al., 2018; Schmidt et al., 2022). Issuers, such as universities, create credentials and record them on a decentralized registry. Holders, such as graduates, store these credentials in their personal systems, such as digital wallets. Verifiers, such as employers, authenticate the holders' identities by accessing only the necessary data and without needing direct contact with the holders. Therefore, SSI principles align with process control, where controllers guide processes toward desired outcomes through continuous monitoring and enforcement of predefined rules.

Contribution to enhance data sovereignty: SSI contributes to retaining data ownership, exercising control over data, and enhancing security. Considering ownership, SSI allows holders to manage their digital identities directly, ensuring that they are the sole custodians of their identity. Moreover, holders can also specify which aspects of their identity are shared and under what circumstances (Naik & Jenkins, 2020). Considering control over data, SSI allows holders to have the power to steer the data flow, for example, by revoking their personal data identity. Considering security, SSI mitigates traditional security risks, such as the vulnerabilities associated with managing multiple passwords across various platforms, which are often targets for malicious entities (Tan et al., 2023).

Challenge: SSI implementation presents several challenges. First, managing multiple key pairs for decentralized identifiers is complex. Second, scalability and reliability issues exist because SSI primarily employs distributed ledger technology. Lastly, building trust for broad SSI adoption requires effort due to legal uncertainty and the immaturity of standards (Tan et al., 2023).

6.2.4 Privacy-enhancing technology

Definition: Privacy-enhancing technology (PET) is "… a class of technical measures which aim at preserving the privacy of individuals or groups of individuals." (Heurix et al., 2015, p. 1). These technologies vary widely, including privacy filters (Bauer et al., 2019), geo-encryption (Esposito et al., 2016; Esposito et al., 2019), database encryption (Plateaux et al., 2013), differential privacy (Gupta et al., 2020), privacy-preserving process mining (Mannhardt et al., 2019), pseudonymization (Lauf et al., 2022), and privacy identifiers (De Mooy, 2017), to name a few. In the context of data sovereignty, Schäfer et al.' (2023) find three PET instances that enhance sovereignty: Homomorphic Encryption (HE), Trusted Execution Environment (TEE), and Multiparty Computation (MPC). We focus on discussing these three PETs.

HE enables computations on encrypted data, ensuring the output matches the results performed on unencrypted data (Gentry, 2009). THE refers to processor components that protect data during use, maintaining confidentiality and integrity by securing communication channels for encryption requirements, like private keys (Sabt et al., 2015). Meanwhile, MPC is a cryptographic method that allows numerous parties to compute functions while keeping their inputs private (Du & Atallah, 2001). Although these three PETs aim to enhance data sovereignty through encrypted data computations, their methods differ: HE processes a single encrypted dataset, TEEs create secure environments for isolated computations, and MPC supports distributed computations without exposing data.

Applicability in the data sharing processes: Generally**,** Homomorphic Encryption (HE), Trusted Execution Environment (TEE), and Multiparty Computation (MPC) are applicable in the *usage* phase of data sharing. Take HE, for instance. It allows computations on encrypted data, shaping how this data is processed without ever needing decryption. Similarly, TEE establishes secure sections within a processor to ensure confidentiality and data integrity during computations, thus directly impacting the process. Finally, MPC maintains privacy by enabling collaborative computation without revealing individual inputs.

Control mode: PET primarily functions as a form of *process* control. As elaborated above, PET influences how data is processed and manipulated during the usage phase of data sharing**.** This aligns with process control principles, where controllers guide processes toward desired outcomes by ensuring adherence to predetermined guidelines and rules.

6.2.5 Smart contracts

Definition: Smart contracts are often viewed as the next generation of usage control due to their immutability capabilities (Chiquito et al., 2022; Siddiqui et al., 2022). Smart contracts are

“…any self-executing program running in the distributed ledger environment, and it is often meant to implement automated transactions agreed by the parties” (Governatori et al., 2018, p. 378). While traditional contracts rely on paper-based legal documents, smart contracts embed legal terms and consensus in computer-based languages. Therefore, smart contracts offer automatic contract execution, enable greater transparency, and provide secure infrastructure for business data sharing (Petersen, 2022). Our sample, for instance, discusses smart contract integration with access control (Chen et al., 2020), explores their alignment with self-sovereign identity (Hong & Kim, 2020), and examines smart contract use cases (Nagel & Lycklama, 2021).

Moyano et al. (2021) highlight smart contract scenarios in data marketplaces. First, data customers provide a draft contract by defining data product needs and stating their tentative willingness to pay. Subsequently, data marketplace operators facilitate the negotiation between providers and consumers. In this negotiation, customers need to pay a deposit. Once both actors agree and sign a contract, operators grant Application Programming Interface (API) access to customers. In doing so, customers can access the agreed data products. The APIs are linked with the agreed smart contract so that consumers can access data products merely based on the agreed data usage terms. If consumers misuse the agreed terms later, their deposit will not be released. They also may deal with dispute resolution.

Applicability in the data sharing processes: Smart contract covers the entire data sharing process, including the *preparation* phase (e.g., defining metadata products), *agreement* formation (e.g., contract creation), and *usage* (e.g., enforcing data usage).

Control mode: Smart contract serves as a form of *process control* by automating and regulating the steps of data sharing processes, covering the reparation, agreement, and usage phases. This aligns with process control principles, where controllers guide processes toward desired outcomes through continuous monitoring and enforcement of predefined rules.

Contribution to enhance data sovereignty: Smart contracts can enhance data sovereignty, specifically in the facets of *data ownership* and *control*. Regarding ownership, smart contracts help retain the rights of data providers by offering a pre-filled template that defines data sharing use cases. These templates cover terms of use, monetary incentives, and the data types to be shared (Moyano et al., 2021). Considering data control, smart contracts provide data provenance to enable transparency of data access and usage. At a more advanced level, smart contracts can automatically monitor data compliance usage (Karger et al., 2021; Tuler De Oliveira et al., 2022). Furthermore, data providers can automatically revoke the license if consumers violate use and access rights (Jagals et al., 2021).

Challenges: Smart contracts are subject to several limitations. Möhring et al. (2018) point out the considerable effort required for their implementation. Challenges such as limitations in the programming language and inefficient debugging tools complicate development. The smart contract development ecosystem also lacks essential resources like best practices, code samples, community bases, external libraries, and standardized frameworks (Zou et al., 2021). Another challenge is the *Write Once, Read Many* characteristics of blockchains. This characteristic prohibits modifications to existing contracts, thereby necessitating the creation of new versions for any updates. (Crosby et al., 2016).

6.2.6 Code of conduct

Definition: A code of conduct outlines a collection of shared norms, values, and principles that influence actions and decision-making within an organization or community (Van Der Burg et al., 2021). In the context of data sharing, prominent examples include the code of conduct from the International Data Space Association (IDSA) and Gaia-X. The IDSA develops the IDSA Rulebook, offering guidelines for implementing common data sharing services that align with legal and regulatory standards. Meanwhile, Gaia-X introduces the Gaia-X Framework, articulating three core pillars guiding the operations of their respective communities: federation, compliance, and data exchange. A code of conduct can target specific data sharing communities. For example, a widely agreed code of conduct in the agricultural sector encourages contractual arrangements as the shared norm for data sharing, ensuring clarity over data originators and ownership rights. Likewise, for genomic and health data sharing, specific conduct codes have been established (Knoppers et al., 2011; Matar et al., 2023).

Applicability in the data sharing processes: Codes of conduct typically present abstract, high-level guidance in a generic form, encompassing various aspects of the data sharing processes. For instance, the IDSA rulebook addresses all stages: it outlines metadata definition in the *preparation* phase, details data contract negotiation in the *agreement* phase, and discusses data usage oversight in the *usage* phase.

Control mode: Codes of conduct are developed to meet community needs, promoting a shared understanding of acceptable behaviors. This approach aligns with *clan* control, which also emphasizes ethical consensus and accommodates diverse interests within the clan, typically through member negotiation (Lian, 2021; Scheider, Lauf, & Geller, 2023).

Contribution to enhance data sovereignty: Establishing a code of conduct is beneficial to enhance data sovereignty (Nagel & Lycklama, 2021; Scheider, Lauf, & Geller, 2023). The impact of a code of conduct on aspects of sovereignty depends on its content. However, a code of conduct may contribute to all sovereignty facets. For instance, the EU's data sharing code of conduct establishes *ownership* rights, ensuring actors (e.g., farmers or agri-chain operators) are entitled to benefits from their data use. The code of conduct also contributes to the *control* facet, mandating that data be collected and used only as specified in the contract and technically enforced where feasible. The code of conduct also covers the *security* facet, specifying enhancements like watermarking, encryption, and secure internet flow. The code also addresses *compliance*, mandating GDPR adherence where relevant and addressing liability and intellectual property rights issues. Finally, codes of conduct contribute to the *responsibility* facet by defining the roles of data sharing actors in agriculture, including input suppliers, farmers, processors, and stakeholders.

Challenges: As a guiding principle, codes of conduct can be abstract and vague, resulting in unclear terms (Van Der Burg et al., 2021). This raises concerns about the practicality of their implementation and enforcement. Furthermore, codes of conduct may overlap or conflict with existing ones. Determining the most suitable entities to develop unbiased codes is also challenging. Finally, the attempt to balance the diverse priorities of various stakeholders to enhance membership and engagement may weaken the foundational values of codes of conduct (Wiseman et al., 2019).

6.2.7 Dynamic consent

Definition: If data providers share personal data, they must secure consent from data subjects—identifiable individuals from whom the data originate. Consent involves an explicit, voluntary agreement from data subjects for their data processing (Nagel & Lycklama, 2021). In a more advanced form, dynamic consent enables data subjects to manage their personal data in real-time, adapting to their evolving preferences (Hummel et al., 2018). For example, dynamic consent enables data subjects to grant or revoke consent, adjust access rights, or delegate data management to third parties (Cuno et al., 2019; Nagel & Lycklama, 2021). Dynamic consent can be embedded in access control architecture (Munoz-Arcentales et al., 2019). Nevertheless, one critical challenge in dynamic consent is the extensive engagement required from the data subjects. To address this, recent efforts focus on automating dynamic consent (e.g., Scheider, Lauf, Möller, et al., 2023).

Applicability in the data sharing processes: Dynamic consent covers the *preparation* and *usage* phase of business data sharing. In the preparation stage, data providers must obtain explicit consent before sharing data products derived from data subjects. During the usage phase, they must accommodate changes in the data subjects' preferences (cf. Kaye et al., 2015). For instance, if a data subject requests deletion, the data provider must comply by updating their terms of use and removing the data from data consumers.

Control mode: Dynamic consent operates as a form of *process* control, regulating the procedures and rules for data providers managing the personal data of data subjects, where applicable. It aligns with process control principles, where controllers direct processes toward desired outcomes by continually monitoring and enforcing predefined rules.

Contribution to enhance data sovereignty: If data sharing involves personal data, dynamic consent mainly contributes to data sovereignty facets of *ownership*, *control,* and *compliance*. In ownership, dynamic consent aids data subjects in retaining their rights by allowing them to specify preferences regarding their data usage. Concerning control, dynamic consent enables data subjects to guide the information flow, especially if their preferences change. As for compliance, it ensures that business data sharing practices align with crucial legislative standards, such as GDPR in the European Union (Lauf et al., 2022). This preventive measure mitigates legal liabilities for data providers and protects against data exploitation incidents, like the Facebook-Cambridge Analytica scandal that misused data for profit (Hu, 2020).

Challenges: Dynamic consent faces several challenges. It must align with changing policies, standards, and practices (Kaye et al., 2015). Dynamic consent also deals with consent fatigue, where users become overwhelmed by much consent content (Schlehahn et al., 2020). Previous research also finds that dynamic consent is problematic due to its dependence on information technology and its potential to worsen the digital divide, resulting in unequal access and exclusion concerns (Mascalzoni et al., 2022).

6.2.8 Summary of control mechanisms

Table 6.1 summarizes the seven control mechanisms identified in the analyzed literature. Four mechanisms (i.e., usage control, smart contract, dynamic consent, and code of conduct) are helpful in the entire data sharing process. In contrast, certification and self-sovereign identity are specific to the agreement phase, while privacy-enhancing technology is relevant only during the usage phase.

Most control mechanisms in our study fall under process control, including usage control, privacy-enhancing technology, smart contract, and dynamic consent. We also identify two mechanisms as input control: certification and self-sovereign identity. Advanced forms of self-sovereign identity can also function as output control. Interestingly, we find no mechanism categorized as self-control.

Table 6.1. Control mechanisms to enhance data sovereignty

	Application in data sharing process			**Control mode**					**Contribution to data sovereignty facet**				
Control mechanisms	**Preparation**	**Agreement**	**Usage**	**Input**	**Process**	**Output**	**Self**	**Clan**	**Ownership**	**Control**	**Security**	**Compliance**	**Responsibility**
Certification		✓		✓							✓	✓	✓
Usage control	✓	✓	✓		✓				✓	✓			
Self-sovereign identity		✓			✓				✓	✓	✓		
Privacy-enhancing technology			✓		✓						✓		
Smart contract	✓	✓	✓		✓				✓	✓			
Dynamic consent	✓	✓	✓		✓				✓	✓		✓	
Code of conduct	✓	✓	✓					✓	✓	✓	✓	✓	✓

Each control mechanism in our study targets specific facets of sovereignty. With its broad scope, the code of conduct can address all facets of sovereignty. Certification primarily covers aspects of security, compliance, and responsibility. Usage control, smart contract, and dynamic consent focus on ownership and control facets. Meanwhile, self-sovereign identity and privacy-enhancing technology focus on the security facet.

6.3 Selecting control mechanisms

We select control mechanisms to enhance data sovereignty in the context of our study by considering the theoretical perspective of control theory. Cram et al. (2016) highlight how *control environment*s drive these selections. In our study, relevant control environments include a) the characteristic of data as an experience good, b) the stage of the platform's lifecycle, c) the data provider-consumer relationship, and d) the data sharing process. This leads us to focus on formal control, especially integrating input and process controls. We discuss the justification for selecting control mechanisms based on each control environment as follows.

Data as an experience good. In meta-platforms, the primary shared product is data goods. Data, being an *experience good,* presents challenges in evaluating its quality and value. Additionally, it is a *non-rivalrous good,* allowing for low-cost duplication and simultaneous use by multiple parties (Koutroumpis et al., 2020). Thus, exchanging data products triggers high uncertainty. Wiener et al. (2023) find that an *authoritative-control style,* which correlates to a top-down approach and utilizes formal control modes, can be more effective in dealing with uncertainty than an *enabling style* that aims for intensive interactions to enable informal control. An authoritative-control style provides clear guidance and direction, avoiding the confusion of seeking too many consensuses, which Wiener et al. (2023) refer to as *too many voices* that worsen uncertain conditions. Therefore, in the context of uncertain data goods, selecting formal control is likely more advantageous than informal control.

The stage of the platform's lifecycle. The meta-platforms are still in their infancy, meaning they are in the exploration stage instead of the commercialization stage. In this early stage, formal control portfolios are generally better regarding speed and efficiency (Beese et al., 2023). At this stage, where resources are limited, formal control modes yield immediate, tangible results. In contrast, informal control modes often take longer to produce observable outcomes. These quick, tangible results from formal controls are crucial for demonstrating the platforms' capabilities and attracting potential users. Therefore, in this early lifecycle stage, formal control is more suitable.

The data provider-consumer relationship. Meta-platforms enable interactions among actors who have no prior relationship. Consequently, unlike traditional business data sharing settings like supply chain networks, where goals are clear and participants know each other (van den Broek & van Veenstra, 2015), meta-platforms require a selective approach to identify well-behaved participants. Mukhopadhyay et al. (2016) highlight the appropriateness of formal control, especially input control, in selecting partners with suitable attitudes. This is because input control provides a structured and transparent method of evaluating potential actors to gatekeep those with the same value and who possess specific experiences and skills. Thus, input control is helpful to pre-select data providers and consumers.

Data sharing processes. Data sharing processes typically involve well-defined stages, consisting of preparation (e.g., describing meta-data), agreement (e.g., creating a contract), and usage (e.g., monitoring data usage) (see Section 3 for the detailed elaboration of these processes). These generic processes are embedded in reference architectures for data exchange (e.g., Firdausy et al., 2022; Scheider, Lauf, Möller, et al., 2023). Therefore, according to Ouchi (1979), process control mechanisms are particularly suitable when the process activities are well-defined, but the output is less predictable (e.g., due to the nature of data as experience good). Process control is appropriate because it enables thorough monitoring of each step, operating under the premise that diligent adherence to the process will yield the anticipated outcomes, even when the exact nature of these outcomes remains uncertain.

Control portfolio. So far, we have elaborated on how formal control, especially input and process control, is appropriate to enhance data sovereignty in the context of our study. Moving forward, we argue for the necessity of forming a control portfolio rather than relying solely on a single control mechanism. Control mechanisms are rarely standalone; they often mix to gain significant results. Building on our earlier discussion, our focus now shifts to developing a portfolio that integrates various formal control mechanisms.

Wiesche et al. (2013) find that process controls are often integrated with input controls in uncertain conditions. This integration allows process control to derive insights from various processes, identifying new and unexpected findings. Subsequently, these insights inform input control, enabling a more effective pre-screening of actors. Thus, in the context of business data sharing via meta-platforms, we can also combine process and input control. Process control draws insights from data sharing processes, while input control determines participant selection criteria. Together, these mechanisms mutually reinforce each other. For example, insights acquired from the process control could signal a demand for specific participant abilities or past experiences. These insights could subsequently be incorporated into the input control's selection criteria. In all, we aim to combine these two control modes.

Smart contract as process control and certification as input control. Building on our prior discussion, we concentrate on formal control mechanisms, emphasizing the integration of input and process controls. The only input control we find is certification; then, we focus on this technology. For process control, we identify five control mechanisms: usage control, Self-Sovereign Identity (SSI), Privacy-enhancing Technology (PET), smart contracts, and dynamic consent. Due to resource constraints, we need to consider the trade-off between breadth and depth. Consequently, we select a singular control mechanism from process control for detailed analysis.

We did not focus on PET as our review finds that it tends to emphasize the security aspect. Moreover, the *privacy* term in PET makes potential adopters and platform users generally think that PET is merely a privacy protection tool despite its critical role in enhancing control over data (Agahari et al., 2022). Therefore, focusing on PET could misdirect our respondents that we focus on the privacy aspect, which is beyond the scope of our sovereignty facet. Moreover, PET has gained considerable attention as a tool to enhance data sovereignty (see a review by Schmidt et al., 2022). Hence, we focused more on underexplored control mechanisms.

Our study did not focus on dynamic consent as it pertains more to individual data sovereignty, which diverges from our focus on organizational perspectives. We also excluded SSI from our focus, as it primarily addresses identifier data. This scope is too narrow for our broader interest in sharing data products. Usage control is promising because it enables the monitoring of data usage. However, we leaned toward selecting smart contracts because of their superiority in immutability. In fact, smart contracts are often viewed as the next generation of usage control (Chiquito et al., 2022; Siddiqui et al., 2022). Consequently, we can view smart contracts as an instantiation of usage control.

Hypotheses for control mechanisms. Our analysis in Section 6.2.5 indicates that smart contracts may contribute to the data sovereignty facets of ownership and control. In terms of ownership, smart contracts assist in safeguarding data providers' rights using pre-defined templates that specify the terms of use, financial incentives, and the types of data to be shared. Regarding control, smart contracts provide data provenance, automatic monitoring of data usage, and data revocation. Therefore, we propose the following hypothesis.

> *H1: Smart contracts enhance the data sovereignty facets of ownership (H1.a) and control (H1.b)*

Section 6.2.1 elaborates on how certifications may contribute to data sovereignty facets of security, compliance, and responsibility. For compliance, certifications increase awareness among data sharing participants about necessary compliance standards, as obtaining certification requires passing knowledge assessments. Certifications enhance the security facet by pushing data sharing actors to adhere to globally accepted standards like ISO/IEC 27001 for information security. Regarding responsibility, certifications help to delineate the roles and responsibilities of different actors. This is achieved through the establishment of clear processes and setting explicit expectations for each participant. Therefore, we propose the following hypothesis.

> *H2: Certifications enhance the data sovereignty facets of security (H2.a), compliance (H2.b), and responsibility (H2.c)*

Figure 6.2 summarizes the hypotheses for control mechanisms enhancing data sovereignty in the context of this study.

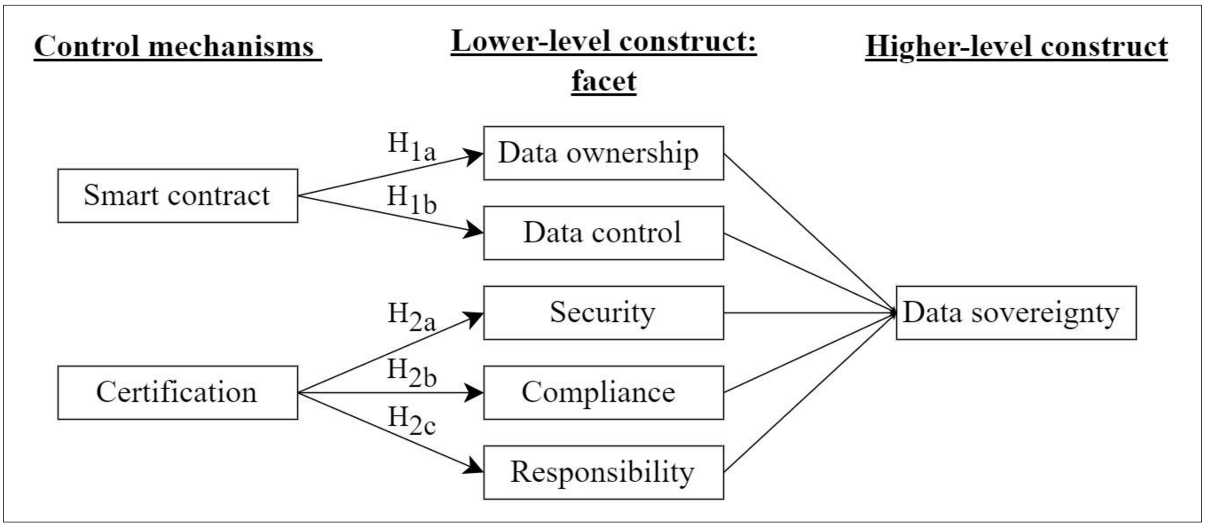


Figure 6.2. The hypotheses for control mechanisms enhancing data sovereignty

6.4 Conclusion of Chapter 6

This chapter aimed to answer the fourth research question: "*What control mechanisms can enhance data sovereignty in business data sharing via a meta-platform for data marketplaces?*" We found one control mechanism that belongs to input control: certification. We identified five control mechanisms within process control: usage control, self-sovereign identity, privacy-enhancing technology, smart contracts, and dynamic consent. Finally, we found a code of conduct as clan control (see Section 6.2).

By considering the control environment, we chose formal control, especially input and process control. For each input and process control mode, we selected one control mechanism. We focused on certification as input control and smart contracts as process control. We hypothesized that smart contracts enhance the data sovereignty facets of ownership and control; meanwhile, certifications enhance the data sovereignty facets of security, compliance, and responsibility.

By selecting smart contracts and certifications as our control mechanisms, we narrow the scope of this study. In Chapter 7, we will formulate design principles and develop a meta-platform prototype incorporating these mechanisms. In Chapter 8, we will test the perceived efficacy of smart contracts and certifications for enhancing data sovereignty.

Chapter 7: Prototype of a Meta-Platform for Data Marketplaces

Chapter 6 selected two control mechanisms to enhance data sovereignty in a meta-platform for data marketplaces: smart contracts and certifications. We hypothesized that smart contracts positively impact data ownership and control; certifications positively influence the security, compliance, and responsibility facets of data sovereignty.

This chapter develops a prototype for a meta-platform for data marketplaces, incorporating the control mechanisms of smart contracts and certifications. This chapter answers the fourth research question: *What do the developed control mechanisms look like in the meta-platform setting?* This research question emerges from a limited understanding of the design principles (the "how") and instantiations (the "what") of control mechanisms that enhance sovereignty in meta-platforms (scientific gap 3). We address this question by employing the prototyping approach.

This chapter consists of five sections. Section 7.1 discusses the prototype objective, while Section 7.2 elaborates on the prototyping approach. Section 7.3 identifies design principles for smart contracts and certifications, which Section 7.4 embeds into the prototype interfaces. Finally, Section 7.5 concludes this chapter.

7.1 Prototyping objective

A prototype is "…any representation of a design idea—regardless of medium" (Houde & Hill, 1997, p. 369) and serves as an initial version that implements various aspects of the final product (Bernstein, 1996). Prototypes enable researchers to interact with potential users, collecting feedback that informs further development and system validation (Martin, 2003).

In this study, the prototype creates a functional representation of a data marketplace meta-platform with control mechanisms of smart contracts and certifications. Developing a prototype is crucial because no hands-on meta-platform examples exist in business data sharing practices. A prototype enables participants to gain hands-on experience with the relatively novel meta-platform concept and facilitates evaluating the control mechanisms in a realistic setting. Specifically, the meta-platform prototype functions as an instrument for the 2x2 factorial experimental study discussed in Chapter 8. Prototyping is suitable for experimental studies as it allows for the manipulation of control mechanisms (Eladhari & Ollila, 2012).

7.2 Prototyping approach

We adapt a common prototyping approach in design science research that consists of four steps (e.g., Dellermann et al., 2019; Schilling et al., 2019): 1) specifying meta-requirements, 2) identifying design principles, 3) developing design features (or interfaces), and 4) evaluating the prototype. The subsequent sections detail each step.

7.2.1 Step 1: Specifying meta-requirements

We specified meta-requirements that serve as goodness criteria based on the data sovereignty facets we found in Chapter 5: data ownership, data control, security, compliance, and responsibility. *Ownership* concerns data property rights, representing privileges over data products. *Control* involves managing and directing data product flows. *Security* emphasizes protecting against threats and mitigating risks. *Compliance* ensures adherence to legal and regulatory standards, and *responsibility* delineates roles and expectations. These facets serve as meta-requirements (i.e., goodness criteria) to guide the design and evaluation control mechanisms on data sovereignty.

7.2.2 Step 2: Identifying design principles

Design principles (DP) refer to "… prescriptive statements that indicate how to do something to achieve a goal" (Gregor et al., 2020, p. 1622), guiding artifact development. We adapted Gregor et al.'s (2020) framework for presenting DPs, which includes four main components: 1) aim, implementer, and user; 2) context; 3) mechanisms; and 4) rationale. The structure of a DP template is outlined below:

> *DP Name: For Implementer I to achieve or allow for Aim A for User U in Context C, employ Mechanisms M1, M2, ... M_n because of Rationale R.*

This study derived design principles from state-of-the-art literature on smart contracts and certifications. To explain the rationale behind these principles, we employed kernel theories as a *warrant by* approach, referring to "…finding supportive evidence/argumentation for why something [artifact] works" (Möller et al. 2022, p. 8). By drawing on kernel theories of the control and signaling theories, we argue why and how these DPs may enhance specific facets of data sovereignty. An example of a smart contract design principle for enhancing data control is presented below.

> *DP_DC: For meta-platform operators (I) to allow data providers (U) to enhance data control, thus enabling data sovereignty (A) in business data sharing through meta-platforms (C), employ contract enforcement (M_1), data provenance (M_2), and data revocation (M_3).*

To understand how a design principle mechanism works, let us consider the second mechanism to retain control over data: data provenance (DP_DC_M_2). Data provenance allows providers to monitor the origin and trajectory of their data in data sharing (Meier et al., 2021). Control theory suggests that data provenance facilitates process control because it offers data providers insight into the journey of their data products. This insight allows providers to identify and address any discrepancies from set conditions (Silva et al., 2019), thereby improving their control over data. Reflecting on signaling theory, the traceability offered by blockchain-based systems can enhance quality perceptions (Yong et al., 2020; Yoo et al., 2015). Consumer choices often rely on credence attributes, such as specific details about a product's creation or handling process (Fernqvist & Ekelund, 2014). Such details are crucial in forming quality perceptions, particularly with unfamiliar brands (Treiblmaier & Garaus, 2023). In the context of meta-platforms, the nature of data as experience good heightens uncertainty, especially when data providers and consumers lack established relationships. Nonetheless, enabling traceability via data provenance mechanisms can mitigate this uncertainty. By offering detailed and verifiable information on data usage, data provenance signals transparency and, in turn, assures data providers about maintaining control over their data.

7.2.3 Step 3: Developing design features (or interfaces)

Developing a prototype involves 1) defining business data sharing tasks and 2) creating prototype interfaces. We elaborate on these two aspects in the following sections.

7.2.3.1 Defining business data sharing tasks

We first clarified the interaction scenario of a data provider in a meta-platform before defining business data sharing tasks. As discussed in Chapter 4, we focus on the one-stop shop meta-platform, specifically when *data providers directly connect to a meta-platform*. In this scenario, data providers are not associated with any marketplaces and then join a meta-platform to share their data. In doing so, providers can reach consumers from many participating marketplaces. We chose this interaction scenario to emphasize the perspectives of the data providers, who are the problem owners of data sovereignty concerns.

After clarifying the meta-platform scenario, we developed a hypothetical use case where research participants play a role as a data provider, a telecommunication company called TELCO. TELCO shares its basic data products, Called Detail Records (CDRs), which consist of statistics such as internet usage patterns or churn rates. These records are valuable for banks when constructing customer profiles for new credit card products. We created a video to explain this use case.[2] Figure 7.1 presents snapshots of the video explanation.

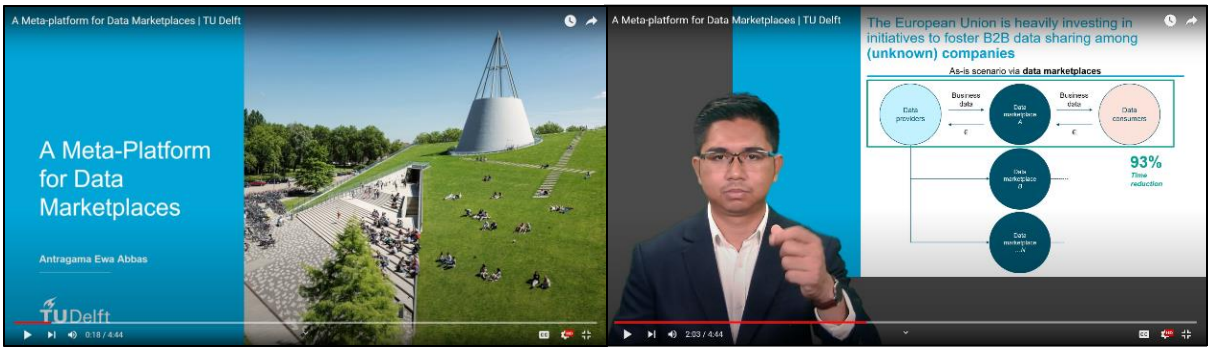

A Meta-platform for Data Marketplaces | TU Delft
A Meta-Platform for Data Marketplaces
Antragama Ewa Abbas
TUDelft
0:18 / 4:44
A Meta-platform for Data Marketplaces | TU Delft
The European Union is heavily investing in initiatives to foster B2B data sharing among (unknown) companies
As-is scenario via data marketplaces
Data providers
Business data
€
Data marketplace A
Business data
€
Data consumers
Data marketplace B
Data marketplace ...N
93%
Time reduction
2:03 / 4:44

Figure 7.1. Snapshot of video explanation

Afterward, we defined four tasks for research participants interacting with the TRUSTS meta-platform,[3] reflecting generic data sharing processes: preparation (e.g., describing metadata), agreement (e.g., creating a contract), and usage (e.g., monitoring data usage). Task 1 consists of simple subtasks to familiarize participants with the prototype. Task 2 describes the metadata of a data product, while Task 3 creates a contract for data sharing. Lastly, Task 4 allows participants to exercise the control capabilities provisioned by a meta-platform.

We created relevant interfaces for each task, resulting in 47 interfaces in total. For example, Subtask 1.1 focuses on introducing the prototype. Hence, data providers interact with

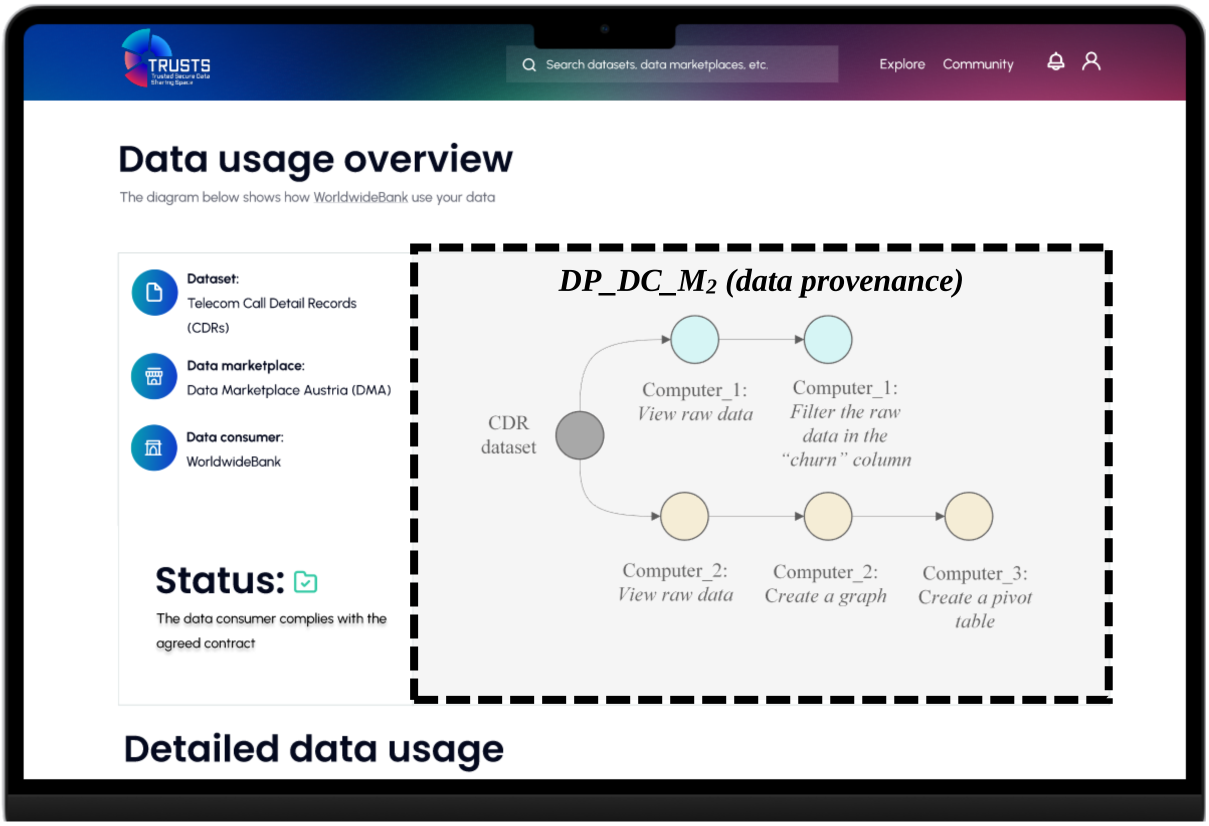
[2] https://youtu.be/9b7iKM3BiMs, accessed 13 February 2024.

[3] The PhD candidate developed this prototype as part of the Trusted Secure Data Sharing Space (TRUSTS) project work. TRUSTS is an EU-funded project aiming to design a meta-platform for data marketplaces.

the interfaces: *I_1.1.1 Before you begin (1), I_1.1.2 Before you begin (2), and I_1.1.3 Task 1 description.*

7.2.3.2 Developing prototype interfaces[4]

We developed a prototype to address data sovereignty concerns as part of an EU project consortium: the Trusted Secure Data Sharing Space (TRUSTS). The TRUSTS project creates a meta-platform for data marketplaces, which is highly in line with this study. Therefore, we used some elements of the project in the prototype (e.g., the project name, logo, and color palette). In developing the prototype interfaces, we considered the previously identified design principles. For example, we embedded the design principle of DP_DC_M$_2$ (Data provenance) in the interface *I_4.1.2 View data usage (1)* (refer to Figure 7.2).


TRUSTS
Trusted Secure Data Sharing Space
Search datasets, data marketplaces, etc.
Explore
Community

Data usage overview

The diagram below shows how WorldwideBank use your data

Dataset: Telecom Call Detail Records (CDRs)

Data marketplace: Data Marketplace Austria (DMA)

Data consumer: WorldwideBank

Status:

The data consumer complies with the agreed contract

DP_DC_M₂ (data provenance)
CDR dataset
Computer_1: View raw data
Computer_1: Filter the raw data in the "churn" column
Computer_2: View raw data
Computer_2: Create a graph
Computer_3: Create a pivot table

Detailed data usage

Figure 7.2. I_4.1.2: View data usage (1)

7.2.4 Step 4: Evaluating the prototype

We conducted a three-step evaluation cycle to assess the prototype's usability. Usability is critical as it relates to how users can learn, understand, and efficiently interact with a socio-technical to accomplish their goals (Nielsen, 1994). High usability is crucial in this study as it directly affects participants' ability to gain hands-on experience with the control mechanisms embedded in the meta-platform setting and understand their potential effects on data sovereignty. Table 7.1 summarizes the three-step evaluation cycle.

[4] All contents in the prototype interfaces are for illustration purpose only.

In Cycle 1, we identified key areas of improvement. This includes making our prototype more accessible by embedding direct links, clarifying the non-necessity of account creation, and communicating device compatibility. We also optimized performance through image compression, improving visual and navigational clarity, and refining contents to prevent confusion.

In Cycle 2, we focused on improving 1) the video explanation and 2) the prototype exploration experience. The participants' feedback yielded three main takeaways from the video explanation. First, adding subtitles would make the content clearer and more accessible to participants with different auditory processing abilities or language skills. Second, repositioning the narrator would prevent the blocking of texts and images in the presentation. Finally, enlarging the image and text size would enhance readability. The second evaluation cycle revealed three key takeaways concerning the prototype experience. First, providing consistent instructions is essential for better navigation. Second, making task descriptions more explicit aids participants in comprehending the required actions. Lastly, extending the time for participants engaging with the meta-platform to complete the required tasks is necessary.

Table 7.1. A three-step evaluation cycle

Cycle	Date	Setting	Goal	Activity
1	28 April 2022	24 MSc students in an interactive lecture	To get early feedback on usability aspects	Students interacted with the first version of the prototype, wrote improvement areas and challenges, and shared their opinions on Menti.com to facilitate discussion. We also observed any difficulties they encountered when using the prototype.
2	13 May 2022	6 PhD students in an in-person workshop	To test the usability of the second version of the prototype, including a video explanation	Participants watched a video explanation of the prototype, took notes for improvement, and then explored the prototype following task instructions. The feedback was then collectively reviewed, and the most critical points were prioritized for improvement.
3	1 June 2022	39 practitioners working on a data marketplace meta-platform in an in-person workshop	Focusing on getting feedback related to two control mechanisms: smart contracts and certifications	Participants had a 10-minute session to explore the prototype. After this exploration, they wrote feedback on the Miro board, focusing on the smart contracts and certifications.

In Cycle 3, we focused on evaluating smart contracts and certifications. Regarding smart contracts, a more accurate representation of data provenance is required to demonstrate data usage monitoring. For certifications, suggestions included adding a checklist mark for certified data marketplaces, increasing the thickness of the grey color as it tended to be less visible, and providing more detailed explanations about the International Data Space certifications to demonstrate their value. Additionally, participants mentioned the redundancy between data marketplace logos and names and recommended changing the sidebar from the right side to the left to make it more intuitive. Furthermore, they advised removing the “love” and “rating” icons, as these could act as confounding factors. Lastly, they pointed out spelling errors that needed correction and suggested changing the certification stamp color from red to green to convey a sense of approval.

All detailed feedback for enhancement suggestions and prototype modifications is detailed in Online Appendix 2. Having detailed our approach to prototyping, we now define the design principles of smart contracts and certifications in the subsequent sections.

7.3 Identifying design principles

7.3.1 Smart contracts

Based on the elaboration in Chapter 6, we formulated the following hypothesis for smart contracts:

H1: Smart contracts enhance the data sovereignty facets of ownership (H1.a) and control (H1.b).

We discuss the design principles of smart contracts to enhance the sovereignty facets of ownership and control in Sections 7.3.1.1 and 7.3.1.2, respectively.

7.3.1.1 Data ownership

Data ownership refers to the exclusive rights of data providers to claim the possession of data, hence being able to determine what should happen to the shared data (e.g., access, modification, and use) (Fadler & Legner, 2022). One potential design principle derived from the literature is provisioning *a terms-of-use template with automatic metadata generation* (Clack, 2018; Tateishi et al., 2019). This mechanism draws an analogy to application programming interfaces in the software development context, which act as repository boundary objects (cf. Ghazawneh & Henfridsson, 2010). Here, repository boundary objects refer to tools that facilitate communication across different parties by providing shared, structured formats for information sharing. In our study, the terms-of-use template offers data providers a structured guide to articulate their data sharing conditions. The terms specified in this template subsequently serve as a basis for generating metadata that reflects the agreed-upon conditions (e.g., Demichev et al., 2021).

Control theory suggests that detailed guidelines for contract specifications, for example, in the project management context, improve performance by clearly delineating duties, obligations, and rewards while also setting out key service level agreements and contingencies (Srivastava & Teo, 2012). This specificity outlines clear expectations and measures for project performance, thereby bridging the understanding gap between the parties involved. Contract specificity, thus, embodies an attempt to exert control to maintain standards and achieve desired outcomes (Srivastava & Thompson, 2012). In the context of data sharing via meta-platforms, providing a terms-of-use template operates similarly to contract specification. It explicitly lays out data usage conditions, hence enabling data ownership retention.

From the signaling theory perspective, having a detailed terms-of-use template in a contract, especially when it illustrates how risks are managed and contingencies are handled, can indicate a party's reliability. For example, parties that absorb the minimal cost in case of exceeding budget signals are unreliable in project management. Thus, contracts serve as a signaling device (Banerjee & Duflo, 2000). In the meta-platform context, the provided terms-of-use template also performs a similar signaling function. Meta-platform operators signal their reliability by offering templates explicitly addressing operational risk management and contingency planning. Consequently, data providers may perceive the platform as a facilitator for protecting their ownership rights and enhancing their sense of data ownership. To sum up, we propose the following:

> The first design principle mechanism for enhancing data ownership of data providers is to provide a terms-of-use template to create a business data sharing contract with automatic metadata generation that reflects the agreed-upon conditions (DP_DO_M$_1$)

The first design principle mechanism (DP_DO_M$_1$) provides a terms-of-use template to create a standardized format for developing data sharing contracts. Nevertheless, data providers may still struggle to complete the template due to insufficient knowledge. To tackle this issue, the second design principle mechanism aims to offer *guided configuration for determining data ownership.* According to Lee (2019), providing configuration guidance can help platform users define ownership by presenting them with explanations, examples, or recommendations to fill each contract element. This helps platform users make informed decisions about their data-sharing preferences and the impact on their ownership rights.

Guided configuration facilitates process control from the control theory standpoint. In organizational learning, for instance, a guided configuration of routinization can improve performance when employees face uncertain tasks (Liu et al., 2010). This improvement occurs because a guided configuration helps to codify and leverage accumulated knowledge via single-loop learning, a process of detecting and correcting errors within existing procedures. Applying this understanding in meta-platforms, a guided data ownership configuration serves a similar purpose. Specifically, this configuration process may help data providers navigate the complexity and uncertainty associated with defining data ownership rules of their data products. Consequently, this leads to a greater possibility of retaining data ownership.

From the signaling theory perspective, offering reliable guidance to ease uncertain tasks generates credible signals (Zhou et al., 2022), leading to positive outcomes, such as user engagement and purchasing behavior (Wells et al., 2011). Providing guided data ownership configuration can also serve as a credible signal of meta-platform operators' dedication to helping data providers retain their data ownership. Based on the above discussion, we propose the following:

> The second design principle mechanism for enhancing data ownership of data providers is to provide guided data ownership configuration to data providers (DP_DO_M$_2$)

Providing a terms-of-use template (DP_DO_M$_1$) and guided data ownership configuration (DP_DO_M$_2$) can assist data providers in defining their data-sharing preferences. However, it is essential to grant data providers the freedom to describe their data usage conditions beyond the structured template. In achieving this, one potential design principle mechanism is to provide *customizable data ownership settings* (Reyman, 2013).

Control theory explains that customization is a modification tool based on learning processes (Chown, 2021). In our context, data providers have the option to customize ownership settings to meet their unique data ownership needs, informed by their experiences in business data sharing. This personalized approach moves away from a generic one-size-fits-all policy, allowing for a more detailed expression of data ownership and fostering a more robust sense of ownership retention. Considering the signaling theory, customization acts as a strategic positioning tool by differentiating a platform operator from others, especially by demonstrating its commitment via resource availability and capabilities (Skaggs & Snow, 2004). In our study, customization may allow meta-platform operators to showcase their commitment to accommodating diverse data ownership preferences. Providing customizable settings showcases the operator's resources and capabilities, in turn, assuring data providers of their ability to maintain data ownership. Hence, we propose the following principle:

> The third design principle mechanism for enhancing data ownership of data providers is to provide to provide customizable ownership settings (DP_DO_ M$_3$)

Table 7.2 summarizes the design principles of smart contracts to enhance data ownership.

Table 7.2. Design principles of smart contracts to enhance data ownership.

Implementer (I), User (U), Aim (A), Context (C), and Mechanisms (M)		For meta-platform operators (I) to allow data providers (U) to enhance data ownership, thus enabling data sovereignty (A) in business data sharing through meta-platforms (C), employ a terms-of-use template with automated metadata generation (M$_1$), guided data ownership configuration (M$_2$), and customizable ownership settings (M$_3$).
Mechanisms		***Rationale***
DP_DO_M$_1$	A terms-of-use template with automated metadata generation	This mechanism provides a structured guide for defining data-sharing preferences and automatically generates metadata. Providing contract specifications exerts process control by enforcing standards. In addition, this mechanism acts as a signaling device to demonstrate the meta-platform's reliability in reducing operational risks.
DP_DO_M$_2$	Guided data ownership configuration	Guided configuration assists data providers in setting data ownership preferences based on standardized procedures. This mechanism improves the ability of data providers to define data ownership through single-loop learning. This mechanism also acts as a credible signal of operators' dedication to helping data providers retain their data ownership.
DP_DO_M$_3$	Customizable ownership settings	Customizable settings allow for a tailored approach to data ownership, aligning with data providers' specific needs that go beyond a generic one-size-fits-all policy. Furthermore, this mechanism demonstrates the meta-platform operator's resource readiness and adaptability.

7.3.1.2 Data control

Data control refers to the ability of data providers to steer data sharing flows according to predefined agreements with data consumers (Hummel et al., 2021; Tapia et al., 2011). Previous research highlights *contract enforcement* as a key mechanism to enhance data providers' control over their shared data (Bastiaansen et al., 2019, Lauf et al., 2022). Contract enforcement facilitates the continued monitoring of agreed data sharing conditions between providers and consumers, thus ensuring adherence to established agreements (Beck et al., 2018; Carvalho & Karimi, 2020; Petersen, 2022). Smart contracts serve as vehicles for contract enforcement, as they technologically embed agreements into codes. These codes can facilitate all stages of the contracting process, ranging from negotiation to performance (Mik, 2017).

From the perspective of control theory, enforcing contracts enables process control. For example, in the context of organizational cybersecurity, enforcement mechanisms such as role-based access control function as preventive measures against unauthorized data access. This is due to such enforcement mechanisms guiding employees to adhere to cybersecurity protocols while also enabling controllers (e.g., managers) to detect security breaches (Alqahtani & Erfani, 2021). Translated this understanding into the context of meta-platforms, enforcing contracts serves a similar purpose. It safeguards data providers from the misuse of their data products beyond what is agreed in contracts through continuous monitoring throughout the data sharing process. From a signaling theory standpoint, providing enforcement is a strong signal of the sender's intent because it is perceived as a costly investment and, therefore, shows genuine commitments (Colwell et al., 2011). Applying these insights to the meta-platform context, offering enforcement of terms of use signals the platform's commitment to delivering costly, technologically sophisticated solutions for data control. This commitment reassures data providers of their ability to control the data products they share. Therefore, we propose:

> The first design principle mechanism for enhancing data providers' control over their shared data is to provide contract enforcement (DP_DC_M$_1$)

While the first design principle mechanism (DP_DC_M$_1$) emphasizes contract enforcement to ensure adherence to agreed data sharing conditions, it does not directly address the need for data providers to trace the origin and lifecycle of their data. This tracing is known as *data provenance* (Lee et al., 2017); moreover, given the dynamic nature of meta-platforms where data moves across different entities, maintaining a detailed record of data transformations and movements becomes vital. In all, provenance generally enables data traceability (Meier et al., 2021).

As discussed in Section 7.2.2, data provenance facilitates process control because it offers data providers visibility into data product usage. This visibility enables providers to detect and rectify any deviations from the agreed terms of use (Silva et al., 2019), thus strengthening control over their shared data products. Reflecting on the signaling theory, the traceability capability of blockchain-based systems can positively impact perceptions (Yong et al., 2020; Yoo et al., 2015). Product choices often rely on certain credence characteristics, such as detailed specifics related to the product's creation or handling process (Fernqvist & Ekelund, 2014). Such information helps to shape quality perceptions, especially when dealing with unfamiliar brands (Treiblmaier & Garaus, 2023). In the meta-platform context, the inherent nature of data as an experience good triggers uncertainty, mainly when data providers and consumers do not have established relationships. However, introducing traceability through data provenance mechanisms can counter this uncertainty. By presenting detailed and verifiable information about the data's origins and handling, these mechanisms provide transparency and, consequently, reassure data providers of the control over their data. Based on the above elaboration, we propose the following:

> The second design principle mechanism for enhancing data providers' control over their shared data is to provide data provenance (DP_DC_M$_2$)

Implementing contract enforcement (DP_DC_M$_1$) and data provenance (DP_DC_M$_2$) may potentially enhance data providers' control over their shared data. However, it is imperative to consider situations where data providers may need to revoke their data (or metadata) according to modifying terms of use or in the case of conflicts (Firdausy et al., 2022). Hence, a design principle mechanism that enables *data revocation* is necessary (DP_DC_M$_3$). As suggested by Lauf et al. (2022), incorporating data deletion or data expiration dates within the terms-of-use contracts could facilitate data revocation.

Control literature suggests that revocation relates to ephemerality, the ability to be temporary (Morlok et al., 2018). In the context of social media platforms, Morlok et al. (2018) discovers that ephemerality features enhanced users' control over their shared content, largely due to the ability to manage the information flow over time. This infers that revocation enables process control within these platforms, allowing users to manage the timeline and conditions of their shared content. In our study, data revocation could also enhance data providers' control by granting them the ability to determine the lifecycle of their shared data. Therefore, we propose the following design principle:

> The third design principle mechanism for enhancing data providers' control over their shared data is to provide data revocation (DP_DC_M$_3$)

Table 7.3 summarizes the design principle mechanisms of smart contracts to enhance data control.

Table 7.3. Design principle mechanisms of smart contracts to enhance data control.

Implementer (I), User (U), Aim (A), Context (C), and Mechanisms (M)		For meta-platform operators (I) to allow data providers (U) to enhance data control, thus enabling data sovereignty (A) in business data sharing through meta-platforms (C), employ contract enforcement (M$_1$), data provenance (M$_2$), and data revocation (M$_3$).
Mechanism		***Rationale***
DP_DC_M$_1$	Contract enforcement	This mechanism ensures that data consumers adhere to the agreed contracts by technically enforcing these contracts. Implementing this on the meta-platform signals technological sophistication and commitment to data control.

Implementer (I), User (U), Aim (A), Context (C), and Mechanisms (M)		For meta-platform operators (I) to allow data providers (U) to enhance data control, thus enabling data sovereignty (A) in business data sharing through meta-platforms (C), employ contract enforcement (M_1), data provenance (M_2), and data revocation (M_3).
DP_DC_M_2	Data provenance	This mechanism offers data providers insights into the usage of their data products. Moreover, data provenance signals transparency, reassuring data providers about their ability to control their data products.
DP_DC_M_3	Data revocation	This mechanism allows data providers to revoke their data or metadata if terms of use are violated or conflicts arise. Data revocation triggers *ephemerality* (or temporariness), giving data providers control over the lifespan of their shared data.

7.3.2 Certifications

Based on the elaboration in Chapter 6, we formulated the following hypothesis for certifications:

H2: Certifications enhance the data sovereignty facets of security (H2.a), compliance (H2.b), and responsibility (H2.c).

We discuss the design principles of certifications to enhance the sovereignty facets of security (Section 7.3.2.1), compliance (Section 7.3.2.2), and responsibility (Section 7.3.2.3).

7.3.2.1 Security

Security emphasizes protecting against threats and mitigating risks related to business data sharing. One potential design principle derived from the literature is *displaying certification seals* (Lins et al., 2019). Obtaining certification seals indicates that actors have thoroughly pre-screened before accessing digital platforms (Adam et al., 2022). This pre-screening demonstrates their adherence to specific objectives during the registration phase, such as security standards (Croitor et al., 2021). Control theory suggests that such input control acts as a gatekeeper, positively influencing performance and preventing potential security issues that may be challenging to resolve later (Thies et al., 2018).

Signaling theory indicates that certification seals serve as visual indicators of adherence to security standards. For example, platform operators earn certifications to signal a superior degree of security (Lins & Sunyaev, 2017), mainly because they provide security assurance (e.g., the platform has no malware issues) (Hu et al., 2010; Lins et al., 2020; Ponte et al., 2015) and lowering users anxiety about security issues (Aiken, 2006). In our context, data providers can identify which data sharing actors, such as marketplace operators and consumers, possess these certification seals. This visibility enables them to make informed decisions about engaging with specific marketplaces and consumers, making data providers feel more secure in sharing their business data. Therefore, we propose the following:

> The first design principle mechanism for enhancing the security of data providers is to display certification seals (DP_S_M_1)

Data sharing actors showcase their commitment to strong security measures by *earning certifications that align with recognized security standards* (e.g., ISO 27001 and IEC 62443). Following these standards not only simplifies resource allocation for certification applicants (e.g., by allowing the use of existing proofs) but also provides clear guidelines for meeting security requirements (Menz, Resetko, & Winkel, 2019). Although obtaining such certifications can be costly, the investment paradoxically signals a strong commitment to security (Kang & Zhou, 2019; Shin et al., 2019). In our case, obtaining such certifications ensures that data providers adhere to established security measures and encourages other data sharing actors, like marketplace operators and consumers, to follow the same measures. This enhances overall security in business data sharing. Based on these observations, we suggest the following design principle mechanism:

> The second design principle mechanism for enhancing the security of data providers is to ensure certification compatibility with established security standards (DP_S_M$_2$)

Table 7.4 summarizes the design principles of certification to enhance security.

Table 7.4. Design principles of certifications to enhance security.

Implementer (I), User (U), Aim (A), Context (C), and Mechanisms (M)		For meta-platform operators (I) to allow data providers (U$_1$) to enhance security, thus enabling data sovereignty (A) in business data sharing through meta-platforms (C), display certification seals (M$_1$) and ensure certification compatibility with established security standards (M$_2$).
Mechanism		***Rationale***
DP_S_M$_1$	Certification seals	Certification seals serve as visual signals that data sharing actors adhere to security standards. This visibility enables data providers to make informed choices about which marketplaces and consumers to engage with.
DP_S_M$_2$	Compatibility with established security standards	Earning certifications that meet recognized security standards is expensive, signaling commitment from data sharing actors to follow security measures.

7.3.2.2 Compliance

Compliance represents the adherence to relevant legal and regulatory frameworks (Hummel et al., 2021), especially for sharing business data. Implementing *certification validity audits* is the first design principle mechanism for enhancing compliance. Certification validity audits check relevant regulations and technical standards by conducting audits, both before joining a platform and periodically afterward (Greulich et al., 2020; Lansing et al., 2019). These certification validity audits are like assurance statements (cf. Lowry et al., 2012), signaling a cue related to expertness. This demonstrates that platform operators or user groups conducting these audits are proficient in understanding and continuously adhering to regulatory frameworks.

Following this logic, data providers undergo certification audits to enhance their compliance knowledge and maintain continuous adherence. Furthermore, these audits empower data providers to selectively engage with data marketplace operators and consumers, using the audit as a cue of compliance know-how. Therefore, certification validity audits serve as a mechanism for emphasizing regulatory framework compliance. Drawing from this insight, we propose the following design principle:

> The first design principle mechanism for enhancing compliance of data providers is to provide certification validity audits (DP_C_M_1)

Another design principle mechanism to enhance compliance is to provide *explicit compliance statements*. Certifications must be explicit about their compliance coverages, as these act as signals of adherence to specific regulations or standards. For example, the EU introduces a register of so-called *EU-recognized data intermediaries*, signaling adherence to the European Data Governance Act[5]. In doing so, certification sets clear expectations for those seeking (and seeing) it (Anwar & Gill, 2021). Consequently, this clarity enhances the assurance of those seeking certification (cf. Sturm et al., 2014). In our study, data providers who obtain certifications with explicit compliance statements gain certainty about their compliance coverage. In addition, data providers can verify if data marketplace operators and data consumers are certified, and such providers can understand the scope of these certifications. This ensures that all involved parties, especially data providers, are confident in their adherence to relevant regulatory frameworks. We propose the following design principle:

> The second design principle mechanism of certifications for enhancing compliance of data providers is to provide explicit compliance statements (DP_C_M_2)

Certification must include platform operators offering *integrated legally-valid management and dispute resolution* (e.g., Moyano et al., 2021). In our study, it means that meta-platform operators should provide data providers with tools to create, access, and download legally binding contracts. Data providers should be able to review these contracts to ensure they accurately reflect the terms of use. Furthermore, there should be a clear process for addressing disputes, including situations where data misuse is suspected (e.g., data used in ways that violate the agreed terms). Huang et al. (2005) suggest that this mechanism offers structural assurance through the lens of signaling theory, demonstrating that the meta-platform has enacted protective legal measures to defend data providers' interests. This establishes a legal foundation for data providers, thereby enhancing their adherence to applicable legal and regulatory frameworks for business data sharing. Hence, we propose the following:

> The third design principle mechanism for enhancing compliance of data providers is to have integrated legally-valid contract management and dispute resolution (DP_C_M_3)

Finally, *endorsement from authoritative bodies* can also enhance the data sovereignty facet of compliance. Generally, endorsement from authoritative bodies works better than self-description signals (Zhou et al., 2022). Such endorsements invoke the authority principle,

[5] https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services, accessed on 13 February 2024.

leading platform users to trust and follow the guidance, recommendations, or opinions of authoritative entities when making decisions (Lins & Sunyaev, 2022). This is because the authority principle is part of peripheral processing, in which platform users rely on straightforward cues like endorsements to make decisions rather than engaging in extensive, in-depth content analysis. In our study, data providers receiving certifications from recognized endorsing bodies are more likely to adhere to relevant legal and regulatory frameworks. This is particularly true when these frameworks (e.g., European Data Governance act) are established by the endorsing authorities themselves (e.g., European Commission). Furthermore, data providers can choose data marketplace operators and consumers based on these certifications. This means data providers can make more informed decisions about engagement based on these signals, enhancing their compliance with legal and regulatory frameworks. We propose the following:

> The fourth design principle mechanism for enhancing compliance of data providers is to have endorsement from authoritative bodies (DP_C_M_4)

Table 7.5 summarizes the design principles of certifications to enhance compliance.

Table 7.5. Design principles of certifications to enhance compliance.

Implementer (I), User (U), Aim (A), Context (C), and Mechanisms (M)		For meta-platform operators (I) to allow data providers (U_1) to enhance compliance, thus enabling data sovereignty (A) in business data sharing through meta-platforms (C), employ certification validity audit (M_1), explicit compliance statements (M_2), integrated legally-valid contract management and dispute resolution (M_3), and endorsement from authoritative bodies (M_4).
Mechanism		***Rationale***
DP_C_M_1	Certification validity audit	This mechanism allows data providers to understand and continuously adhere to regulatory frameworks. This also allows data providers to selectively engage with data marketplace operators and consumers, using the validity audits as a cue of compliance know-how.
DP_C_M_2	Explicit compliance statements	Explicit compliance statements define the compliance coverages, singling compliance with standards that improve the perceived assurance of data providers.
DP_C_M_3	Integrated legally-valid management and dispute resolution	This mechanism signals structural assurance, indicating that meta-platform operators have enacted protective legal measures to safeguard the interests of data providers.
DP_C_M_4	Endorsement from authoritative bodies	Endorsements invoke the authority principle, increasing compliance of data providers by following authoritative guidance.

7.3.2.3 Responsibility

The data sovereignty facet of responsibility delineates roles and expectations (Hummel et al., 2021), especially between meta-platform and participating data marketplace operators, to provision appropriate mechanisms for data providers. The first design principle mechanism for enhancing responsibility is to provide *explicit delineations* within certification criteria. Explicit delineations formally define the responsibilities expected of the involved parties, including specifying their tasks and identifying the required skills (e.g., Schumann & Döring, 2022). Explicit delineations are evident in certification acquisition processes. For instance, to obtain data sharing certifications from the International Data Spaces Association (IDSA), applicants must initially specify their roles (Menz, Resetko, & Otto, 2019). This clarification is crucial as it directly influences the type of certification awarded. Roles vary widely, including core participants like data providers, intermediaries such as data marketplace operators, and third-party providers like application developers, each with unique requirements. This initial step ensures a clear understanding of responsibilities, tasks, and necessary skills, meaning having explicit delineations sends signals that all parties understand their obligations (cf. Lansing et al., 2018). Based on this understanding, we propose the following:

> The first design principle mechanism for enhancing responsibility division is to have *explicit delineations* (DP_R_M$_1$)

Enhancing responsibility also involves *providing transparent information about certification bodies*. Certification bodies are organizations that issue certifications, which can be granted by standardization bodies, public agencies, industry associations, or private auditors (Lansing et al., 2018). The choice of certification body is critical, as it affects the legitimacy of certification acquirers. Third-party certification bodies, like IDSA, are more credible than first-party signals as they are not directly involved in transactions (Zhou et al., 2022). Receiving transparent information about the chosen certification body enables involved parties, such as the data providers in our study, to critically assess the certification requirements. This is particularly important for understanding the explicit delineation of responsibility (see the previous design principle mechanism). Earning certification from legitimate bodies signals the commitment of the parties to their responsibilities tailored to their roles (Lauf et al., 2022). Based on this understanding, we propose the following:

> The second design principle mechanism for enhancing responsibility division is to provide transparent information about the certification body (DP_R_M$_2$)

Table 7.6 summarizes the design principles of certifications to enhance responsibility.

Table 7.6. Design principles of certifications to enhance responsibility.

Implementer (I), User (U), Aim (A), Context (C), and Mechanisms (M)		For meta-platform operators (I) to allow data providers (U$_1$) to enhance responsibility, thus enabling data sovereignty (A) in business data sharing through meta-platforms (C), employ explicit delineations (M$_1$) and provide transparent information about the certification body (M$_2$).
Mechanism		***Rationale***
DP_R_M$_1$	Explicit delineations	This mechanism formally defines the responsibilities expected of the involved parties, including specifying their tasks and identifying the required skills, hence signaling that all parties understand their obligations.
DP_R_M$_2$	Transparent certification body information	Earning certification from legitimate bodies signals the commitment of the parties to their responsibilities, tailored to their roles.

7.4 Developing prototype interfaces

Section 7.4 describes the developed prototype interfaces, ordered by four tasks elaborated in Section 7.2.3. Task 1 familiarizes data providers with the TRUSTS meta-platform. Task 2 describes the metadata of a data product, while Task 3 generates an automatic contract. Finally, Task 4 allows data providers to exercise the control capabilities of the TRUSTS meta-platform. We also discuss the connection between interfaces and design principles when relevant.

Due to page limitations, we detail the prototype interfaces in Online Appendix 3. The following sections offer an overview of each task, its associated interfaces, and descriptions thereof. We also present a few examples of the prototype interfaces.

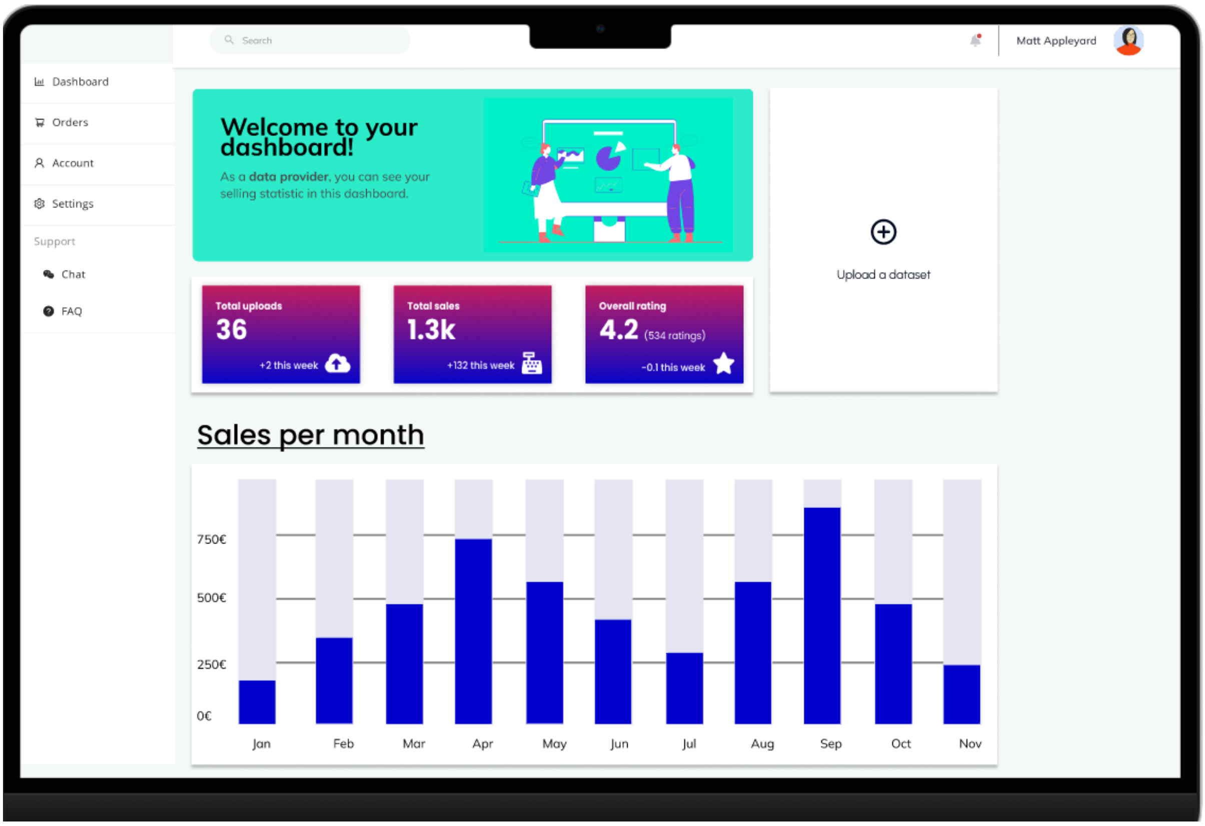
7.4.1 Task 1: Familiarizing data providers with the prototype

Task 1 familiarizes data providers with the prototype by providing essential information for interacting with the TRUSTS meta-platform. Table 7.7 shows the division of this task into three subtasks. The first subtask provides general guidance on how to use the prototype. The second subtask guides data providers through exploring the homepage, where they can learn about data marketplace participants and TRUSTS business processes. The third subtask showcases how a data provider can sign in and access their dashboard. The dashboard provides an account overview and displays available key performance indicators such as total uploads, total sales, overall rating, and sales per month. Although the interfaces in Task 1 do not directly relate to specific design principles, they are essential for data providers to understand the meta-platform's overall structure and offered features.

Table 7.7. Task 1 description

ID	Interface	Description
Subtask 1.1: Introducing the TRUSTS meta-platform prototype		
I_1.1.1	Before you begin	I_1.1.1 provides the necessary information to use the prototype.
I_1.1.2	Before you begin (2)	I_1.1.2 provides the necessary information to use the prototype.
I_1.1.3	Task 1 description	I_1.1.3 explains Task 1.
Subtask 1.2: Exploring the homepage		
I_1.2.1	Explore homepage	I_1.2.1 presents the primary information of the TRUSTS meta-platform, including introducing data marketplace participants and TRUSTS business processes.
Subtask 1.3: Signing in as a data provider		
I_1.2.2	Sign in	I_1.2.2 signs in a data provider in the TRUSTS meta-platform.
I_1.2.3	View dashboard	I_1.2.3 provides an overview of the data provider's account and available key performance indicators, such as total uploads, total sales, overall rating, and sales per month.

We present the interface *I_1.2.3 View dashboard* as an example (refer to Figure 7.3). After signing in, data providers access their personalized dashboard, which shows key metrics such as upload counts, sales figures, and overall ratings. Additionally, data providers can upload data products from the dashboard, leading them to Task 2.



Welcome to your dashboard!

As a **data provider**, you can see your selling statistic in this dashboard.

Figure 7.3. I_1.2.3: View dashboard

7.4.2 Task 2: Describing the metadata of a data product

Data providers need to describe the metadata of a dataset in Task 2. This task comprises three subtasks that guide data providers to prepare data sharing (refer to Table 7.8). Subtask 2.1 requires data providers to complete the provided template to describe their dataset. In Subtask 2.2, data providers must verify their dataset's compliance with GDPR requirements by conducting a self-assessment and providing any relevant sample data for analysis. Subtask 2.3 guides data providers in selecting suitable data marketplaces for sharing their dataset information (i.e., metadata) to reach a wider audience of potential consumers.

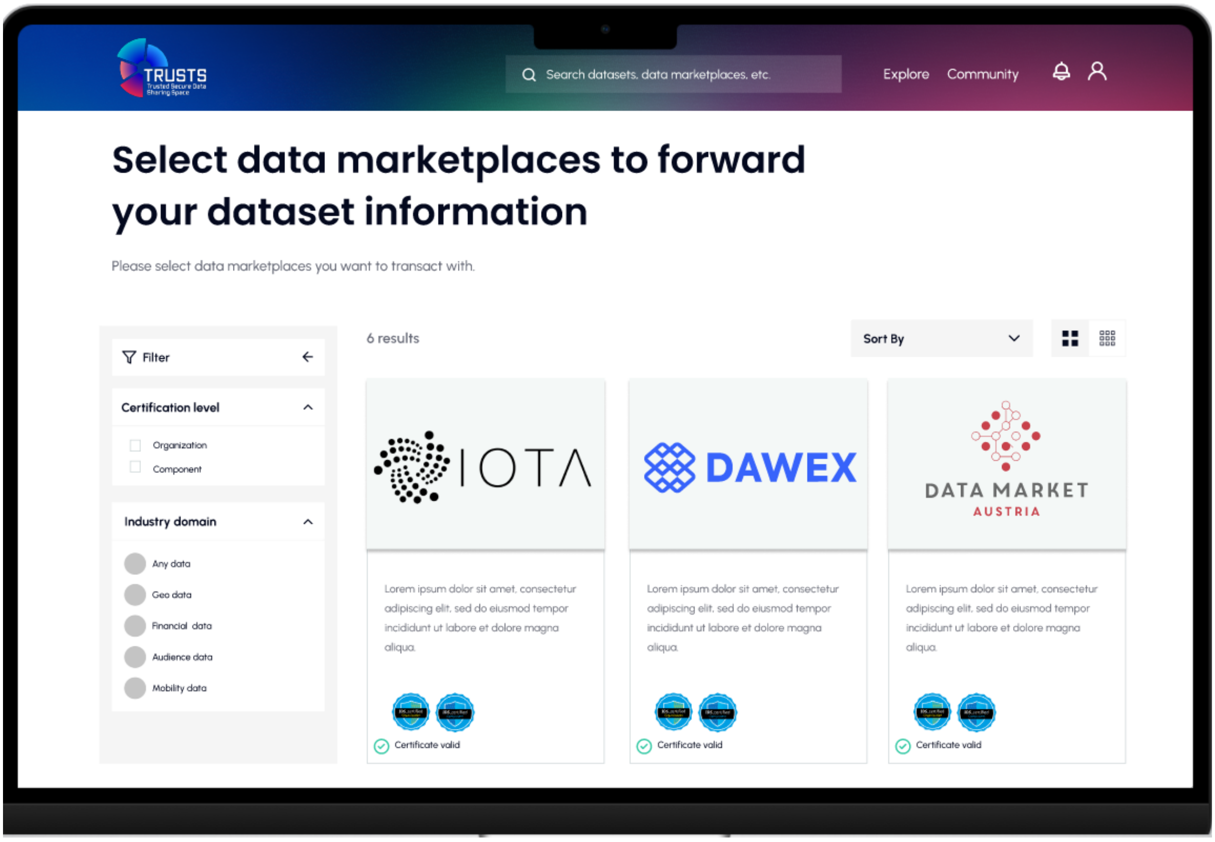
Table 7.8. Task 2 description

ID	Interface	Description	
Introducing Task 2			
I_2	Task 2 introduction	I_2 explains Task 2.	
Subtask 2.1: Describing the dataset by filling out the template			
I_2.1.1	Describe dataset	In I_2.1.1, data providers describe the dataset to be shared via the TRUSTS meta-platform, including information such as title, description, data type, and dataset tags.	***Design principles:*** • DP_DO_M$_1$: A terms-of-use template with metadata generation

ID	Interface	Description	
I_2.1.2	Upload dataset	I_2.1.2 uploads the dataset by selecting a file from a repository and enabling overview data samples.	- DP_DO_M$_2$: Guided data ownership configuration - DP_DO_M$_3$: Customizable ownership settings
I_2.1.3	Select data storage	I_2.1.3 selects data storage for the dataset, either in its own infrastructure, cloud storage provided by the TRUSTS meta-platform, or data consumer infrastructure.	
I_2.1.4	Define terms of use	I_2.1.4 specifies the term of use by selecting billing schema, period of validity, and detailed data usage conditions.	
Subtask 2.2: Checking the compliance with GDPR requirements			
I_2.2.1	Check GDPR compliance	I_2.2.1 checks GDPR compliance by performing a self-assessment. The meta-platform will also analyze the sample data provided (if available).	
Subtask 2.3: Selecting data marketplaces to share metadata			
I_2.3.1	Decide data marketplaces	I_2.3.1 chooses the data marketplaces to share metadata with. Data providers can filter data marketplace based on their certification level or industry domain.	***Design principles:*** - DP_C_M$_1$: Certification validity audit - DP_S_M$_1$: Certification seals
I_2.3.2	View certificate status	I_2.3.2 reviews the certification earned by a data marketplace. The data marketplace information includes headquarters, certified since, operates in, and website. The interface also states that the International Data Space Association (IDSA) is a certification body.	***Design principles:*** - DP_C_M$_1$: Certification validity audit - DP_C_M$_2$: Explicit compliance statements - DP_R_M$_1$: Explicit delineations - DP_R_M$_{2:}$ Transparent certification body information - DP_S_M$_1$: Certification seals
I_2.3.3	View certificate information	I_2.3.3 informs the IDS-certified component and organization. This page also shows endorsement from the European Union.	***Design principles:*** - DP_C_M$_1$: Certification validity audit - DP_C_M$_2$: Explicit compliance statements - DP_C_M$_4$: Endorsement from authoritative bodies - DP_S_M$_2$: Compatibility with established security standards
I_2.3.4	View updated dashboard	I_2.3.4 shows the updated dashboard after uploading the dataset and adding metadata to a data marketplace.	

We provide an example of how data providers interact with the prototype interfaces to complete *Subtask 2.3: Selecting data marketplaces to share metadata.* Subtask 2.3 requires data providers to choose the participating data marketplaces to distribute their dataset's metadata. As shown in Figure 7.4, *I_2.4.1* lists available participating data marketplaces, each represented by its logo, a brief description, and relevant certification information. Integrating these certification elements into the prototype shows the implementation of two key design principles: DP_C_M$_1$ (Certification validity audit) and DP_S_M$_1$ (Certification seal).

Data providers can arrange the list according to their specific criteria using the sorting feature at the top of the interface. Additionally, a filter bar is located on the left side of the interface, allowing data providers to narrow down their selection by certification levels or industry domains.



Select data marketplaces to forward your dataset information

Please select data marketplaces you want to transact with.

6 results

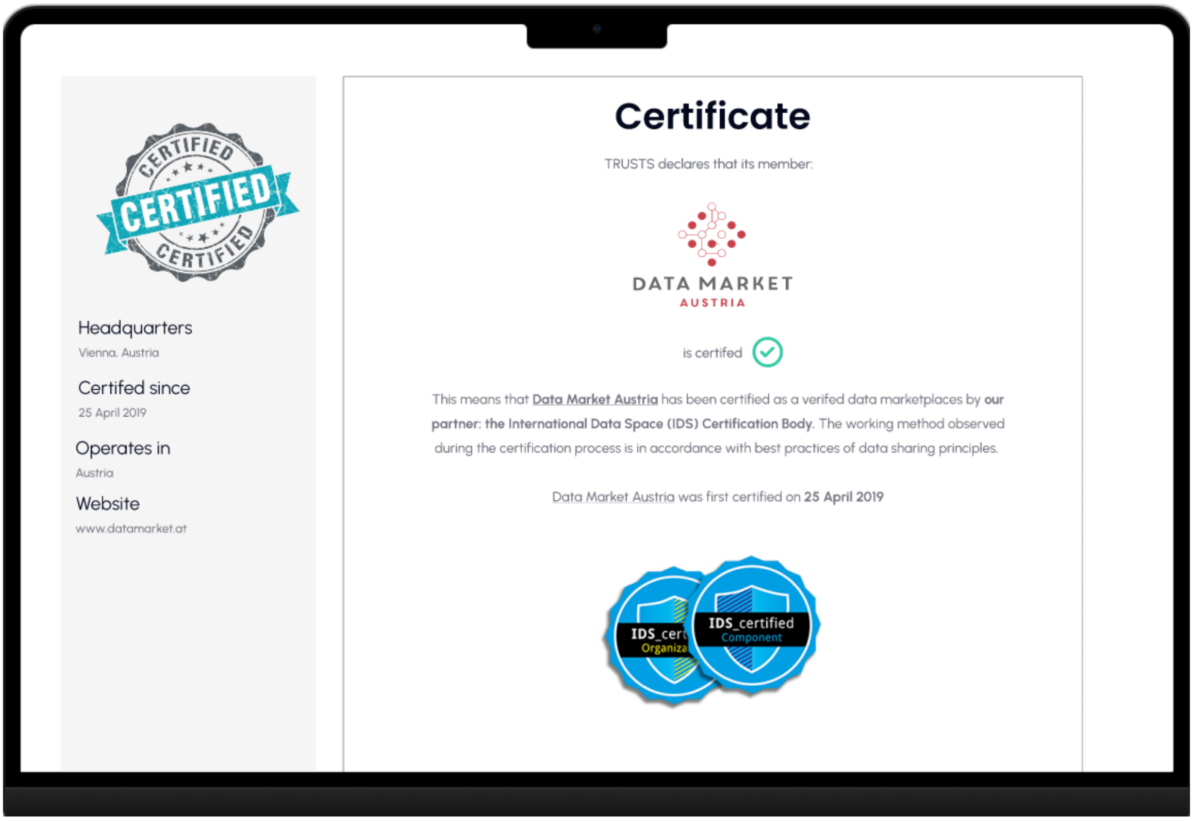
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Figure 7.4. I_2.3.1: Decide data marketplaces

Data providers can view the certification details of a specific data marketplace in *I_2.4.2* (Figure 7.5), which embeds several design principles. In this illustration, the certificate for Data Market Austria incorporates DP_C_M$_1$ (Certification validity audit from authoritative bodies) and DP_S_M$_1$ (Certification seals) by displaying the International Data Space (IDS) certification logo. *I_2.4.2* also showcases DP_ C_M$_2$ (Explicit compliance statements) as it clearly states that Data Market Austria follows the best data sharing practices from IDS. Moreover, *I_2.4.2* integrates DP_R_M$_1$ (Explicit delineations) and DP_R_M$_2$ (Certification body information) by including signatures from both the TRUSTS chief executive officer and the representative of the IDS certification body. These signatures highlight the roles and responsibilities of the parties involved in the certification process. On the left side of the interface, a certification stamp is visible, providing additional information about Data Market Austria, such as its headquarters in Vienna, Austria, the certification date, the country it operates in, and the website address.



Headquarters
Vienna, Austria

Certifed since
25 April 2019

Operates in
Austria

Website
www.datamarket.at

Certificate

TRUSTS declares that its member:

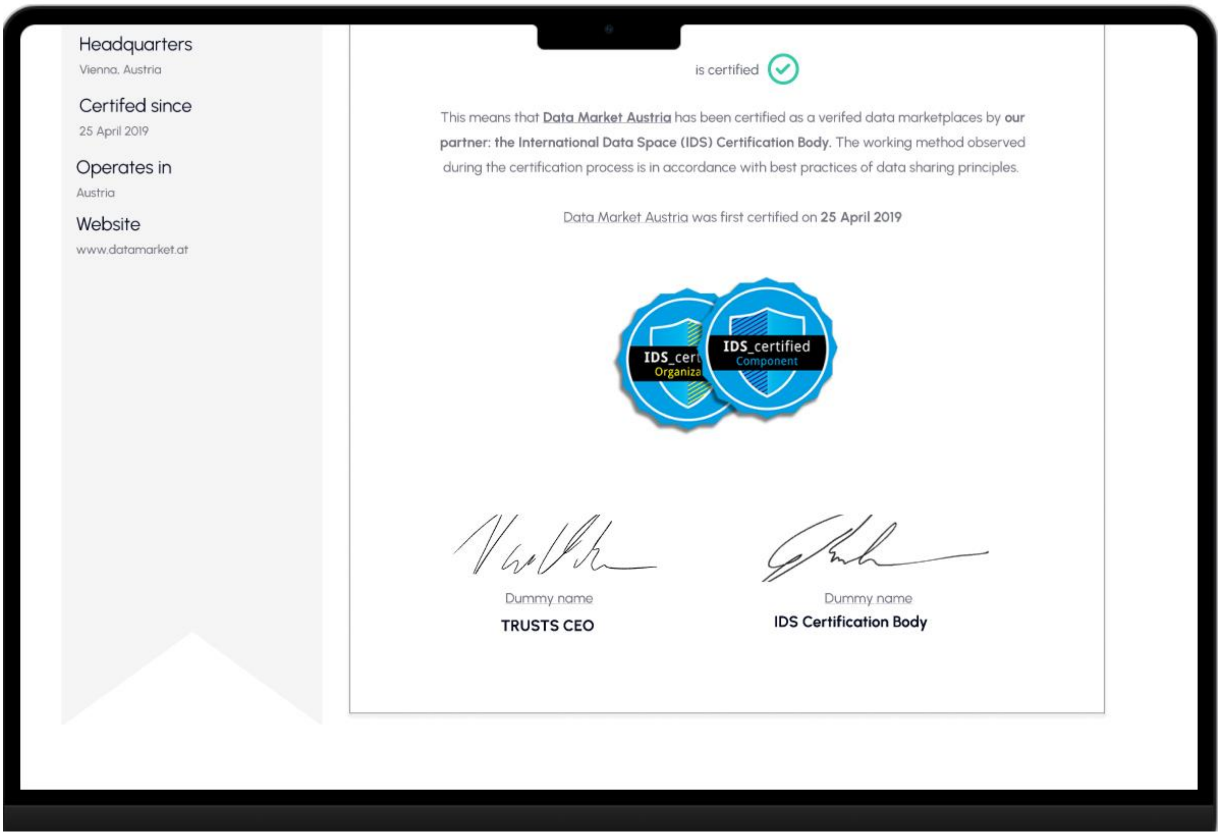
DATA MARKET
AUSTRIA

is certifed ✓

This means that Data Market Austria has been certified as a verifed data marketplaces by **our partner: the International Data Space (IDS) Certification Body**. The working method observed during the certification process is in accordance with best practices of data sharing principles.

Data Market Austria was first certified on **25 April 2019**

Figure 7.5. I_2.4.2: View certificate status 1



Headquarters
Vienna, Austria

Certifed since
25 April 2019

Operates in
Austria

Website
www.datamarket.at

is certified ✓

This means that Data Market Austria has been certified as a verifed data marketplaces by **our partner: the International Data Space (IDS) Certification Body**. The working method observed during the certification process is in accordance with best practices of data sharing principles.

Data Market Austria was first certified on **25 April 2019**

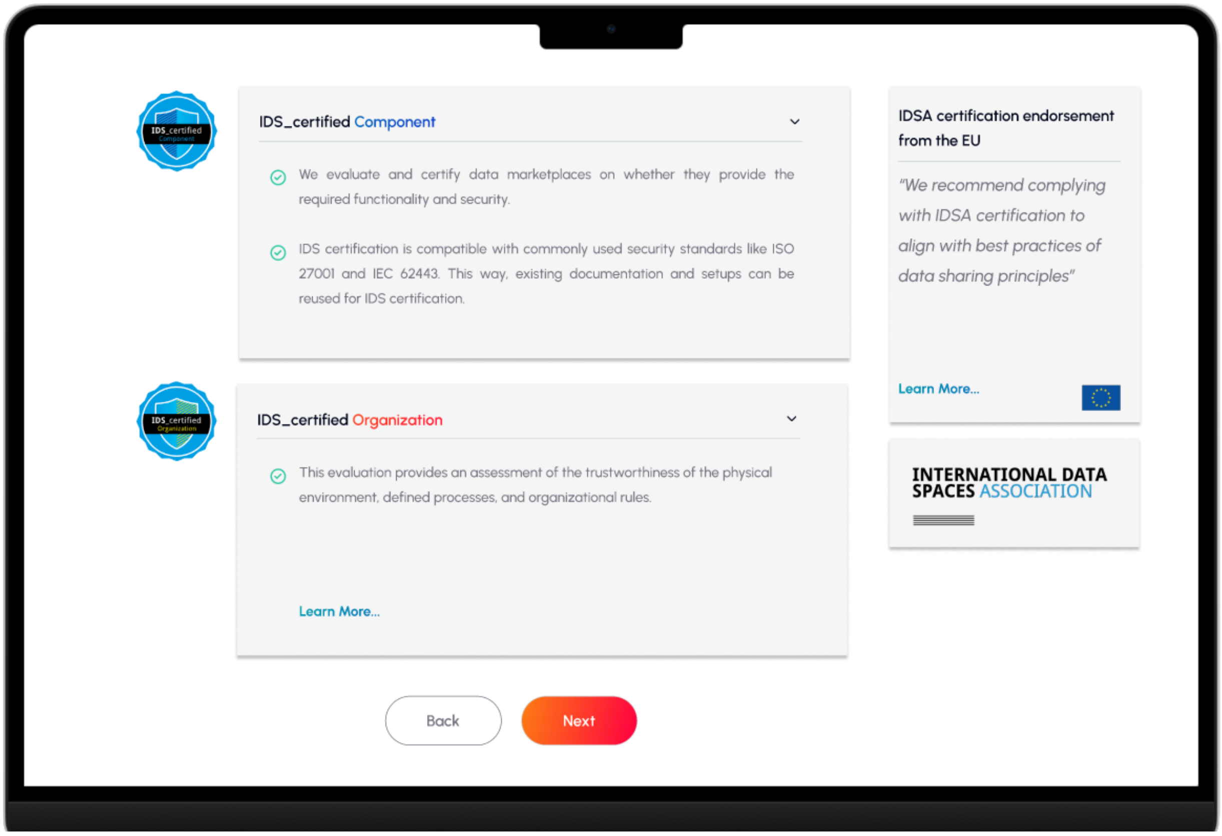
Dummy name
TRUSTS CEO

Dummy name
IDS Certification Body

Figure 7.6. I_2.4.2: View certificate status 2

Data providers continue to engage with *I_2.4.3* (Figure 7.7). In this interface, data providers can view the certifications earned by Data Market Austria, which include the IDS_certified Component and IDS_certified Organization. As suggested by design principle DP_S_M$_2$ (Compatibility with established security standards), the IDS_certified Component logo indicates that Data Market Austria has been assessed to meet the necessary security requirements. This certification is compatible with well-known security standards like ISO 27001 and IEC 62443, allowing for reusing existing documentation and setups for IDS certification.

Following design principle DP_C_M$_2$ (Explicit compliance statements), the IDS_certified Organization logo signifies that Data Market Austria's physical environment, processes, and organizational rules have been evaluated, offering an explicit compliance statement and demonstrating adherence to data sharing best practices. On the right side of the interface, the EU's IDSA certification endorsement, in line with design principle DP_C_M$_4$ (Endorsement from authoritative bodies), emphasizes the importance of complying with IDSA certification to align with data-sharing best practices. The IDSA logo, following design principle DP_C_M$_1$ (Certification validity audit), further validates the certification, confirming that an authoritative body has audited the process.



IDS_certified Component

We evaluate and certify data marketplaces on whether they provide the required functionality and security.

IDS certification is compatible with commonly used security standards like ISO 27001 and IEC 62443. This way, existing documentation and setups can be reused for IDS certification.

IDS_certified Organization

This evaluation provides an assessment of the trustworthiness of the physical environment, defined processes, and organizational rules.

IDSA certification endorsement from the EU

"We recommend complying with IDSA certification to align with best practices of data sharing principles"

IDS_certified Component
IDS_certified Organization
Learn More...
Learn More...
INTERNATIONAL DATA SPACES ASSOCIATION
Back
Next

Figure 7.7. I_2.4.3: View certificate information

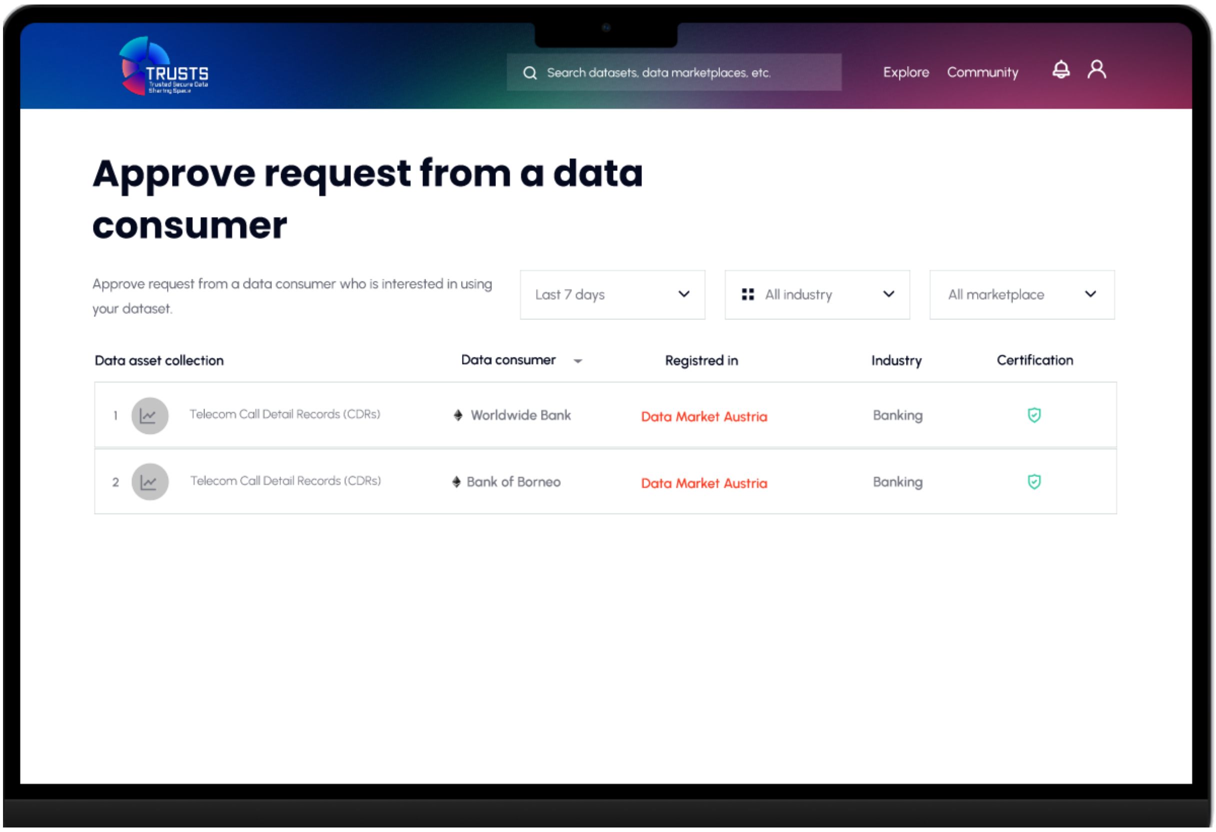
7.4.3 Task 3: Creating a contract

Task 3 focuses on creating a contract within the TRUSTS meta-platform. This task is divided into three subtasks: approving a request from a data consumer, generating an automatic contract, and viewing the contract. Table 7.9 summarizes the description of Task 3.

Table 7.9. Task 3 description

ID	Interface	Description	
Introducing Task 3			
I_3	Task 3 introduction	I_3 explains Task 3.	
Subtask 3.1: Approving a request from a data consumer			
I_3.1.1	Select a request	I_3.1.1 selects a request from data consumers for using the dataset.	**Design principle:** • DP_C_M_1: Certification validity audit
I_3.1.2	Accept data consumer	I_3.1.2 approves data consumers who are interested in using the uploaded dataset. This includes reviewing their intended use. The data consumer contains information on whether they have also acquired a certificate. This interface also refers to the data consumer website and their contact information.	
Subtask 3.2: Generating an automatic contract			
I_3.2.1	View smart contract explanation	I_3.2.1 explains smart contracts and shows the automatic contract generation process.	**Design principle:** • DP_DC_M_1: Contract enforcement • DP_C_M_3: Integrated legally-valid management and dispute resolution
I_3.2.2	View contract	I_3.2.2 presents contract details between a data provider and a consumer registered in a data marketplace. Contract overview details include data product title, description, data product type, billing schema and pricing, validity period, data storage, term of use, data use case, and compliance.	
Subtask 3.3: Viewing your contract			
I_3.3.1	See the contract PDF file	I_3.3.1 shows the automated generated contract in PDF format.	**Design principle:** • DP_C_M_3: Integrated legally-valid contract management and dispute resolution

We provide examples of how data providers conduct *Subtask 3.1: Approving a request from a data consumer* and *Subtask 3.2: Generating an automatic contract.* The interface *I_3.1.1 select a request* presents data providers with a table displaying requests from data consumers interested in using their dataset (refer to Figure 7.8). The table showcases essential information about each request, such as the data product collection, data consumer details, registration in a specific data marketplace, industry type, and certification status. In this example, the data consumers are Worldwide Bank and Bank of Borneo, registered in Data Market Austria and operating within the banking industry. Both data consumers have a certification status marked with a "v" (checklist), reflecting their adherence to the design principle DP_C_M1 (Certification validity audit), which focuses on ensuring certification validity through auditing processes. Data providers can also employ filter functions to view requests from specific periods, industries, or data marketplaces.


TRUSTS
Trusted Secure Data Sharing Space
Search datasets, data marketplaces, etc.
Explore
Community

Approve request from a data consumer

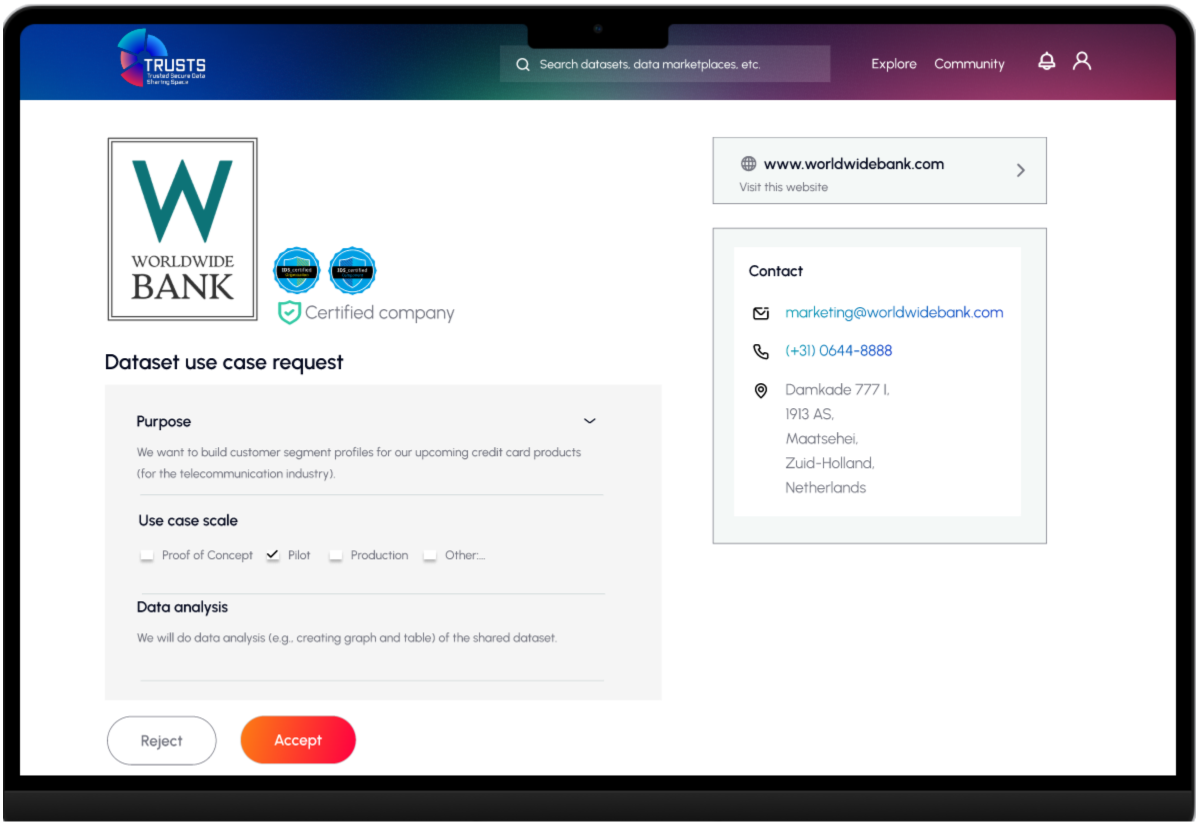
Approve request from a data consumer who is interested in using your dataset.

Last 7 days
All industry
All marketplace

	Data asset collection	Data consumer	Registred in	Industry	Certification
1	Telecom Call Detail Records (CDRs)	Worldwide Bank	Data Market Austria	Banking	✓
2	Telecom Call Detail Records (CDRs)	Bank of Borneo	Data Market Austria	Banking	✓

Figure 7.8. I_3.1.1: Select a request

Data providers interact with *I_3.1.2* after choosing a request (Figure 7.9). The interface presents detailed information about the data consumers and data providers are considering accepting. The interface incorporates the design principle DP_C_M1 (Certification validity audit) by displaying the data consumer's logo, IDSA certification seals, and a "certified company" checklist. Data providers can examine the data consumer's intended purpose and data analysis plans. The right panel shows the data consumer's contact details and website information for further communication. They can accept or reject the request using the provided buttons. Once data providers decide, they move to the next step, which involves generating an automatic contract.


TRUSTS
Trusted Secure Data Sharing Space
Search datasets, data marketplaces, etc.
Explore
Community
WORLDWIDE BANK
Certified company
Reject
Accept

Dataset use case request

Purpose

We want to build customer segment profiles for our upcoming credit card products (for the telecommunication industry).

Use case scale

□ Proof of Concept ☑ Pilot □ Production □ Other:...

Data analysis

We will do data analysis (e.g., creating graph and table) of the shared dataset.

www.worldwidebank.com
Visit this website

Contact

✉ marketing@worldwidebank.com

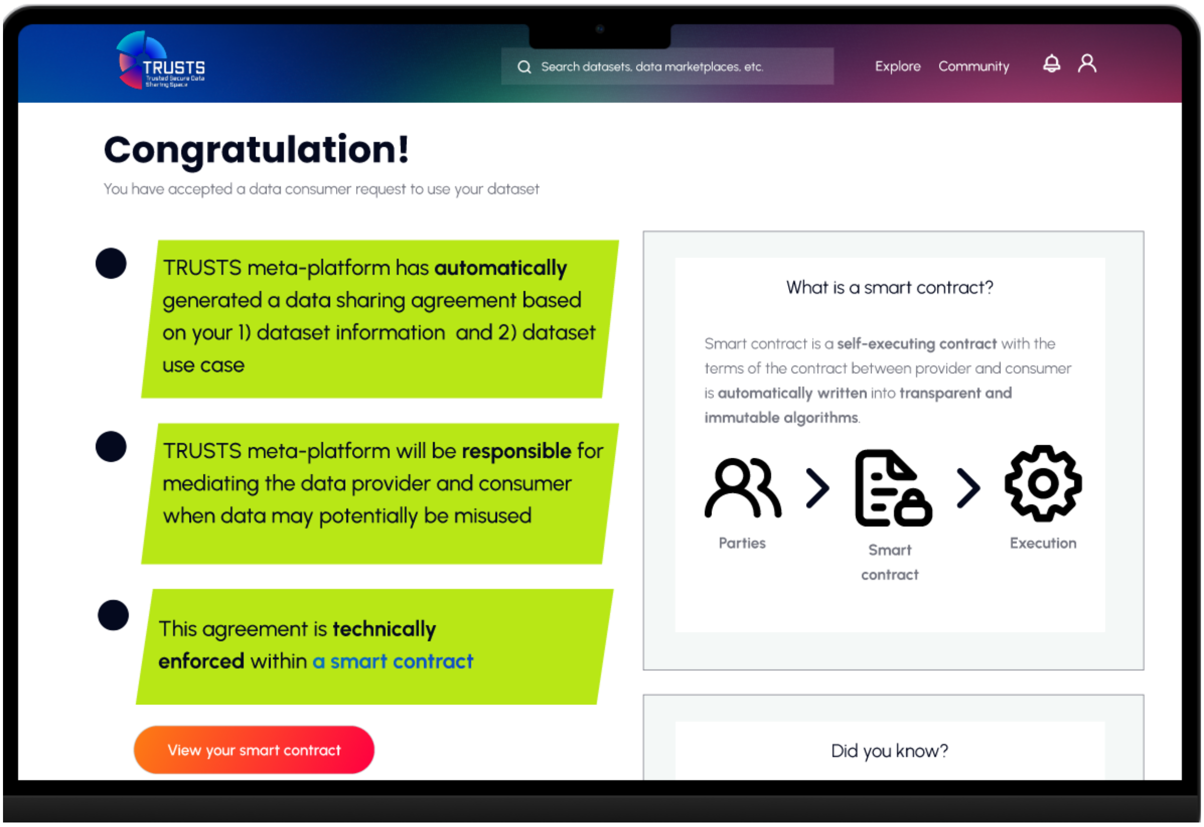
☎ (+31) 0644-8888

Damkade 777 I,
1913 AS,
Maatsehei,
Zuid-Holland,
Netherlands

Figure 7.9. I_3.1.2: Accept a request

Data providers engage with *I_3.2.1* to receive an explanation about smart contracts when they accept a request (Figure 7.10). The prototype notifies data providers of their successful acceptance of a data consumer's request. The prototype has automatically generated a data-sharing agreement enforced within a smart contract, demonstrating the implementation of the design principles DP_DC_M$_1$ (Contract enforcement) and DP_C_M$_3$ (Integrated legally-valid contract management and dispute resolution). The interface also briefly explains smart contracts, highlighting their transparent, immutable, and self-executing nature. Data providers can then view their generated smart contract by clicking the "View your smart contract" button.

Data providers can view a contract summary between the TELCO company (data provider) and WorldwideBank (data consumer) registered in Data Market Austria on *I_3.2.2* (refer to Figure 7.11). The contract contains crucial information, including data product title, description, type, billing schema, pricing, period, data storage, terms of use, data use case, and compliance information. The left panel interface offers data providers navigation options for managing the smart contract, such as adding an addendum clause, viewing the PDF file, checking data usage, accessing technical assistance, or raising a dispute. This interface demonstrates the design principle DP_C_M$_3$ (Integrated legally-valid contract management and dispute resolution) by providing a clear and detailed contract overview generated automatically through the TRUSTS meta-platform.



Congratulation!

You have accepted a data consumer request to use your dataset

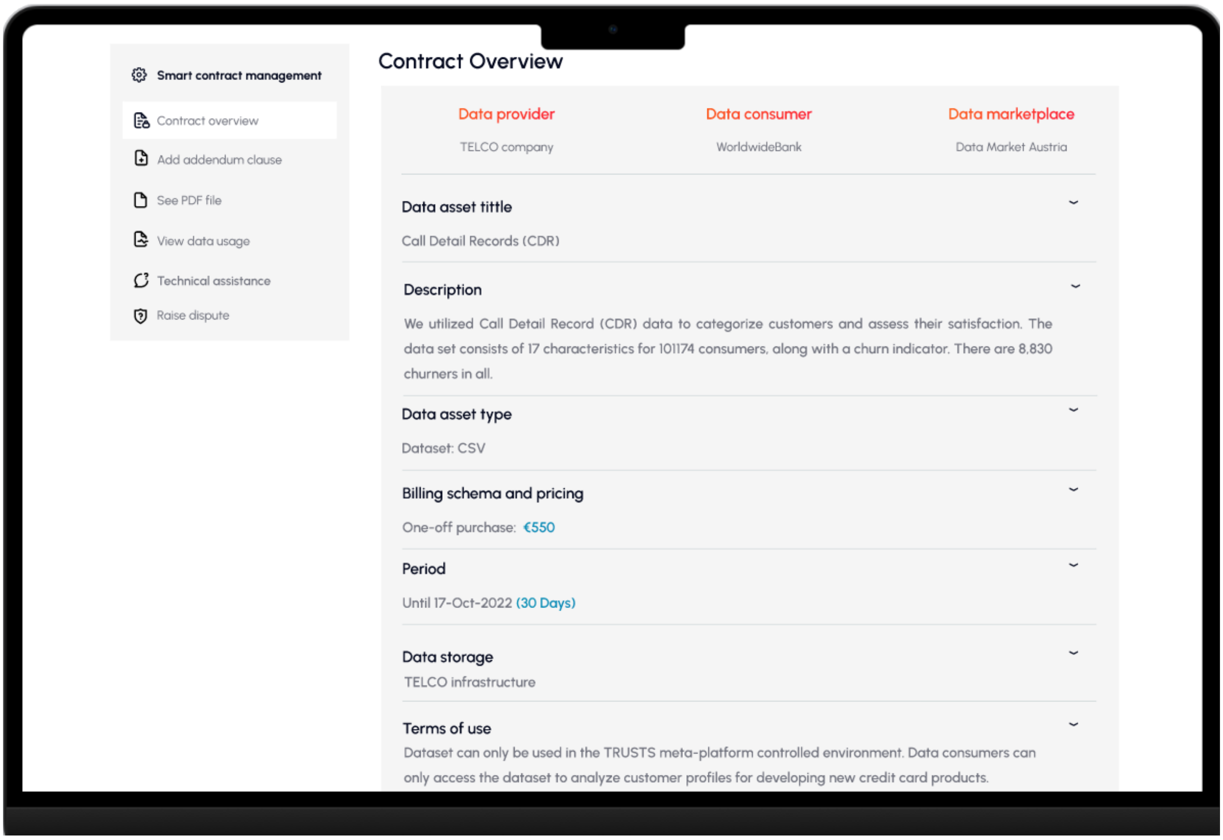
- TRUSTS meta-platform has **automatically** generated a data sharing agreement based on your 1) dataset information and 2) dataset use case
- TRUSTS meta-platform will be **responsible** for mediating the data provider and consumer when data may potentially be misused
- This agreement is **technically enforced** within a smart contract

What is a smart contract?

Smart contract is a **self-executing contract** with the terms of the contract between provider and consumer is **automatically written** into **transparent and immutable algorithms**.

Did you know?

Figure 7.10. I_3.2.1: View smart contract explanation



Contract Overview

Data provider	Data consumer	Data marketplace
TELCO company	WorldwideBank	Data Market Austria

Data asset tittle

Call Detail Records (CDR)

Description

We utilized Call Detail Record (CDR) data to categorize customers and assess their satisfaction. The data set consists of 17 characteristics for 101174 consumers, along with a churn indicator. There are 8,830 churners in all.

Data asset type

Dataset: CSV

Billing schema and pricing

One-off purchase: €550

Period

Until 17-Oct-2022 (30 Days)

Data storage

TELCO infrastructure

Terms of use

Dataset can only be used in the TRUSTS meta-platform controlled environment. Data consumers can only access the dataset to analyze customer profiles for developing new credit card products.

Figure 7.11. I_3.2.2: View contract

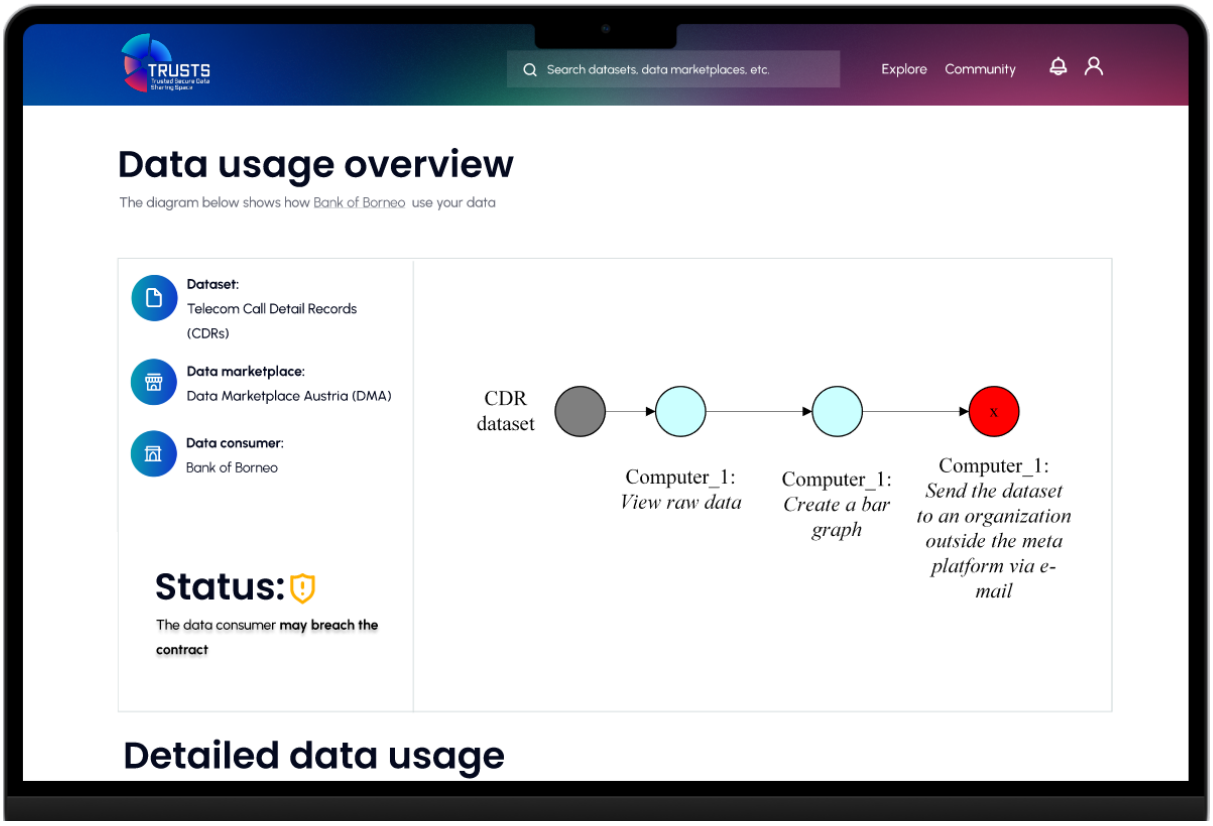
7.4.4 Task 4: Controlling how a data consumer uses the dataset

Task 4 aims to guide data providers through controlling how data consumers utilize their data. The primary focus is on ensuring data sovereignty by tracking data usage and identifying potential contract breaches (Subtasks 4.1 and 4.2), raising disputes (Subtask 4.3), and withdrawing dataset metadata (Subtask 4.4). Table 7.10 provides an overview of the description of Task 4.

Table 7.10. Task 4 description

ID	Interface	Description	
Introducing Task 4			
I_4	Task 4 introduction	I_4 explains Task 4.	
Subtask 4.1: Viewing the data usage overview from the WorldwideBank			
I_4.1.1	Select contract 1	I_4.1.1 provides an overview of data product contracts. Data providers select an ongoing contract with WorldwideBank with no indication of data misuse.	**Design principle:** • DP_DC_M_2: Data provenance
I_4.1.2	View data usage 1	I_4.1.2 shows how data consumers use the data. The interfaces show an "Okay" status, indicating that the data consumer likely complies with the agreed contract. The interface also shows the provenance graph and detailed data usage information (e.g., time, description, and workspace).	
Subtask 4.2: Viewing the data usage overview from the Bank of Borneo			
I_4.2.1	Select contract 2	I_4.2.1 provides an overview of data product contracts. The data provider will select an ongoing contract with the Bank of Borneo with a data misuse indication.	**Design principle:** • DP_DC_M_2: Data provenance
I_4.2.2	View Data usage 2	I_4.2.2 provides similar information with I_4.1.2. The main difference is that the interface indicates that the data consumer may breach the contract.	
Subtask 4.3: Raising a dispute because of a contract breach			
I_4.3.1	Raise dispute	I_4.3.1 asks data providers to raise a dispute by providing a reason and selecting an appropriate action, such as withdrawing the dataset. This interface also shows the contract ID, dataset information, the correspondence data marketplace, and data consumer.	**Design principle:** • DP_C_M_3: Integrated legally-valid contract management and dispute resolution

ID	Interface	Description	
I_4.3.2	Confirming dispute submission	I_4.3.2 informs data providers that the meta-platform operators will handle the dispute and that the data consumer currently has no access to the dataset.	
Subtask 4.4: Withdrawing dataset description (i.e., metadata) from Data Market Austria			
I_4.4.1	Withdraw metadata	I_4.4.1 withdraws metadata from Data Market Austria due to dispute processes.	**Design principle:** • DP_DC_M3: Data revocation
Task epilogue			
I_TE.1	Thank you notes	I_TE.1 provides further information for data providers to go back to the questionnaire page.	
I_TE.2	Acknowledgment and attribution	I_TE.2 presents information about acknowledgment and attribution related to the development of the prototype.	


TRUSTS
Trusted Secure Data Sharing Space
Search datasets, data marketplaces, etc.
Explore
Community

Data usage overview

The diagram below shows how Bank of Borneo use your data

Dataset: Telecom Call Detail Records (CDRs)

Data marketplace: Data Marketplace Austria (DMA)

Data consumer: Bank of Borneo

Status:

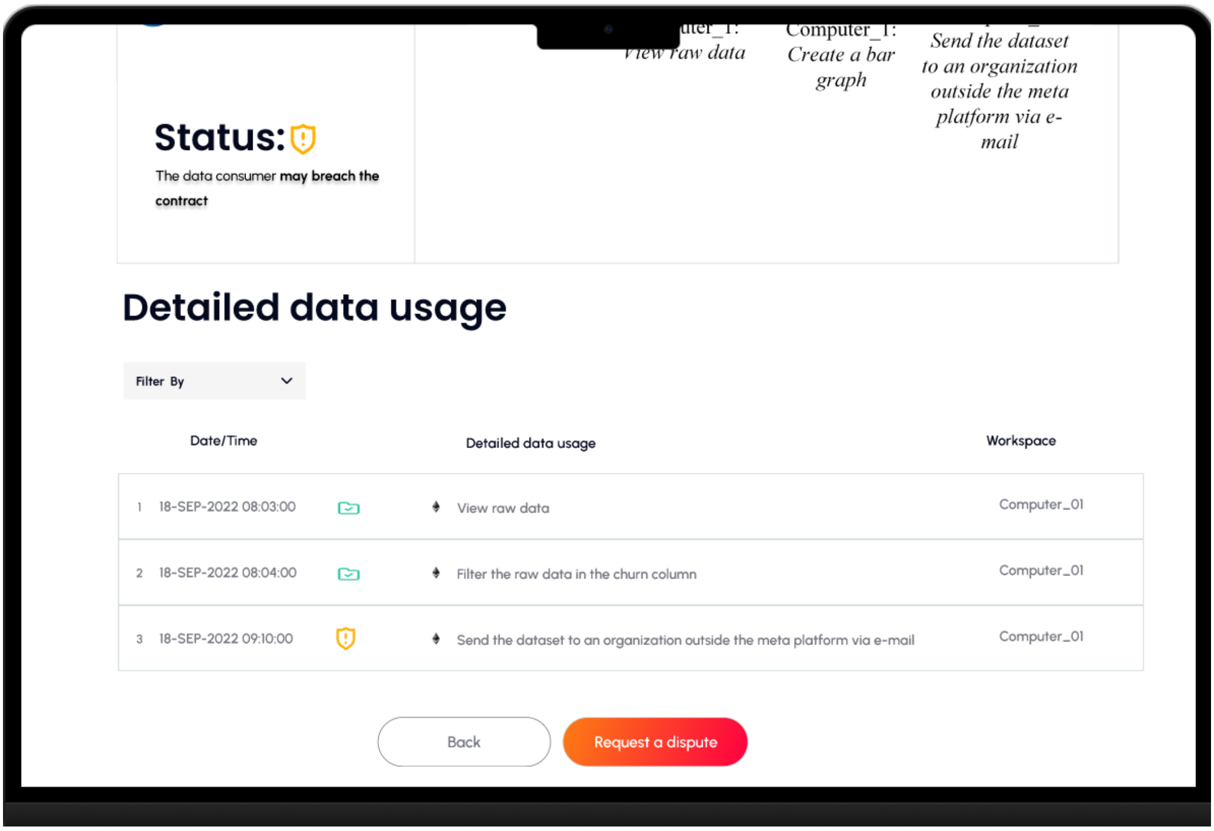
The data consumer may breach the contract

CDR dataset
Computer_1: View raw data
Computer_1: Create a bar graph
Computer_1: Send the dataset to an organization outside the meta platform via e-mail
x

Detailed data usage

Figure 7.12. I_4.2.2: View data usage 2

We provide examples of how data providers complete *Subtask 4.2: Viewing the data usage overview from the Bank of Borneo.* In the interface *I_4.1.1 Select contract 1*, data providers can select a contract with *the warning sign.* Data providers are redirected to *I_4.2.2* to check the details (Figure 7.12 and 7.13). *I_4.2.2* indicates that the data consumer may breach the contract, and the provenance graph shows precisely why and how it may happen (e.g., sending the dataset outside the organization without using the meta-platform infrastructure). Data providers can proceed to raise a dispute by clicking the appropriate button.



uter_1: View raw data

Computer_1: Create a bar graph

Send the dataset to an organization outside the meta platform via e-mail

Status:

The data consumer **may breach the contract**

Detailed data usage

	Date/Time		Detailed data usage	Workspace
1	18-SEP-2022 08:03:00		View raw data	Computer_01
2	18-SEP-2022 08:04:00		Filter the raw data in the churn column	Computer_01
3	18-SEP-2022 09:10:00		Send the dataset to an organization outside the meta platform via e-mail	Computer_01

Figure 7.13. I_4.2.2: View data usage 2

7.5 Conclusion of Chapter 7

This chapter addressed the fourth research question of this study: *What do the developed control mechanisms look like in the meta-platform setting*? To answer this question, we identified design principles (Section 7.3) and embedded them into relevant interfaces for each task (Section 7.4).

We identified design principles that retain data ownership of data providers through smart contracts, including a terms-of-use template with automated metadata generation, guided data ownership configuration, and customizable ownership settings. To enable data providers to maintain control over their shared data, smart contracts must enable contract enforcement, data provenance, and data revocation.

In terms of certifications, principles such as employing seals and compatibility with established standards can enhance the security of data providers when sharing their business data. In addition, certifications that include validity audits, explicit compliance statements, integrated legally-valid contract management and dispute resolution, as well as endorsement from authoritative bodies, can enhance data providers' adherence to legal and regulatory frameworks. Finally, certifications can foster clear responsibility division by incorporating explicit delineations and providing transparent certification body information.

We developed four business data sharing tasks to guide data providers in using our prototype and created relevant interfaces for each task, resulting in a total of 47 interfaces. Task

1 consists of simple subtasks designed to familiarize participants with the prototype. Task 2 involves describing the metadata for the shared dataset, while Task 3 focuses on creating and managing contracts. Lastly, Task 4 allowed participants to exercise the control capabilities of the meta-platform.

In the next chapter, we will utilize this prototype to evaluate the perceived efficacy of control mechanisms to enhance data sovereignty when conducting business data sharing via a meta-platform for data marketplaces. We will conduct a controlled experiment to conduct the evaluation.

PART 4: THE EVALUATION SPACE

Chapter 8: Evaluating the Perceived Efficacy of Control Mechanisms[1]

The previous chapter developed a prototype for a meta-platform for data marketplaces, incorporating the control mechanisms of smart contracts and certifications. We developed this prototype by incorporating the design principles derived from the control and signaling theories. The prototype consists of four business data sharing tasks and has 47 interfaces.

This chapter evaluates the perceived efficacy of control mechanisms to enhance data sovereignty in a meta-platform for data marketplaces. We address research question 5: *To what extent do data providers perceive that the control mechanisms (i.e., smart contracts and certifications) enhance data sovereignty for business data sharing through a meta-platform[2] for data marketplaces?* We ask this question to know whether our proposed mechanisms align with the expectations of data providers as the problem owners of sovereignty concerns. In addition, this question also allows us to reflect on the design knowledge formulated in the problem and solution spaces. We address this question by conducting a controlled experiment.

This chapter consists of five sections. Section 8.1 describes the evaluation design. Section 8.2 develops a data sovereignty measurement model. Section 8.3 assesses the perceived efficacy of control mechanisms for enhancing data sovereignty, while Section 8.4 discusses the findings. Finally, Section 8.5 concludes this chapter.

8.1 The evaluation design

This chapter evaluates the perceived efficacy of control mechanisms, namely smart contracts and certifications, to ensure sovereign data sharing via meta-platforms. We define *efficacy* as "the ability to produce a desired or intended result."[3] Although technical evaluation of data sovereignty (e.g., Firdausy et al., 2022), smart contracts (e.g., Hai & Liu, 2022), and certifications (e.g., Menz et al., 2019) exist, they may not fully capture the subjective experiences of data providers using these mechanisms. For instance, the control that smart contracts offer may not always match the perceived control experienced by data providers due to various factors, including the complexity of the smart contracts or the ability to interpret how smart contracts work. Thus, evaluating the perceived efficacy of control mechanisms is critical in understanding their impact on enhancing data sovereignty beyond the technical aspects.

In this chapter, the evaluation strategy focuses on the artificial setting for formative purposes. The setting is relevant because we want to check efficacy "...the artifact instantiation that causes an observed outcome and only the artifact" rather than effectiveness, "…the artifact instantiation works in a real situation" (Venable et al., 2016, p. 82). Formative purposes refer

[1] Parts of this chapter are based on the following publication:
Abbas, A. E., Agahari, W., Ofe, H., Zuiderwijk, A., & de Reuver, M. (2023). *Toward Sovereign Data Exchange Through a Meta-Platform for Data Marketplaces: A Preliminary Evaluation of the Perceived Efficacy of Control Mechanisms*. 36th Bled eConference – Digital Economy and Society: The Balancing Act for Digital Innovation in Times of Instability, Bled, Slovenia.

[2] For the remainder of this chapter, the term *meta-platform* always refers to meta-platforms in the data marketplace setting for business data sharing, unless stated otherwise.

[3] http://www.oxforddictionaries.com/definition/english/efficacy, accessed on 22 December 2023.

to evaluating and refining the prototype during its development, allowing for improvements and adjustments based on the observed outcomes.

The evaluation consists of two steps. In Step 1, we develop a data sovereignty measurement model. In Step 2, we assess the perceived efficacy of control mechanisms for enhancing data sovereignty. We describe each of these steps in the following subsections.

8.2 Step 1: Developing a data sovereignty measurement model

Because the measurement of data sovereignty does not yet exist, we developed the questionnaire questions (i.e., indicators) inspired by MacKenzie et al. (2011). This process entailed two phases: a) conceptualization and measurement development and b) indicator evaluation.

8.2.1 Conceptualization and measurement development

Based on our findings in Chapter 5, we conceptualize data sovereignty as a multi-faceted construct consisting of five facets: data ownership, data control, security, compliance, and responsibility. We consult the existing literature on data sharing to find (or derive) indicators for each facet of data sovereignty.

Data ownership is the exclusive right and authority to make decisions regarding data products (Hummel et al., 2021). Despite the ongoing debate on who should own data products (e.g., an individual, an organization, or a platform) (Lee et al., 2017), we focus here on the organization as a unit of analysis because end-users of a meta-platform are organizations, not individuals. We define four indicators for data ownership: (1) data providers should be able to express the term of use of data sharing, (2) be involved in determining (monetary) incentives (Dalmolen et al., 2020), (3) define the data types (Lee et al., 2017), and (4) decide which data marketplace receives the metadata description (Abbas et al., 2022).

Control over shared data refers to the ability of data providers to steer data sharing flows according to pre-defined agreements (Hummel et al., 2021). We define four indicators for data control. First, data providers can technically enforce terms of use of data sharing (Dalmolen et al., 2020). In doing so, data providers can track the data usage history (the second indicator). Third, data providers should be able to determine where they can store the shared (meta)data (Dalmolen et al., 2020). Finally, if something happens, data providers can withdraw their (meta)data (Lauf et al., 2022).

Building from the work of Hartono et al. (2014) and Hummel et al. (2021), we propose four indicators for *security*: (1) meta-platforms should prevent the disclosure of the shared data to unauthorized parties, (2) prevent the alteration of the shared data, (3) enable data providers to execute data sharing transactions without system failures, and (4) implement up-to-date security features.

Another critical data sovereignty facet relates to *compliance*. As data sharing is subject to specific regulations, data providers should (1) receive sufficient information to avoid violating laws and regulations, (2) obtain sufficient (technical) procedures to respond to those laws and regulations, and (3) utilize dispute mechanisms to handle conflicts (if any, with data consumers) (Hummel et al., 2021).

One distinguishing facet of data sovereignty due to the context novelty is the *responsibility* facet, primarily because of the complex constellations of data marketplaces via a meta-platform. As discussed in Chapter 5, it should be clear who is responsible for what to ensure sovereign data sharing. Hence, we propose the three indicators: meta-platforms should (1) responsibly select data marketplace participants that adhere to data sharing standards, (2) divide responsibilities between the meta-platform and the data marketplace participants, and (3) take responsibility if the sensitive data is misused or stolen. In summary, we use these five data sovereignty facets to evaluate the perceived efficacy of control mechanisms in meta-platforms.

We assessed the *content validity* of the measurement model as part of the prototype evaluation (cycle 2) elaborated in Chapter 7. The evaluation consisted of a workshop with six socio-technical researchers, each specializing in areas such as artificial intelligence and open data sharing. During the workshop, we presented research instruments for discussion (i.e., the video, prototype, and questionnaire). Participants reviewed and discussed indicators for each sovereignty facet in the questionnaire session, assessing the wording and categorization. While we received suggestions for minor wording improvements, such as reducing question length and correcting typos, there was no feedback on categorization, indicating overall content validity.

8.2.2 Indicator evaluation

This step assesses the validity and reliability of the data sovereignty measurement model. Given the five facets contributing to data sovereignty, we characterize our model as a Hierarchical Component Model (HCM). We employed a standard approach to validate the measurement of the HCM in SmartPLS 4: a joint two-stage approach (Ringle et al., 2012). In the first stage, we evaluated all indicators regarding indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. In the second stage, we formed a latent composite score of each facet and evaluated their convergent validity, collinearity issues, and relevance (Hair et al., 2021).

We conducted a survey study to assess the validity and reliability of the data sovereignty measurement model, recruiting 93 participants residing in Europe through the Prolific platform (47 female, 46 male). The sample size was determined using G*Power statistical calculations. Most participants were young to middle-aged adults (31-45 years old, 51%), followed by young adults (17-30 years old, 40%) and older adults (9%). Educational backgrounds were diverse, with 46% holding a Master's degree and 33% possessing a Bachelor's degree. The target participant profile included employees with management experience and leadership responsibilities. A significant proportion of participants (82%) had planned or conducted business-sensitive data sharing, and 75% self-reported being knowledgeable about data marketplaces.

The online survey via Qualtrics consisted of three elements: a video explanation, a prototype, and a questionnaire. As described in Chapter 7, the video explained a hypothetical scenario where participants play the role of a data provider, a telecommunication company called TELCO.[4] Data providers will share their business data about *call detail records* via a meta-platform. Next, participants engaged with the prototype by completing a series of pre-defined tasks.[5] Task 1 consisted of simple sub-tasks designed to familiarize participants with the prototype. Task 2 involved describing metadata associated with the platform, while Task 3 focused on creating and managing contracts. Lastly, Task 4 allowed participants to exercise the control capabilities of the meta-platform. After exercising the prototype, participants filled out a questionnaire. In addition to the previously elaborated indicators in Section 8.2.1, we employed global indicators such as (DS_G): "*I believe the meta-platform enables sovereignty for the sensitive data that I would share.*" These global indicators were utilized as an enabler to check the convergent validity of the data sovereignty facets (see Table 8.3 for the list of global indicators). Participants provided their responses on a 5-point Likert scale. Prior to participation, we obtained informed consent and maintained confidentiality throughout the research. The TU Delft ethical committee approved the study protocol, ensuring compliance with all ethical considerations.

The reliability of each indicator is confirmed, as the outer loading (λ) for all indicators is within the range of 0.6 and 0.9 (Hair et al., 2021). The internal consistency reliability for each facet is also established, as indicated by the composite reliability (rho_a) score for each greater than 0.7. Convergent validity is likewise confirmed, as the Average Variance Extracted (AVE) for all aspects surpasses 0.5. Consequently, we opted against removing any indicators. As for discriminant validity, the Heterotrait-monotrait ratio (HTMT) for all facets is below the recommended threshold of 0.9, except for Security (S) and Responsibility (R). Thus, we examine cross-loadings and remove one item (S_4), establishing discriminant validity. Our measurement model comprises five data sovereignty facets. Specifically, the facet of data ownership is represented through four indicators (DO_1, DO_2, DO_3, DO_4), data control through four indicators (DC_1, DC_2, DC_3, DC_4), compliance through four indicators (C_1, C_2, C_3, C_4), responsibility through three indicators (R_1, R_2, R_3), and finally, security through three indicators (S_1, S_2, S_3). We also confirm the validity of a generic data sovereignty construct measured by six global indicators.

Next, we calculated the Latent Variable (LV) score for each data sovereignty facet from the Hierarchical Component Model (HCM) of data sovereignty (Figure 8.1). The convergent validity is established as ($\beta = 0.713$, $p = 0.00$) and $R^2 > 0.5$, indicating that these facets well represent data sovereignty. The HCM exhibits no collinearity issue, as all facets have a Variance Inflation Factor (VIF) less than 5. Although Outer Weight (OW) testing shows significance only for the responsibility (OW = 0.38, $p = 0.01$) and security facets (OW = 0.38, $p = 0.00$), we retain the other facets since their outer loadings are greater than 0.5, as suggested by Hair et al. (2021). A detailed explanation of this step, including survey indicators and the complete analytical statistics, is available in Online Appendix 4.

[4] The video can be accessed here.

[5] The prototype can be accessed here.

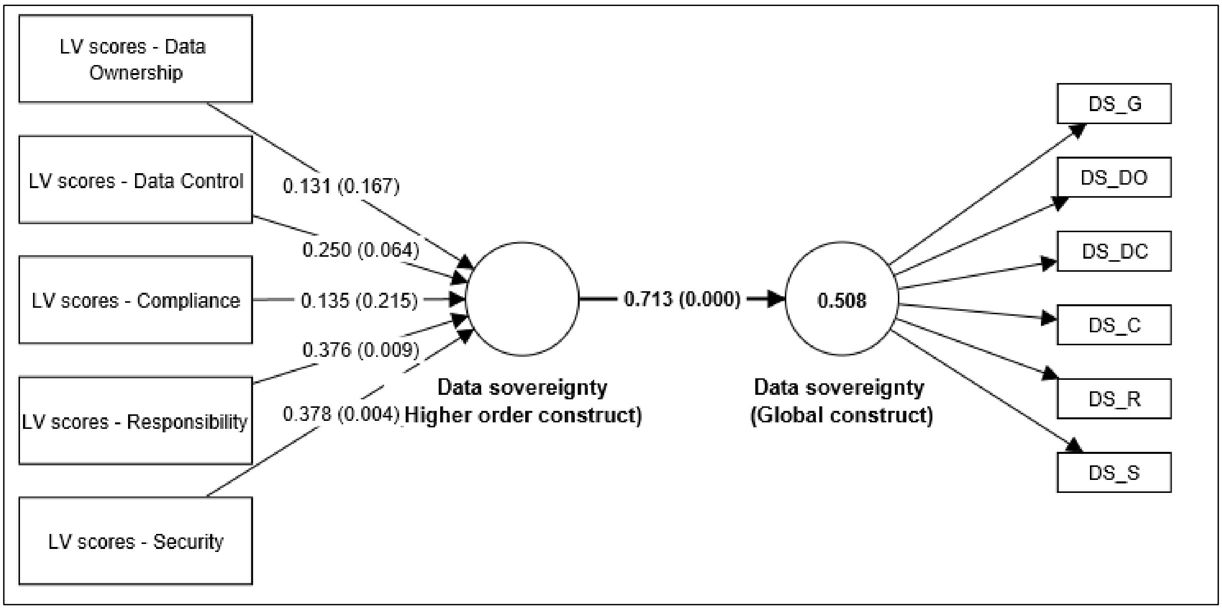


Figure 8.1. Hierarchical component model of data sovereignty

8.3 Step 2: Conducting a controlled experiment

Having developed the data sovereignty measurement model, Step 2 evaluates the perceived efficacy of control mechanisms (i.e., smart contracts and certifications) to enhance data sovereignty in meta-platforms. We conduct a between-subject 2x2 factorial experiment. The controlled experiment is an essential tool for evaluation in Design Science Research (DSR) and is often regarded as the *gold standard* for establishing causal relationships between constructs (Kampling et al., 2016; Lonati et al., 2018). In DSR, experiments can assess how specific design components contribute to fulfilling design requirements, thereby demonstrating the efficacy of the artifact (Mettler et al., 2014).

Mettler et al. (2014) outline three key principles of experiments in DSR: 1) control, 2) randomization, and 3) manipulation. Control includes using a group that serves as a benchmark for comparing the efficacy responses of one or more treatment groups. Randomization involves the unbiased allocation of participants to either control or treatment groups. Manipulation refers to the adjustment of artifacts under various conditions. Independent variables represent the components of the artifact that can be modified, while dependent variables reflect the changes observed in response to varying conditions. In experiments, researchers only change independent variables to observe their effects on dependent variables (Mettler et al., 2014).

We conduct an online rather than a lab experiment due to several key advantages. Online experiments offer increased efficiency, enhanced external validity, improved population validity, and heightened ecological validity (Fink, 2022). Online experiments provide greater efficiency because they reduce the need for physical lab space, advanced equipment, and research staff. Online experiments enhance external validity by allowing researchers to access more diverse and global participants. Population validity is similarly improved, as online experiments can involve larger sample sizes, which in turn strengthens statistical power and facilitates more effective use of between-subjects designs (Fink, 2022). Ecological validity is heightened in online experiments, as participants complete tasks in natural environments using their devices, closely resembling real-world situations. In conclusion, the benefits of efficiency, external validity, population validity, and ecological validity offered by online experiments make them a more suitable choice for our study.

8.3.1 Threat to validity

The validity of an online experiment can be compromised by various factors, such as construct, internal, external, and statistical validity (Field & Hole, 2002; Lonati et al., 2018). Table 8.1 outlines these potential threats and describes our measures to minimize these risks.

Table 8.1. Thread to validity and mitigation

Category	Threat	Description	Mitigation to strengthen the validity
Internal validity	Incorrect causal inference	Inadequate manipulation of dependent variables in experimental design, such as confounding factors that cause variations between the treatment and control groups beyond the intervention.	- Assigning participants randomly to the control and treatment groups. It ensures that any differences between the groups are due to the intervention rather than confounding factors. - Only manipulating the prototype based on the presence of control mechanisms to ensure that the differences observed are directly related to the intended intervention.
	Demand effects	Participants feel obligated to answer according to socially desired behaviors due to 1) hierarchical status, 2) social approval, 3) the presence of the researcher, and 4) exposing the experiment's goal.	- Employing an online experiment with self-paced testing, allowing participants to interact independently with the research instruments (Fink, 2022). - Ensuring the informed consent does not include information about dependent and independent variables.
	Lack of manipulation checks	No confirmation that independent variables were effectively manipulated as intended by researchers.	- Inquiring if participants were aware of the smart contract and certification features in the study after the main questions. This approach prevents the demand effect by spoiling the goal of the study for participants. - Employing a mediation model by incorporating trust and perceived risks (see Chapter 9). The mediation model, in a way, checks whether the manipulation affected participants as intended (e.g., their trust level goes up, and they feel less concerned about risks).
	Time threats	Participants took either too short or too long to complete the experiment.	- Carefully analyze the completion time in Qualtrics. If there is something suspicious, ask participants for their

Category	Threat	Description	Mitigation to strengthen the validity
			reasoning. Based on that, either reject or accept their participation in Prolific.
	Instrument changes	Changing the research instruments (i.e., video, prototype, questionnaire) that affect the result.	- No adjustments were made during the controlled experiment.
Statistical validity	Failed randomization / Group threats	Samples are not randomly distributed; hence, the effects are caused by sample characteristics instead of the treatment.	- Assigning participants to a group by utilizing Qualtrics' built-in randomization features, which help ensure random allocation of participants to different experimental conditions.
	Small sample size	The small sample size makes it sensitive to outliers and results in low statistical power.	- Using larger sample sizes, which are calculated based on G*Power.[6]
	Issues of non-compliance	Participants did not comply with research protocols or failed the manipulation checks.	- Signaling participants to follow the instructions seriously by asking content-related, attention, and manipulation check questions. - Replacing participants via Prolific if they did not follow protocols, such as failing attention checks or using incompatible devices.
External validity	Generalizability	The finding is only applicable in the online experiment setting.	- While not claiming to be representative, we aimed for diversity in the participant sample (see Table 8.5).
	Subject pool effects	Using students as a primary source of participants.	- Chose a sample based on the UK population instead of students
	Over-use of specific groups of people that are over-represented in research studies	Unbalanced sample characteristics.	- While not claiming to be representative, we aimed for diversity in the participant sample (see Table 8.5).

8.3.2 Experiment procedures

This section elaborates on the experiment procedures. First, we recap the following hypotheses discussed in Chapter 6:

> *H1: Smart contracts positively enhance the data sovereignty facets of ownership (H1.a) and control (H1.b)*

[6] https://www.psychologie.hhu.de/arbeitsgruppen/allgemeine-psychologie-und-arbeitspsychologie/gpower, accessed on 25 December 2023.

H2: Certifications positively enhance the data sovereignty facets of security (H2.a), compliance (H2.b), and responsibility (H2.c).

To test the hypotheses, we conducted a 2x2 factorial experiment, forming four scenarios based on the presence of control mechanisms (see Table 8.2).

Table 8.2. Four scenarios for the controlled experiment

	No certification	**Certification**
Traditional contract	Scenario I	Scenario II
Smart contract	Scenario III	Scenario IV

In the first scenario, neither smart contracts nor certifications are available to participants. The second scenario involves certifications paired with traditional contracts. The third scenario includes smart contracts without certifications. In the fourth scenario, participants experience the presence of both smart contracts and certifications.

The key distinction between the presence of smart contracts and traditional contracts is evident in Task 4. As described in Chapter 7, Task 4 allows participants to exercise the control capabilities of the meta-platform. Participants utilizing traditional contracts cannot access a data usage overview via data lineage. Additionally, data providers cannot view data usage logs and receive live status updates regarding potential data contract breaches by data consumers. In the case of disputes, data providers must submit their own proof of evidence, as the meta-platform does not automatically provide this information. We also adjusted the landing page, removing the info about control-shared data via blockchain. Finally, we removed smart contract explanations and buttons in the contract overview screens.

We manipulated the prototype to show the presence of certifications in three ways. First, we removed the certification logo from data marketplaces and the certification checkmark from data consumers. Second, we removed the certification filter that appears when data providers must choose data marketplaces to interact with. Lastly, we completely removed sections 02_View Certificate 1 and 02_View Certificate 2, which detail the certification procedures. Online Appendix 5 details the prototype manipulations.

8.3.3 Measurement model

We made slight wording adjustments to improve the measurement model of data sovereignty. Table 8.3 presents the final measurement model.

Table 8.3. The final measurement model

Construct	**Code**	**Indicator (Likert scale of 5)**	**Question adapted/ derived/ inspired from**
Data ownership	DO_1	I believe the meta-platform enables me to… …define appropriate terms of use for the sensitive data that I would share.	(Dalmolen et al., 2020; Lauf et al., 2022; Lee et al., 2017)
	DO_2	…define how much money I receive for the sensitive data that I would share.	

Construct	Code	Indicator (Likert scale of 5)	Question adapted/ derived/ inspired from
	DO_3	…define the expiration date for the sensitive data that I would share (if applicable).	
	DO_4	…decide about the type of sensitive data that I would share.	
	DO_5	…decide where the shared sensitive data can be stored (i.e., on the meta-platform, on my own infrastructure, or on the data consumer infrastructure).	
	DO_6	…decide which data marketplace receives the description of the sensitive data that I would share.	
Data control	DC_1	If I would share sensitive data, I believe the meta-platform… …offers me technical means to enforce data sharing contracts.	(Dalmolen et al., 2020; Lauf et al., 2022)
	DC_2	…enables me to monitor data usage based on the agreed data sharing contracts.	
	DC_3	…enables me to track down the history of data usage.	
	DC_4	…enables me to easily withdraw the description of sensitive data from the meta-platform after sharing it.	
Security	S_1	I believe the meta-platform… …prevents the disclosure of my sensitive data that I would share with unauthorized parties.	(Hartono et al., 2014)
	S_2	…prevents the alteration of my sensitive data that I would share by unauthorized parties.	
	S_3	…enables me to execute data-sharing transactions without system failures.	
Compliance	C_1	If I would share sensitive data, I believe the meta-platform… …provides me with sufficient information to avoid violating laws and regulations.	(Hummel et al., 2021; Kim, 2020; Lauf et al., 2022)
	C_2	…enables me to understand the content of laws and regulations.	
	C_3	…provides me with procedures to respond to laws and regulations.	
	C_4	…provides me with dispute mechanisms to handle potential conflicts with data consumers.	
	C_5	…provides me with legally valid data sharing contracts.	
Responsibility	R_1	I believe the meta-platform… …responsibly selects data marketplace participants that adhere to data exchange standards.	(Hochwarter et al., 2000; Segars & Grover, 1999)
	R_2	…clearly divides responsibilities between the meta-platform and the data marketplace participants.	
	R_3	…takes responsibility for organizing mediation processes between me and data consumers if the sensitive data that I would share is misused or stolen.	
Data sovereignty	DS_DO	I believe the meta-platform enables me to… …be the owner of the sensitive data that I would share.	Self-developed
	DS_DC	…control the sensitive data that I would share.	

Construct	Code	Indicator (Likert scale of 5)	Question adapted/ derived/ inspired from
(Global indicator)	DS_C	…comply with relevant laws and regulations for sharing sensitive data.	
	DS_R	…takes responsibility for supporting data providers.	
	DS_S	…enables me to securely share my sensitive data.	
	DS_G	…enables sovereignty for the sensitive data that I would share.	

We included manipulation check questions (see Table 8.4). A manipulation check involves asking participants questions about the manipulated variable to ensure they understand the manipulation as intended. Additionally, we added demographic questions (Hauser et al., 2018).

Table 8.4. The manipulation and demographic questions

Code	Indicator
SC	To what extent did you notice “smart contract” in the prototype?
C	To what extent did you notice “certification” in the prototype?
AGE	What is your gender?
GEN	What is your AGE (in YEARS)? E.g., 28
COUNTRY	List of Countries
EDU	What is the highest level of school you have completed or the highest degree you have received?
EMPLY	What best describes your employment status over the last three months?
IND	Which of the following industries best describes the sector you are or were primarily working in?
ROLE	Which of the following best describes your role at work?
OS	How many employees work in your organization?
FAM	In a real situation, how familiar is your organization with sharing sensitive data with other organizations (e.g., through inter-organizational information exchange, data marketplaces, etc.)?
EXP	In a real situation, does your organization have any experience in sharing sensitive data through data marketplaces?

8.3.4 Analysis method

We calculated the aggregate scores of each construct to conduct a two-way ANOVA. This statistical method examines the impact of two independent variables on a single continuous dependent variable and accounts for interaction effects (Field, 2013). A two-way ANOVA is relevant because it compares the effects of two distinct control mechanisms, smart contracts and certifications, on different elements of data sovereignty. Specifically, smart contracts influence control and ownership, while certifications affect security, compliance, and responsibility. Using ANOVA also reduces the risk of Type I errors (false positives) and addresses potential interaction effects, offering advantages over multiple independent t-tests.

8.3.5 Sample

We recruited 188 participants through Prolific, surpassing the recommended sample size of 128, as determined by G*Power calculations. This calculation assumed a default value of medium effect size (0.25) and a power of 0.8. Table 8.5 summarizes the demographic portrayal of our sample.

Table 8.5. The demographic portrayal of participants (n=188)

		Scenario				
		S1	**S2**	**S3**	**S4**	**All**
		%	**%**	**%**	**%**	**n**
Gender	Female	52.1%	44.7%	48.9%	56.4%	96
	Male	45.8%	55.3%	46.8%	43.6%	89
	Others	2.1%	0.0%	4.3%	0.0%	3
Education	Associate degree (2-year)	8.3%	2.6%	8.5%	7.3%	13
	Bachelor’s degree	35.4%	28.9%	34.0%	32.7%	62
	Doctoral degree (Ph.D.)	2.1%	2.6%	2.1%	5.5%	6
	High school graduate	25.0%	13.2%	2.1%	18.2%	28
	Less than high school	2.1%	0.0%	2.1%	0.0%	2
	Master’s degree	8.3%	26.3%	29.8%	20.0%	39
	Some college but no degree	18.8%	26.3%	21.3%	16.4%	38
Employment	A stay-at-home parent	10.4%	2.6%	2.1%	1.8%	8
	Retired	14.6%	13.2%	6.4%	14.5%	23
	Student	2.1%	10.5%	10.6%	9.1%	15
	Looking for work	6.3%	7.9%	4.3%	3.6%	10
	Working full-time	35.4%	36.8%	51.1%	45.5%	80
	Working part-time	25.0%	23.7%	19.1%	20.0%	41
	Other	6.3%	5.3%	6.4%	5.5%	11
Role	N/A	39.6%	39.5%	29.8%	34.5%	67
	Administrative Staff	10.4%	10.5%	8.5%	3.6%	15
	Consultant	8.3%	0.0%	0.0%	5.5%	7
	Junior Management	0.0%	0.0%	10.6%	3.6%	7
	Middle Management	10.4%	10.5%	12.8%	14.5%	23
	Researcher	0.0%	2.6%	0.0%	0.0%	1
	Self-employed/Partner	4.2%	5.3%	2.1%	9.1%	10
	Skilled Laborer	6.3%	7.9%	4.3%	1.8%	9
	Support Staff	4.2%	2.6%	10.6%	3.6%	10
	Trained Professional	14.6%	13.2%	14.9%	20.0%	30
	Upper Management	2.1%	7.9%	6.4%	3.6%	9
Organizational size	N/A	39.6%	39.5%	29.8%	34.5%	67
	1-9	12.5%	13.2%	12.8%	12.7%	24
	10-49	10.4%	7.9%	6.4%	10.9%	17
	50-249	10.4%	15.8%	14.9%	10.9%	24
	More than 250	27.1%	23.7%	36.2%	30.9%	56
Data sharing familiarity	Not at all familiar	50.0%	42.1%	29.8%	32.7%	72
	Not so familiar	10.4%	21.1%	17.0%	23.6%	34
	Somewhat familiar	22.9%	28.9%	34.0%	29.1%	54

		Scenario				
		S1	S2	S3	S4	All
		%	%	%	%	n
	Very familiar	16.7%	7.9%	19.1%	14.5%	28
Data marketplace experience	Never heard	52.1%	42.1%	48.9%	45.5%	89
	Know but never shared	39.6%	52.6%	46.8%	45.5%	86
	Shared multiple times	0.0%	2.6%	2.1%	5.5%	5
	Share once	8.3%	2.6%	2.1%	3.6%	8

Table 8.6 displays the results of Pearson Chi-Square tests, which evaluate the association between demographic variables and scenario groups. All p-values exceed 0.05, indicating no significant associations between these variables and the groups.

Table 8.6. Pearson Chi-Square tests

Demographic Variable	Pearson Chi-Square	df	p-values
Gender	6.299	9	0.710
Education	20.943	18	0.282
Employment	13.799	18	0.742
Role	33.507	30	0.301
Organizational Size	3.633	12	0.989
Data Sharing Familiarity	8.864	9	0.450
Data Marketplace Experience	6.923	9	0.645

8.3.6 Revalidating the measurement model

Following the same procedure as Step 1, we revalidated the measurement model due to minor changes in the questionnaire. This analysis led to the removal of DO_2 to ensure validity and reliability. Table 8.7 summarizes the final measurement model.

Table 8.7 The summary of the final measurement model

Data sovereignty facet	Indicator	Convergent validity		Internal consistency reliability			Discriminant validity
		Loading	AVE	Cronbach's Alpha	Reliability p_A	Composite reliability p_c	HTMT
		>0.7	>0.5	>0.6	>0.6	>0.6	Lower than 0.9?
Data Ownership	DO_1	0.723	0.523	0.776	0.776	0.845	Yes
	DO_3	0.748					
	DO_4	0.781					
	DO_5	0.669					
	DO_6	0.691					
Data Control	DC_1	0.797	0.594	0.774	0.774	0.854	Yes
	DC_2	0.774					
	DC_3	0.758					

Data sovereignty facet	Indicator	Convergent validity		Internal consistency reliability			Discriminant validity
		Loading	AVE	Cronbach's Alpha	Reliability p_A	Composite reliability p_c	HTMT
		>0.7	>0.5	>0.6	>0.6	>0.6	Lower than 0.9?
	DC_4	0.754					
Security	S_1	0.885	0.66	0.772	0.772	0.853	Yes
	S_2	0.764					
	S_3	0.784					
Compliance	C_1	0.752	0.604	0.803	0.803	0.863	Yes
	C_2	0.77					
	C_3	0.738					
	C_4	0.706					
	C_5	0.768					
Responsibility	R_1	0.841	0.68	0.764	0.764	0.864	Yes
	R_2	0.835					
	R_3	0.796					

8.3.7 Findings

Initially, we performed manipulation checks to verify the recognition of smart contracts and certifications by participants. As shown in Table 8.4, we asked each participant two seven-point Likert-type questions (i.e., To what extent did you notice [smart contracts, certifications] in the prototype?). We conducted an ANOVA test to assess whether participants identified the presence/absence of smart contracts and certifications. The mean difference between smart contracts (sc) and traditional contracts (tc) was statistically significant (Mean_$_{sc}$ = 5.68, Mean_$_{tc}$ = 2.91, F$_{1,184}$ = 350.02, $p < 0.01$); similarly, the mean difference between certification (c) and no certification (nc) was statistically significant (Mean_$_{c}$ = 5.26, Mean_$_{nc}$ = 2.70, F$_{1,184}$ = 309.61, $p < 0.01$). These findings suggest that our manipulation achieved its intended effect.

We checked some assumptions for conducting a two-way ANOVA. Our data is not normally distributed as the Shapiro–Wilk test value < 0.05. We also found a few extreme outliers in our data. However, a two-way ANOVA is robust against normality and outliers if sample sizes are nearly equal across groups and not too small (Field, 2013). The homogeneity of variance was established across all groups as indicated by Levene's test > 0.05. Therefore, we proceeded to do the analysis.

8.3.7.1 Smart contracts

In this section, we examined the effect of smart contracts on data ownership and control (H$_1$). We first investigated the effect of smart contracts on the sovereignty facet of ownership. The main effect analysis revealed no evidence of smart contracts positively influencing data ownership [F(1, 184) = 1.56, *p* = 0.21]. Similarly, there was no evidence of interaction effects between smart contracts and certifications on ownership [F(1, 184) = 0.04, *p* = 0.83] (see Table 8.8 for the detailed result).

Table 8.8. Two-way ANOVA analysis on data ownership

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	0.61	3	0.20	0.54	0.65
Intercept	3253.26	1	3253.26	8773.94	<0.01
Smart contract	0.58	1	0.578	1.56	0.21
Smart contract * Certification	0.02	1	0.02	0.04	0.83
Error	68.23	184	0.37		
Total	3373.40	188			
Corrected Total	68.83	187			

We examined the impact of smart contracts on the sovereignty facet of data control. The main effects analysis showed no evidence that smart contracts positively influence data control [F(1, 184) = 0.02, *p* = 0.90]. Furthermore, we found no evidence of the interaction effect between smart contracts and certifications to influence control over data [F(1, 184) = 2.14, *p* = 0.14] (refer to Table 8.9 for detailed results).

Table 8.9. Two-way ANOVA analysis on data control

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	1.80	3	0.60	1.36	0.25
Intercept	3045.57	1	3088.92	6997.54	<0.01
Smart contract	0.01	1	0.01	0.02	0.90
Smart contract * Certification	0.94	1	0.94	2.14	0.14
Error	81.22	184	0.44		
Total	3236.75	188			
Corrected Total	83.03	187			

8.3.7.2 Certifications

We assessed the perceived efficacy of certifications to the security, compliance, and responsibility facets of sovereignty. Considering security, we found no evidence to support the hypothesis that certifications positively affect security [F(1, 184) = 0.62, *p* = 0.43]. We also found no evidence for the interaction effect between certifications and smart contracts [F(1, 184) = 0.54, *p* = 0.46] (see Table 8.10).

Table 8.10. Two-way ANOVA analysis on security

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	1.44	3	0.48	0.79	0.50
Intercept	2476.68	1	2476.68	4081.31	<0.01
Certification	0.37	1	0.37	0.62	0.43

Smart contract * Certification	0.33	1	0.32	0.54	0.46
Error	111.66	184	0.61		
Total	2630.89	188			
Corrected Total	113.10	187			

Regarding compliance, our main effect analysis indicated that certifications have a positive effect [F(1, 184) = 4.06, *p* = 0.05]. This effect was evident when comparing scenarios with certifications, where the mean (Mean_c) is 4.20, against those without, with a mean (Mean_nc) of 4.02. We detected no interaction effect between certifications and smart contracts [F(1, 184) = 0.79, *p* = 0.37] (see Table 8.11).

Table 8.11. Two-way ANOVA analysis on compliance

Source	**Type III Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Corrected Model	2.07	3	0.69	1.83	0.14
Intercept	3123.38	1	3123.38	8284.96	<0.01
Certification	1.53	1	1.53	4.06	0.05
Smart contract * Certification	0.30	1	0.30	0.79	0.37
Error	69.37	184	0.38		
Total	3256.36	188			
Corrected Total	71.43	187			

Considering responsibility, certifications contributed to enhancing responsibility [F(1, 184) = 6.88, *p* = 0.01], with an interaction effect between smart contracts [F(1, 184) = 2.06, *p* = 0.04] (See Table 8.12).

Table 8.12. Two-way ANOVA analysis on responsibility

Source	**Type III Sum of Squares**	**Df**	**Mean Square**	**F**	**Sig.**
Corrected Model	6.18	3	2.06	4.18	0.01
Intercept	2732.95	1	2732.95	5540.47	<0.01
Certification	3.39	1	3.39	6.88	0.01
Smart contract * Certification	2.06	1	2.06	4.17	0.04
Error	90.76	184	0.49		
Total	2885.11	188			
Corrected Total	96.94	187			

Given the interaction effect between certifications and smart contracts in enhancing the sovereignty facet of responsibility, we further analyzed the estimated marginal means of responsibility (see Figure 8.2). Estimated marginal means, a statistical measure, provide the average prediction of responsibility scores while considering the influence of both certifications and smart contracts. The marginal means indicated a positive correlation between the presence of certifications and responsibility. Specifically, the responsibility score increased from 3.56 to 4.04 using smart contracts. In contrast, without smart contracts, certifications still enhanced the responsibility score, although to a lesser degree, rising from 3.86 to 3.92. This suggests that while certifications independently contribute to the responsibility facet, their perceived efficacy is enhanced when combined with smart contracts.

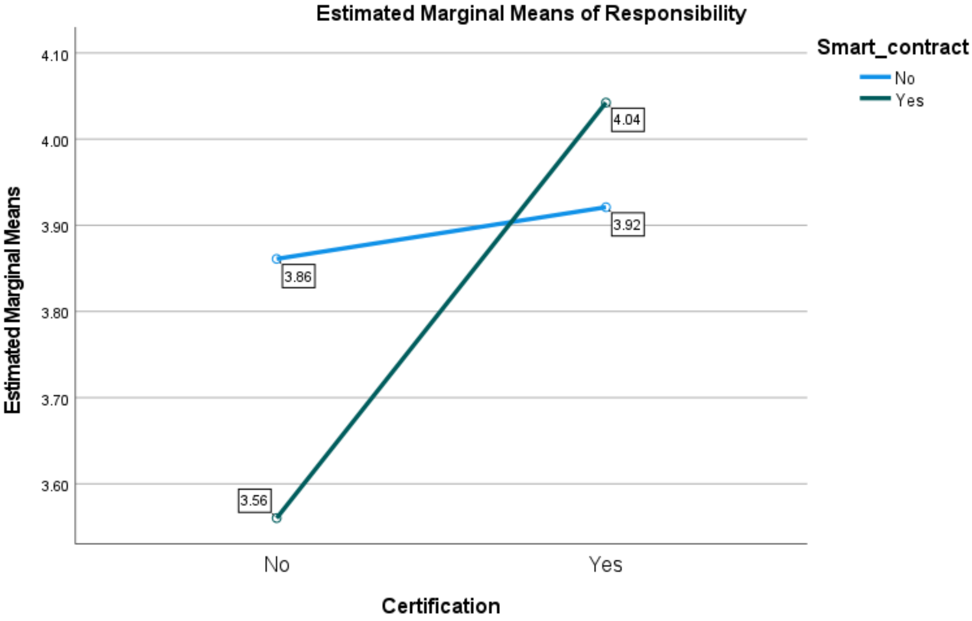


Figure 8.2. Estimated marginal means of responsibility

8.4 Discussion

The previous sections evaluated whether the proposed control mechanisms align with the expectations of data providers as problem owners to enhance data sovereignty. We discuss the key findings for each control mechanism as follows.

8.4.1 Smart contracts

One interesting finding from our study is that we find no evidence that smart contracts positively enhance the sovereignty facets of ownership and control. We did not ask open questions and thus had no direct evidence of why people perceived the experimental condition as they did. We explore potential explanations for these findings, including 1) legal uncertainty and 2) complexity and skepticism in implementing smart contracts in meta-platforms.

1) Legal uncertainties. One potential explanation for data providers perceiving smart contracts as lacking efficacy in retaining ownership rights may relate to the legal uncertainties associated with blockchain technology (Batubara et al., 2018; Fazi, 2022). Challenges in translating traditional contract terms into smart contract language often lead to ambiguities and misinterpretations, mainly when representing complex clauses like data access permissions. This difficulty, alongside the inherent limitations of smart contract languages in capturing legal nuances, could result in coding errors and contractual disputes during smart contract execution (Dixit et al., 2022). Additionally, a lack of contractual knowledge among parties may result in overlooking critical contract elements, necessitating costly legal consultations (Mezquita et al., 2019). Even with the development of model-based and low-code solutions to simplify smart contract creation, these approaches can still be complex for users and may not meet all legal requirements (Dixit et al., 2022). As a result, data providers could still perceive smart contracts as a less reliable means for retaining data ownership.

Due to legal uncertainties, data providers may prefer traditional contracts. Unlike smart contracts, traditional contracts are backed by well-established legal frameworks and enforcement mechanisms, offering data providers greater confidence in protecting their ownership rights. Additionally, data providers are often more familiar and comfortable with traditional contracts due to their long-standing history and widespread use across various sectors. In contrast, smart contracts, being a relatively recent innovation, are not as well understood by many stakeholders (Yang et al., 2020). Therefore, data providers may perceive traditional contracts as already sufficient for retaining data ownership.

Complexity and skepticism in implementing smart contracts in meta-platforms. Data providers may view the implementation of smart contracts in meta-platforms as overly complex. As discussed in Chapter 5, data providers must control data flow in two layers: the meta-platform and the data marketplace. While blockchain-based smart contracts offer data provenance (Moyano et al., 2021), their potential incompatibility when interacting with a meta-platform that federates many marketplaces causes complexity. Although interoperable means such as *side-chain* or *interchain* are essential due to the nature of meta-platforms that federate existing data marketplace, this initiative is generally in its infancy and practically hard to implement (Singh et al., 2020). This complexity might lead data providers to perceive smart contracts as lacking efficacy in meta-platforms. Furthermore, complexity might emerge from the tension over data ownership between data providers and data subjects (i.e., the identifiable individuals from whom the data is collected). The nature of call detail record data may signal to participants that the data ownership rests with the data subjects, not with the providers.

Widespread skepticism towards blockchain-based technologies, including smart contracts, may further compound this complexity. This skepticism is largely due to concerns over scalability, energy consumption, environmental issues, and security vulnerabilities (Batubara et al., 2019; Mnif et al., 2021). These concerns can lead to general mistrust or hesitation about the possible benefits of blockchain and its applications (Kamble et al., 2019). As smart contracts are built on the same underlying technology, data providers may be worried that these perceived limitations and risks could impact the reliability of smart contracts in managing data ownership and control. This explanation is in line with the signaling theory perspective. The signals' efficacy is influenced by the surrounding environment, including prevalent skepticism within or among organizations (Connelly et al., 2011). Environmental distortion happens when the medium transmitting a signal interferes with its clarity. For example, Carter (2006) finds that while press releases are intended as signals, their interpretation by media outlets can significantly alter the original message. The combined impact of implementation complexities and prevailing skepticism towards blockchain technology not only challenges the integration of smart contracts in meta-platforms but also raises questions about their overall effectiveness in enhancing the sovereignty facets of ownership and control.

8.4.2 Certifications

In this section, we discuss the impacts of certifications on the sovereignty facets of compliance, responsibility, and security.

Certification impacts on compliance. We found that certifications positively enhance the sovereignty facet of compliance. The impact of certifications on data providers' perceived compliance in engaging with business data sharing, which adheres to data sharing regulations, corresponds with the existing literature on certifications. For example, Wiengarten et al. (2017) report that organizations with environmental certifications, such as ISO 9001, show enhanced perceived compliance with relevant regulations. This is mainly due to earning certifications enhancing the organizational understanding of relevant regulations (e.g., Winter and May 2001). With increased understanding, organizations become aware of the consequences of non-compliance with regulations and can proactively mitigate these risks. For instance, understanding regulations about efficiently using natural resources in plant-based manufacturing leads organizations to lower energy and water use, and to reduce waste and emissions (Wiengarten et al., 2017). Such actions ensure that these organizations adhere to relevant regulations (Ansah et al., 2020; Melnyk et al., 2003), thereby increasing their perceived compliance.

From the perspective of signaling theory, our proposed design principles for certifications employ peripheral processing cues, which are design elements that affect data provider perception without requiring focused cognitive processing (cf. Lowry et al., 2012). By *showing certification validity* and *providing explicit compliance statements*, we signal expert authority. Such design principles demonstrate that meta-platform operators competently orchestrate data sharing in compliance with relevant regulations. This, in turn, leads to a heightened sense of compliance by data providers. Furthermore, we equip our certifications with endorsements from authoritative bodies. Such endorsements invoke the authority principle. It means that organizations are more inclined to adhere to the guidance, recommendations, or opinions of authoritative bodies (Lins & Sunyaev, 2022). Typically, authoritative endorsements are more effective than mere self-descriptions (Zhou et al., 2022). This principle may be relevant in data sharing contexts. When an authoritative body endorses certified operators, data providers feel more confident that they are following the relevant data sharing rules and regulations.

Certification impacts on responsibility

The positive role of certifications in clarifying responsibility aligns with the existing literature on certifications. For instance, Lansing et al. (2018) find how certifications clarify the responsibilities of cloud service providers. Defining and implementing clear responsibilities for these providers mitigates major cloud-related risks. This clarity allows cloud consumers to rely on cloud providers and concentrate on high-value business decisions. In our study, data providers may perceive certifications to clarify the responsibility division between meta-platforms and participating data marketplaces, enabling them to concentrate on delivering valuable data products. According to the signaling theory perspective, our design principle of *explicitly delineating responsibilities* and *revealing the certification body* serves as a means to showcase efforts to be responsible data sharing operators (cf. Lauf et al., 2022). These efforts signal the dedication of platform operators to responsible actions (cf. Lansing et al., 2018).

An interaction effect of certifications and smart contracts on responsibility. Another interesting finding is how certifications and smart contracts interact to enhance the responsibility facet of data sovereignty but not on the other four facets of data sovereignty. This suggests that certifications independently enhance this facet, but their perceived efficacy is amplified when integrated with smart contracts. Two potential explanations are as follows.

First, certification authenticity is often questionable due to potential manipulation. This may cause data providers to question whether a meta-platform really ensures participating data marketplaces comply with relevant data sharing standards. However, integrating certifications with blockchain-enabled smart contracts could mitigate this concern. Smart contracts execute transactions exclusively with certified parties identifiable in blockchain-based networks (Malsa et al., 2021; Sultana et al., 2023). Therefore, this combination increases data providers' confidence in the meta-platforms' ability to federate data marketplaces that strictly adhere to data sharing standards.

Second, although certifications hold meta-platforms accountable for mediating disputes between data providers and consumers in cases of data misuse, smart contracts can further strengthen this mediation process. When detecting data misuse or responsibility breaches, these smart contracts can trigger specific actions, including alerting meta-platform operators, initiating dispute resolution processes, or enforcing penalties and corrective measures (e.g., Firdausy et al., 2022). Together, certifications and smart contracts ensure the responsibility of meta-platforms to mediate disputes.

Certification impact on security. Our study found no evidence that certification enhances the security facet of sovereignty. One potential explanation for this absence relates to the *temporal limitations* of certifications. Organizations often receive certification based on criteria assessed at a specific time, confirming adherence to certain requirements at the moment of evaluation. Therefore, certifications often work well in the compliance and responsibility facets, where these facets undergo periodic updates and assessments. However, security threats pose a unique characteristic due to their constant real-time evolution. For instance, consider the rapid proliferation of new malware variants and hacking techniques in the cyber landscape. Even with substantial financial investment in obtaining and maintaining security certifications (Mavlanova et al., 2016), certification acquirers may observe that certification bodies struggle to keep up with the rapid pace of cyber security landscapes. Consequently, they may see that certification bodies lag in adapting to new security challenges (Lins & Sunyaev, 2022).

Another reason for this finding may relate to *signal observability*, which measures the ease with which signal receivers can recognize signals (Connelly et al., 2011). One way to improve signal observability is to increase signal *frequency,* as it improves the probability of correct interpretation (Filatotchev & Bishop, 2002). However, we might provide limited information about the International Data Space (IDS) certification in our study. IDS certification is newly developed for data sharing. We only created a single interface explaining the IDS certification. This may not sufficiently detail the security measures the IDS certification encompasses. As a result, data providers may have experienced a lack of detail and clarity regarding the specific security aspects addressed by the certification, its schema, and the various protection mechanisms it employs. For instance, although the IDS certification aligns with ISO/IEC 27001 (international standard for information security management) and IEC 62443 (cybersecurity for operational technology in automation and control systems), data providers may not fully recognize the signals we send.

8.5 Conclusion of Chapter 8

This chapter addressed the fifth research question of the study: *To what extent do data providers perceive that the control mechanisms (i.e., smart contracts and certifications) enhance data sovereignty for business data sharing through a meta-platform for data marketplaces?* We addressed this question to know whether our proposed mechanisms align with the expectations of data providers as the problem owners of sovereignty concerns.

We proposed two hypotheses to assess the perceived efficacy of smart contracts and certifications on the data sovereignty facets. We posited that smart contracts positively enhance the data sovereignty facets of ownership and control, but we found no supporting evidence. We also posited that certifications positively enhance the data sovereignty facets of security, compliance, and responsibility. We found no evidence that certifications positively enhance the sovereignty facet of security. However, we do find evidence that certifications enhance the sovereignty facet of compliance and responsibility. In examining the responsibility facet, we observed an interaction effect with smart contracts. This indicates that certifications independently enhance the responsibility facet, and their efficacy is further amplified when integrated with smart contracts.

The next chapter will evaluate the impacts of data sovereignty on the broader data economy. We will utilize the measurement model and survey data we gathered in this chapter to do so.

Chapter 9: Evaluating Data Sovereignty Impacts

The previous chapter evaluated the perceived efficacy of control mechanisms, specifically smart contracts and certifications, to enhance data sovereignty in meta-platforms[1]. We found no supporting evidence that smart contracts positively enhance the data sovereignty facets of ownership and control. We also found no evidence that certifications positively enhance the data sovereignty facets of security. However, we did discover evidence that certifications enhance the sovereignty facets of compliance and responsibility. In examining the responsibility facet, we observed an interaction effect with smart contracts. This indicates that certifications independently strengthen data sovereignty in the responsibility facet, but their integration with smart contracts amplifies this effect.

This chapter evaluates the impacts of data sovereignty on the broader societal context of the data economy. We address research question 6 of this study: *How does data sovereignty impact the data economy?* Addressing this research question helps to clarify and explain the assumed necessity of data sovereignty for the data economy's growth (scientific gap 4). To answer this question, we employ Partial Least Squares Structural Equation Modelling (PLS-SEM).

This chapter consists of four sections. Section 9.1 discusses the theoretical framework. Section 9.2 elaborates on the research approach. Section 9.3 presents the findings, and Section 9.4 concludes this chapter.

9.1 Theoretical framework

We develop our hypotheses by selecting key factors frequently discussed in data sharing literature for the data economy (see Chapter 3, Section 3.5.5). We focus on factors most likely to be influenced by data sovereignty. These factors include trust (Lauf et al., 2022; Rantanen & Koskinen, 2020a; Richter & Slowinski, 2019), perceived risk (Mariani et al., 2021; Sestino et al., 2023), and willingness to share data (Agahari & de Reuver, 2022; Cichy et al., 2021). Although other factors exist (e.g., data sharing benefits), they lack direct relevance to data sovereignty. Hence, our study excludes them despite prior research recognizing their significance in data economy research (e.g., Fassnacht et al., 2023; Heinz et al., 2022).

Since the relevant factors potentially impacted by data sovereignty include trust, perceived risk, and willingness to share data, we draw from theories on trust and risk to create a nomological network of data sovereignty impacts. Existing theories outline three general mediation models to describe the relationships among trust, risk, and behavioral intentions (Kim & Koo, 2016; Zhai et al., 2022): a) trust influences risk, which then affects behavioral intentions, b) risk influences trust, subsequently impacting behavioral intentions, or c) a bidirectional relationship exists between risk and trust. We develop our hypothesis by considering these mediation models.

[1] For the remainder of this chapter, the term *meta-platform* always refers to meta-platforms in the data marketplace setting for business data sharing, unless stated otherwise.

First, we consider the impact of data sovereignty on trust. Since we take the perspective of data providers as the owners of the data sovereignty problem in this study, we divide trust into two dimensions: trust in (meta-) platform operators and trust in data consumers (cf. Agahari & de Reuver, 2022).

Although research directly connecting data sovereignty with trust is scarce, a few studies have begun to argue about this link. For example, Hellmeier and von Scherenberg (2023) argue that integrating data sovereignty principles in data platform infrastructure strengthens stakeholder trust. This effect originates from the role of data sovereignty in guaranteeing transparent data processing through verifiable records, often complemented by user-friendly, graphical interfaces. Such principles reduce information asymmetries about data usage, fostering trust (Scheider, Lauf, Möller, et al., 2023). Another reason sovereignty increases the trust of data providers is by aiding in the precise definition of use cases, which specify what will and will not happen to data. The precise use case definition increases data provider trust, ensuring data usage follows agreed-upon parameters (Hutterer, 2023). Based on the above explanations, we hypothesize:

> *H1.a: Data sovereignty positively influences data providers' trust in (meta-) platform operators in business data sharing via meta-platforms*

> *H1.b: Data sovereignty positively influences data providers' trust in data consumers in business data sharing via meta-platforms*

Second, we consider how trust influences willingness to share data. In data sharing literature, particularly in hierarchical-based data sharing where businesses are familiar with each other (e.g., in supply chain networks), trust directly influences willingness to share data (Asare et al., 2016; Pavlou & Gefen, 2004). Among various reasons, trust reduces transaction costs, for example, by lessening redundant tests during quality inspections of incoming and outgoing goods (Eurich et al., 2010). Moreover, trust is instrumental in discouraging opportunistic behavior, as it fosters a culture of mutual respect and reliability, thereby reducing the likelihood of parties engaging in self-serving actions at the expense of others (Hart & Saunders, 1997). Therefore, we hypothesize:

> *H2.a: Data providers' trust in (meta-)platform operators positively influences their willingness to share data in business data sharing via meta-platforms*

> *H2.b: Data providers' trust in data consumers positively influences their willingness to share data in business data sharing via meta-platforms*

Third, we consider how data sovereignty influences perceived risks. While direct research linking data sovereignty with perceived risks is limited, some studies have begun to discuss this relationship implicitly. For instance, Opriel et al. (2021) suggest that data sovereignty can diminish risks associated with data breaches, such as through policies on data deletion. In the case of personal data, sovereignty provides anonymization and access control. These capabilities empower individuals to disclose identity information selectively, reducing their perceived risk related to data sharing (Sánchez-Guerrero et al., 2017). Consequently, we hypothesize:

> *H3: Data sovereignty reduces perceived risks of data providers in conducting business data sharing via meta-platforms.*

When data providers perceive data sharing as risky, potentially leading to harm such as loss of competitive advantage or reputational damage, they are likely to refrain from such activities (Dahlberg & Nokkala, 2019; Eurich et al., 2010; Spiekermann, 2019). Hence, we suggest the following hypothesis:

> *H4: Perceived risks reduce the willingness of data providers to share data when in meta-platforms*

Finally, examine how data sovereignty directly influences the willingness to share data. Research indicates that the absence of sovereignty is the primary reason for not considering business data sharing (Hellmeier & von Scherenberg, 2023; Jarke et al., 2019). Consequently, data providers may view data sovereignty as an essential prerequisite for conducting business data sharing. Based on this understanding, we formulate the following hypothesis:

> *H5: Data sovereignty positively influences data providers' willingness to share business data via meta-platforms.*

9.2 Research approach: Structural equation modeling

We employ Structural Equation Modeling (SEM) to evaluate our hypotheses. SEM allows for multivariate analysis, giving researchers the ability to investigate complex relationships among multiple dependent and independent variables simultaneously. Two approaches to SEM exist (Hair et al., 2021): Partial Least Squares Structural Equation Modeling (PLS-SEM) and Covariance-Based Structural Equation Modelling (CB-SEM). This research employs PLS-SEM for several reasons: (a) it suits testing theoretical frameworks focused on prediction; (b) it handles complex structural models with numerous constructs, indicators, and relationships; and (c) it aids in exploring and developing theory. In contrast, CB-SEM is more appropriate for theory testing within well-defined theoretical models, emphasizing model fit and substantial data needs (Hair et al., 2021).

We analyzed the data collected while examining how control mechanisms in meta-platforms enhance data sovereignty (see Chapter 8). This approach is appropriate as it involves data collected from the same participants under consistent conditions, allowing for precise assessment of construct relationships. Consequently, this use of experimental data increases the internal validity of our findings. To recap, we conducted an online survey using Qualtrics (see Chapter 8 for detailed elaboration). The survey comprised a video, a prototype, and a questionnaire. The video explained a hypothetical scenario where participants play the role of a data provider. Data providers will share their business data about call detail records via a meta-platform. Participants then interacted with the prototype by performing specific tasks, followed by completing a questionnaire.

We followed the standard approach to assess a structural model in PLS-SEM by assessing 1) collinearity issues, 2) the significance of construct relationships, 3) the model's explanatory power, and 4) the model's predictive power. Section 9.2.4 details each assessment.

9.2.1 Indicators

Besides data sovereignty indicators, the survey incorporated measures for four constructs to assess the broader impacts of data sovereignty on the data economy. These constructs are Trust in Operator (TO), Trust in Data Consumer (TDC), Perceived Risk (PR), and Willingness to Share Data (WTSD).

We measure trust by adapting indicators from two sources (Agahari & de Reuver, 2022; Venkatesh et al., 2011). We modified existing indicators to measure perceived risks in business data sharing (Agahari & de Reuver, 2022; Rosillo-Díaz et al., 2019). Finally, we adapted indicators from Pavlou (2003) to measure willingness to share data. Table 9.1 provides an overview of the indicators.

Table 9.1. Constructs and their indicators for assessing data sovereignty impacts

Construct	Code	Indicator (Likert scale of 5)	Adapted from
Trust in Operator (TO)	TO_1	I expect that the meta-platform operator… …provides services to facilitate sharing sensitive data in my best interest.	(Agahari & de Reuver, 2022; Venkatesh et al., 2011).
	TO_2	…provides access to genuine services for sharing sensitive data.	
	TO_3	…will be trustworthy in handling the description of sensitive data provided by me.	
Trust in Data Consumer (TDC)	TDC_1	I expect that data consumers will… …fulfill data sharing agreements to use the sensitive data that they obtain through the meta-platform.	(Agahari & de Reuver, 2022; Venkatesh et al., 2011).
	TDC_2	…be honest when handling the sensitive data that they obtain through the meta-platform.	
	TDC_3	…be trustworthy in handling the sensitive data that they obtain through the meta-platform.	
Perceived Risk (PR)	PR_1*	I feel that sharing sensitive data through the meta-platform is risky.	(Agahari & de Reuver, 2022; Rosillo-Díaz et al., 2019)
	PR_2*	There will be uncertainty associated with sharing sensitive data through this meta-platform.	
	PR_3*	I feel that sharing sensitive data through the meta-platform will negatively affect me.	
Willingness to Share Data (WTSD)	WTSD_1	I intend to share sensitive data through this meta-platform.	Pavlou (2003)
	WTSD_2	I predict that I will share sensitive data through this meta-platform in the future.	
	WTSD_3	It is likely that I will share sensitive data through this meta-platform in the near future.	

**Reversed indicator*

9.2.2 Sample

We used the same survey data for our experiment described in Chapter 9. To recap, respondents, all residing in the United Kingdom, were recruited through the Prolific platform. They received a small financial incentive of £4.5 for completing the 30-minute survey. The survey was sent out in February 2023, leading to 188 complete responses. The survey participants are almost evenly distributed between females and males. A significant majority, 84%, hold higher education degrees. Additionally, 77% of participants have work experience, with 66% being familiar with business data sharing. Half of the participants know data marketplaces.

9.2.3 Validity and reliability of the measurement model

Following the same procedure as in Chapter 8, we checked the measurement model for four additional constructs to assess data sovereignty impact: Trust in Operator (TO), Trust in Data Consumer (TDC), Perceived Risk (PR), and Willingness to Share Data (WTSD). Table 9.2 summarizes the measurement model for these constructs, showing the overall validity and reliability.

Table 9.2 The measurement model

Construct	**Indicators**	**Convergent validity**		**Internal consistency reliability**			**Discriminant validity**
		Loadings	**AVE**	**Cronbach's Alpha**	**Reliability p_A**	**Composite reliability p_c**	**HTMT**
		>0.7	**>0.5**	**>0.6**	**>0.6**	**>0.6**	**Lower than 0.9?**
Trust in Operator (TO)	TO_1	0.86	0.713	0.798	0.813	0.881	Yes
	TO_2	0.779					
	TO_3	0.89					
Trust in Data Consumer (TDC)	TDC_1	0.873	0.838	0.903	0.903	0.939	Yes
	TDC_2	0.94					
	TDC_3	0.932					
Perceived Risk (PR)	PR_1*	0.912	0.778	0.856	0.862	0.913	Yes
	PR_2*	0.899					
	PR_3*	0.832					
Willingness to Share Data (WTSD)	WTSD_1	0.955	0.923	0.958	0.961	0.973	Yes
	WTSD_2	0.961					
	WTSD_3	0.966					

9.2.4 Structural model

Figure 9.1 represents the model of data sovereignty impacts on the data economy in a nomological network. The arrow between the construct represents path coefficients and p-value, while the number in the construct represents R^2. The following sections detail the assessment structural model for data sovereignty.

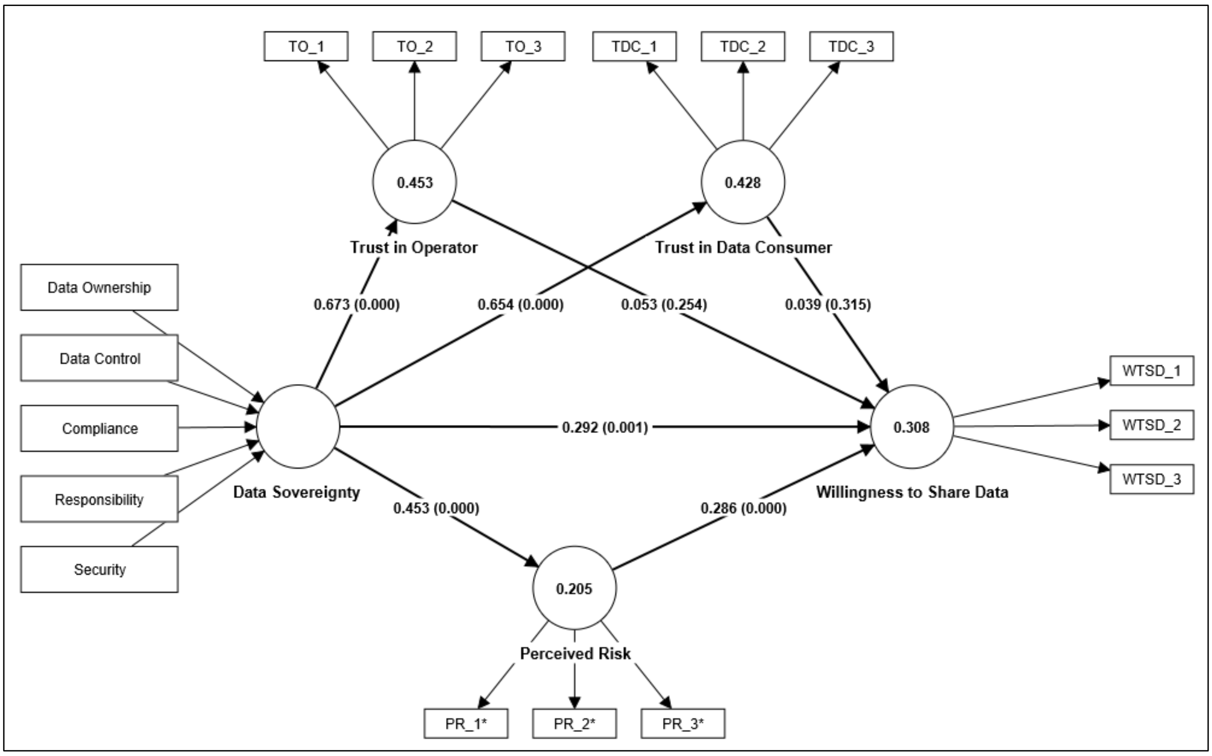


Figure 9.1. The nomological net of data sovereignty

9.2.4.1 Assessing collinearity issues

Collinearity issues emerge when multiple independent variables have strong correlations (Field, 2013). Assessing these issues is critical as calculating path coefficients in a structural model relies on ordinary least squares regressions for each independent variable on its dependent variable. Hence, path coefficients risk bias if independent variables demonstrate collinearity issues. A Variance Inflation Factor (VIF) exceeding five indicates a collinearity issue (Hair et al., 2021). After assessing the VIF score, our structural model has no collinearity issue, as all variables have a VIF score below five.

9.2.4.2 Assessing the significance of construct relationships

We assessed the significance of construct relationships in our model using the path coefficient values. Their values span from -1 to +1. Values close to +1 represent strong positive relationships, while those approaching -1 reflect strong negative relationships. In contrast, values around 0 imply weaker relationships (Hair et al., 2021).

Table 9.3 presents the significance assessment result of construct relationships in our model. Our findings reveal that data sovereignty positively affects trust in meta-platform operators (DS → TO; β = 0.673, p = 0.000) and data consumers (DS → TDC; β = 0.654, p = 0.000) when using meta-platforms for business data sharing. Additionally, data sovereignty reduces the perceived risks associated with business data sharing (DS → PR; β = 0.453, p < 0.000), which, in turn, positively influences the willingness of data providers to share data via meta-platforms (PR → WTSD; β = 0.286, p = 0.000). We also find that data sovereignty has a direct influence on the willingness of data providers to share data via meta-platforms (DS → WTSD; β = 0.292, p = 0.001). However, we find no evidence that trust in meta-platform operators (TO → WTSD; $\beta = 0.053$, $p = 0.254$) and data consumers (TDC → WTSD; $\beta = 0.039$, $p = 0.315$) affect willingness to share data. Therefore, we find evidence to support all our hypotheses except for *H2.a* and *H2.b*.

Table 9.3. The significance assessment result of construct relationships

Relationship	**Path Coefficients *(β)***	***t* Values**	***p* Values**	**95% Confidence Intervals**	**Significance (p < 0.05)?**
DS → PR	0.453	6.856	0.000	[0.348, 0.565]	Yes
DS → TDC	0.654	14.623	0.000	[0.58, 0.727]	Yes
DS → TO	0.673	15.423	0.000	[0.607, 0.749]	Yes
DS → WTSD	0.292	3.228	0.001	[0.143, 0.445]	Yes
PR → WTSD	0.286	3.858	0.000	[0.159, 0.404]	Yes
TDC → WTSD	0.039	0.482	0.315	[-0.094, 0.169]	No
TO → WTSD	0.053	0.661	0.254	[-0.081, 0.184]	No

9.2.4.3 Assessing the model's explanatory power

We evaluated the model explanatory power using the R^2 value. The R^2 value reflects the percentage of variance in the dependent variables accounted for by the independent variables in the model. The R^2 values for each construct are as follows: 0.458 for trust in meta-platform operators, 0.428 for trust in data consumers, 0.205 for perceived risks, and 0.308 for willingness to share data.

According to Hair et al. (2021), the R^2 value can be classified as weak (0.25 or less), moderate (between 0.25 and 0.5), and substantial (greater than 0.5). In this study, the R^2 value for trust in operators, trust in data consumers, and willingness to share data fall within the moderate range, while perceived risk has weak explanatory power. Nevertheless, it is essential to recognize that the primary purpose of the nomological network is not to create a comprehensive model of willingness to share data but to assess the contribution of data sovereignty to this willingness. Indeed, the results confirm that data sovereignty positively contributes to willingness to share data, highlighting the importance of data sovereignty as a critical factor in the growth of the data economy.

We also checked the f^2 value of data sovereignty to all dependent variables: trust in operators = 0.827, trust in data consumers = 0.747, perceived risks = 0.258, and willingness to share data = 0.053. These f^2 values represent the effect sizes of data sovereignty on each dependent variable. Effect sizes are categorized as small (0.02), medium (0.15), or large (0.35) (Cohen, 2013). In this study, data sovereignty moderately influences perceived risks in business data exchange while substantially impacting trust in data consumers and meta-platform operators. Despite its small effect, data sovereignty remains crucial in unraveling the complex factors determining data providers' willingness to share data.

9.2.4.4 Assessing the model's predictive power

Finally, we evaluated the model's predictive power, which determines if our findings apply to the data used in model estimation and other uninvolved datasets. The primary approach to assessing predictive power is $PLS_{predict}$. This analysis involves dividing the data set into training and holdout samples. The training sample estimates model parameters such as path coefficients, indicator weights, and loadings. In contrast, the holdout sample comprises data excluded from the model estimation process. Specifically, we used the Q^2 statistic to evaluate the predictive power in $PLS_{predict}$.

The Q^2 values for the indicators of the target construct (i.e., willingness to share data) are greater than 0 (i.e., 0.212). This result suggests that the model accurately predicts the contributing factors for willingness to share data.

9.3 Discussion

Our findings indicate that data sovereignty enhances trust in (meta-)platform operators and data consumers. This aligns with existing literature on data sharing, which identifies trust as an outcome of data sovereignty (e.g., Brechtel, 2023; Lauf et al., 2022). Primarily, this is because data sovereignty fosters transparency, a crucial factor in building trust (Lauf et al., 2022). We also find that data sovereignty reduces perceived risks, reaffirming assertions in data sharing literature that link data sovereignty to risk reduction (e.g., Walter et al., 2021). This is due to, for instance, enhancing data sovereignty through data control capabilities can prevent knowledge spillovers to competitors (Koutroumpis et al., 2020). Additionally, data sovereignty safeguards providers from losses due to free riders accessing datasets without adequate compensation, potentially devaluing data below its reproduction cost, often near zero (Martens et al., 2020). Furthermore, it shields providers from reputational damage resulting from data breaches (Karger, 2020).

One interesting finding is that the perceived risk of business data sharing acts as a partial mediator between data sovereignty and the willingness of data providers to share data. Following a logic from signaling theory, this may point to a cognitive effect of data sovereignty: when data providers have sovereignty over their data, they tend to view data sharing risks (e.g., data misuse) as lower, thereby increasing their willingness to share data. Data sovereignty as a dependent variable influencing cognitive states matches findings in digital platform literature. For example, Chang and Chen (2008) examine factors such as online store environments (e.g., website quality and brand) that affect the cognitive state of perceived risk and subsequently influence behavioral intentions. However, the partial mediation contributes only a small portion of the total effect size, indicating that additional factors likely influence the relationship between data sovereignty and willingness to share data.

Additionally, we do find that data providers are more likely to trust operators and data consumers when they have sovereignty. However, trust does not mediate the relationship between data sovereignty and willingness to share data. One potential explanation is that data providers who feel sovereign over their data are inherently more willing to share data, not necessarily due to increased trust in operators or data consumers but because sovereignty itself fosters willingness. For instance, data sovereignty involves control over shared data products. If providers can manage their shared data, they need not rely on trust in operators or consumers for business data sharing. They possess the means to ensure that data sharing adheres to agreed terms and conditions, reducing their dependence on others. This finding reinforces the idea in data sharing literature that technology can partially replace trust (e.g., Hawlitschek et al., 2018).

9.4 Conclusion of Chapter 9

This chapter answered the sixth research question of this study: *How does data sovereignty impact the data economy?* Addressing this research question helps to clarify and explain the assumed necessity of data sovereignty for the data economy's growth (scientific gap 4). We focused on factors most likely to be influenced by data sovereignty.

We found that when data providers feel sovereign over their data products, they are more likely to trust both a) meta-platform operators facilitating data sharing and b) data consumers they share data with. Surprisingly, we did not identify a correlation between the trust and their willingness to share data. This suggests that when data providers possess data sovereignty, trust in platform operators and data consumers becomes a less important factor for data sharing. In addition, we discovered that data providers, feeling sovereign over their data products, perceive lower risks in sharing their data. The reduced perceived risks subsequently increase their willingness to share data through meta-platforms. In summary, our study highlights the importance of data sovereignty in the data economy's growth by fostering trust in both meta-platform operators and data consumers, reducing perceived risks, and enhancing the willingness to share data in business data via meta-platforms.

PART 5: EPILOGUE

Chapter 10: Conclusion

This research aimed to create design knowledge for developing and evaluating control mechanisms for business data sharing through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy. To achieve this objective, we employed a design science research approach. In this final chapter, we revisit the research questions, presenting answers by elaborating on the key findings (Section 10.1). We then elaborate on our scientific contributions (Section 10.2). Subsequently, we describe the implications of our findings for practitioners and policymakers (Section 10.3). Finally, we discuss research limitations and propose suggestions for future research (Section 10.4).

10.1 Research questions and key findings

In the following section, we answer our research questions and explain their relevance to our research goal.

Problem space

Research question 1: How do meta-platforms create value in the data marketplace setting?

We answered this question in Chapter 4. In this chapter, we investigated how meta-platforms create value in the data marketplace setting, addressing a design knowledge gap of meta-platforms as a context in which the data sovereignty concern occurs (scientific gap 1). Context understanding guided further exploration of design knowledge across the problem, solution, and evaluation domains.

We identified two value creation archetypes of meta-platforms: discovery aggregators and one-stop shops. In the subsequent paragraphs, we describe the characteristics of each archetype, focusing on their 1) focal value proposition, 2) influence of meta-platforms on data marketplaces, 3) degree of integration between a meta-platform and data marketplaces, and 4) the object of sovereignty.

Discovery aggregators, having a focal value proposition of *core service aggregators*, create value by facilitating the search and dispatch of metadata across multiple marketplaces. The *minimal meta-platform influence* allows data marketplaces to largely retain their autonomy. Alignment between a meta-platform and data marketplaces involves *minimum integration* through simple partnerships by employing basic Application Programming Interfaces (APIs). Such alignments are motivated by *competition*, with data marketplace operators striving for differentiation through their unique offerings. Regarding the object of sovereignty, data providers concentrate on controlling *metadata* spread across various marketplaces.

One-stop shops have a focal value proposition of *multiple service aggregators*. They create value to integrated cross-marketplace offerings services through a unified interface. They do so by standardizing (e.g., providing shared services), regulating (e.g., aligning membership schema), sharing (e.g., computational resources), and experimenting (e.g., establishing programming ecosystems). One-stop shops necessitate *a high level of integration* between meta-platforms and data marketplaces. Two integration approaches exist: a) partnerships with advanced APIs and b) ownership through adopted infrastructure. The advanced APIs of one-stop shops facilitate more than search and dispatch functions; they enable direct data sharing across marketplaces. They allow data providers to transact in a chosen marketplace interface or directly through the meta-platform. On the other hand, with the adopted infrastructure approach, data marketplaces must replace their current infrastructure with a completely new technology framework developed by a meta-platform. Data marketplace operators *collaboratively* form a one-stop shop to leverage their technological capabilities and increase market reach. Finally, the one-stop shops' ability to expand data sharing beyond metadata positions *data products* as the object of sovereignty.

Data sovereignty is especially difficult to realize in the one-stop shop meta-platforms. In contrast to discovery aggregators that focus on metadata, one-stop shops handle both metadata and data products, thereby broadening the data sovereignty *object*. This is significant as the sovereignty object covers both the descriptive elements (metadata) and the actual content (data products). For data providers, data products often hold greater importance than metadata due to their sensitive contents. Improper management of these products can weaken competitive edges. Therefore, we focused on the one-stop shop meta-platforms for the remainder of the study.

Research question 2: What are the key facets of data sovereignty in data sharing through meta-platforms for data marketplaces?

We answered the second research question in Chapter 5, examining what data sovereignty is in the complex meta-platform setting. This inquiry is vital due to the prevalent ambiguities surrounding data sovereignty, signifying a design knowledge gap for specifying *goodness criteria* (scientific gap 2). By exploring the key facets of data sovereignty, this research laid the groundwork in the problem space domain, which then informs the solution and evaluation domains.

We found three *higher-level facets* of data sovereignty, each encompassing several more specific lower-level facets. First, the *protection* higher-level facet encompasses the baseline rights inherently held by data providers for retaining data ownership. These rights stand as a pre-existing condition before any data sharing transactions occur. Second, the *provision* of a higher-level facet encompasses data control, security, and compliance mechanisms provided by meta-platform operators to retain ownership rights during and after data sharing. Third, the *participation* higher-level facet requires clear responsibility division between sovereign entities (i.e., operators of meta-platforms and participating data marketplaces), facilitating active engagements of societal groups (e.g., data providers). The lower-level facets collectively formed the goodness criteria for designing and evaluating control mechanisms to enhance data sovereignty in meta-platforms.

We also identified three key contextual conditions influencing the realization of sovereignty facets: data type, business data sharing setting, and organizational size. Various data types, including structured and live-streamed, pose distinct technical challenges for implementing control mechanisms. Industry-specific data adds layers of compliance complexity. Considering business data sharing settings, ambiguities arise in allocating responsibilities between meta-platform and participating data marketplace operators. Additionally, aligning diverse data marketplace architectures presents technical difficulties in developing control mechanisms. Cross-border sharing in meta-platforms further complicates compliance. Finally, small and medium-sized enterprises face challenges in establishing ownership and control due to limited resources and expertise. In contrast, larger enterprises are more liable to the consequences of non-compliance.

In our study, it is crucial to focus on contextually significant and challenging conditions to enhance data sovereignty; otherwise, data sovereignty may be incorrectly deemed unimportant. Therefore, we focused on basic data products from the telecommunications industry as our chosen data type, meta-platforms as the business data sharing setting, and data providers within larger enterprises as the selected organizational size.

Solution space

Research question 3: What control mechanisms can enhance data sovereignty in data sharing via a meta-platform for data marketplaces?

We answered this research question in Chapter 6 by reviewing control mechanisms to enhance data sovereignty. Currently, a clear overview of such control mechanisms is lacking. Without such an overview, we risk overlooking appropriate mechanisms as *design options* that can fulfill the goodness criteria of data sovereignty.

Our research identified seven control mechanisms in the literature that enhance data sovereignty. These include a) one input control mechanism: certifications; b) five process control mechanisms: usage control, Self-Sovereign Identity (SSI), Privacy-enhancing Technology (PET), smart contracts, and dynamic consents; and c) a clan control mechanism: code of conduct.

We focused on formal controls by considering the control environment (e.g., meta-platforms as a data sharing context). Formal control, unlike informal control, has immediate and tangible effects. Therefore, formal control is particularly beneficial during the infancy stage of meta-platforms, enabling meta-platforms to showcase their capability to attract more users. Integrating multiple control modes to form a control portfolio often leads to superior outcomes, prompting us to combine two formal control modes: input and process control. Input control gatekeeps appropriate actors; meanwhile, process control suits uncertain scenarios, mainly when outputs are challenging to measure due to the nature of data as an experience good. This combination enables process control to provide insights that enhance input control.

Due to resource constraints, we selected one control mechanism for each input and process control mode, thus balancing the breadth and depth of our analysis. For input control, we chose certification, the sole mechanism identified in our review. For process control, PET is not a comprehensive solution as it tends to only address the security facet of data sovereignty. Similarly, dynamic consent is unsuitable because it relates more to individual data sovereignty, which diverges from our focus on organizational perspectives. Likewise, SSI is not adequate as it primarily addresses identifier data. Usage control is more appropriate as it enables the monitoring of data usage. However, we leaned toward selecting smart contracts because of their superiority in immutability. In fact, smart contracts are often viewed as the next generation of usage control. Hence, the most suitable control mechanisms to enhance data sovereignty in business data sharing through meta-platforms for data marketplaces are smart contracts and certifications. This is due to the potential of smart contracts to enhance the data sovereignty facets of ownership and control, while certifications enhance the data sovereignty facets of security, compliance, and responsibility.

Research question 4: What do the developed control mechanisms look like in the meta-platform setting?

We answered this question in Chapter 7. We a) derived principles to design control mechanisms and b) instantiated such mechanisms through a prototype of a meta-platform. Answering this question addressed a design knowledge gap of design principles (the "how") and instantiations of control mechanisms in meta-platforms (the "what) (scientific gap 3).

We specified design principles of smart contracts to enhance *data ownership,* which include a template for terms of use of data products with automatic metadata generation, guided data ownership configuration, and customizable ownership settings. To enhance *control over data,* smart contracts should include contract enforcement, data provenance, and data revocation. In terms of certifications, principles such as displaying seals and ensuring compatibility with established security standards can improve *security*. In addition, principles such as certification validity audit, explicit compliance statements, integrated legally valid contract management and dispute resolution, and endorsement from authoritative bodies can enhance *compliance*. Moreover, certification can foster *responsibility* by incorporating explicit delineations and certification body information. We incorporated these design principles into the relevant prototype interfaces.

Evaluation space

Research question 5: To what extent do data providers perceive that the control mechanisms enhance data sovereignty for data sharing through a meta-platform for data marketplaces?

We presented the answer in Chapter 8. In this chapter, we evaluated the perceived efficacy of control mechanisms to enhance data sovereignty in a meta-platform for data marketplaces. We asked this question to know whether our proposed mechanisms align with the expectations of data providers as the problem owners of sovereignty concerns. Additionally, this evaluation helped us reflect on the design knowledge we formulated in the problem and solution spaces.

Our findings suggested that data providers using meta-platforms with certifications felt more confident in meeting data sharing compliance requirements compared to those using meta-platforms without certifications. Additionally, these data providers perceived a clearer division of responsibility between meta-platform and data marketplace operators. When combined with smart contracts, the clarity of responsibility divisions became even better. Contrary to our expectations, however, we found no significant difference in the perceived security of data providers when sharing data on meta-platforms with certifications compared to those without.

Furthermore, our research found no significant differences in data providers' perception of their ability to retain ownership and control over shared data products in meta-platforms, regardless of the presence of smart contracts. This contradicted our initial expectations. Overall, our findings indicated that data providers recognized the efficacy of certifications in enhancing data sovereignty, but the impact of smart contracts remained less evident.

Research question 6: How does data sovereignty impact the data economy?
To answer this question, we evaluated the impacts of data sovereignty on the broader societal context of the data economy in Chapter 9. Addressing this research question helps to clarify and explain the presumed necessity of data sovereignty for the data economy's growth (scientific gap 4).

We found that when data providers feel sovereign over their data products, they are more likely to trust both a) meta-platform operators facilitating data sharing and b) data consumers they share data with. Surprisingly, we did not identify a correlation between the trust and their willingness to share data. This suggests that when data providers possess data sovereignty, trust in platform operators and data consumers becomes a less important factor for data sharing. In addition, we discovered that data providers, feeling sovereign over their data products, perceive lower risks in sharing their data. The reduced perceived risks subsequently increase their willingness to share data through meta-platforms.

Therefore, our study emphasizes the significance of data sovereignty in the growth of the data economy by a) promoting trust toward meta-platform operators and data consumers, b) reducing perceived risks, and c) increasing the willingness to share business data through meta-platforms.

Overall, we achieved our goal of creating design knowledge for developing and evaluating control mechanisms for business data sharing through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy. Specifically, we achieved our goal by addressing the six research questions discussed above. The following section elaborates on the scientific contributions of the created design knowledge.

10.2 Scientific contributions

10.2.1 Primary contributions

Our study contributes to the Information Systems literature, particularly on the intersection between data sharing and digital platform literature. We contribute by creating design knowledge to develop and evaluate control mechanisms for business data sharing through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy. Specifically, our primary contributions include 1) theorizing the potential impact of control mechanisms on data sovereignty, 2) outlining design options and principles as prescriptive knowledge, 3) defining goodness criteria to enhance data sovereignty, and 4) advancing context understanding of a meta-platform as a business data sharing setting.

1) Theorizing the potential impact of control mechanisms on data sovereignty. Our findings regarding the potential impact of smart contracts challenge the prevailing technical perspective in existing literature, which suggests that smart contracts help data providers retain data ownership (He et al., 2019; Sahoo & Halder, 2021) and exercise control over data (Saini et al., 2021; Zhang et al., 2019). This alternative view suggests that while technically smart contracts, indeed, enhance these two sovereignty facets, data providers may perceive these mechanisms as lacking efficacy. Hence, our finding, to some extent, reaffirms a smaller body of literature that finds smart contracts as still challenging to adopt due to various socio-technical factors (Kannengießer et al., 2022; Vacca et al., 2021; Zou et al., 2021). Our finding also raises question marks regarding the relevance and legitimacy of the extensive work on smart contracts.

In addition, our findings reveal that certifications enhance the data sovereignty facets of compliance and responsibility. These findings align with and complement the earlier studies in different contexts, such as Sturm et al. (2014), who examine the impact of certification on perceived privacy compliance, and Lansing et al. (2018), who find the impact of certification on the responsibility clarity of cloud certification providers. These findings also indirectly prove the validity of our proposed design principles for enhancing compliance (e.g., via giving explicit compliance statements) and responsibility (e.g., via providing certification body information).

In contrast, we found no evidence that data providers perceive certifications as having a high efficacy in enhancing security. This finding offers an alternative perspective to a major stream of literature beyond data sharing, demonstrating that certifications positively impact security (Kim & Kim, 2011; Lins et al., 2020; Lowry et al., 2012). Instead, our results align more closely with a smaller body of literature that reports no significant effect of certification on security (Gerald & Suzanne, 2010; Shah et al., 2014).

These findings offer researchers a new research direction. For example, future qualitative studies could explore why data providers perceive smart contracts to have a lack of efficacy in maintaining data ownership and control. Similarly, exploring why data providers feel certifications lack efficacy in ensuring secure data sharing is interesting. We provided potential explanations for these findings as a starting point in Chapter 8. For smart contracts, data providers may have concerns about 1) legal uncertainty and 2) complexity and skepticism in implementing smart contracts in meta-platforms. For certifications, data providers may have issues with 1) temporal limitations and 2) signal observability. Additionally, a closer examination of the design principles detailed in Chapter 7 through experiments at the principle level could provide insights into how exactly each principle impacts a facet of sovereignty. In doing so, we can refine the design principles, improve the prototype, and conduct a new evaluation. Hence, future research is advisable.

In addition, we make a methodological contribution when theorizing the potential impact of control mechanisms on data sovereignty. We do so by proposing a data sovereignty measurement model that offers researchers an alternative perspective of data sovereignty as a multi-faceted construct. We also proposed indicators for measuring data sovereignty facets. These indicators enable data sovereignty researchers to conduct quantitative research (e.g., survey-based) and theorize on data sovereignty. Additionally, these indicators also serve as alternative evaluation criteria to measure data sovereignty beyond technical aspects (e.g., Biehs & Stilling, 2024; Hellmeier et al., 2023; Zrenner et al., 2019) to include the behavioral aspects of data providers. We also found that the data sovereignty construct has explanatory power over relevant data economy constructs (i.e., trust, perceived risk, and willingness to share data), suggesting predictive validity.

2) Outlining design options and principles as prescriptive knowledge. The existing literature lacks a comprehensive overview of control mechanisms that can enhance data sovereignty. Therefore, we are among the first to synthesize the design knowledge of control mechanisms to enhance data sovereignty. In other words, we provide prescriptive knowledge about *design options* to tackle sovereignty concerns.

We go beyond the existing review of such control mechanisms (e.g., Lauf et al., 2022; Schmidt et al., 2022) by mapping control mechanisms to a) data sharing processes and b) data sovereignty facets. This mapping is crucial for scholars to understand the interplay between control mechanisms, data sharing processes, and data sovereignty facets. Such interplay enables scholars to focus on specific data sharing processes (preparation, agreement, or usage phase) and select control mechanisms that address the selected phase. Otherwise, choosing an inappropriate control mechanism for a specific phase can result in ineffectiveness. For example, implementing certifications in the usage phase might not be effective. Similarly, scholars must select control mechanisms based on the sovereignty facets they aim to address. For example, if the focus is on data ownership, specific control mechanisms like certification might be less relevant. Furthermore, we also linked these control mechanisms to control theory. We mapped the control mechanisms to various control modes. This enables scholars using control theory to argue from a theoretical perspective, selecting specific mechanisms to construct a control portfolio and justifying the appropriateness of such combinations.

We selected smart contracts and certifications as control mechanisms to enhance sovereignty. However, prescriptive knowledge on how to design such mechanisms in the form of *design principles* is lacking. The data sharing literature explores smart contracts (e.g., Alacam & Sencer, 2021; Lohmer et al., 2021), but mainly in hierarchical-based data sharing and seldom explicitly states such design principles. Similarly, the digital platform literature explores smart contracts (e.g., Gong et al., 2021; Mattila et al., 2021; Søgaard, 2021) but does not consider data as a value unit in market-based data sharing. Considering certifications, while the digital platform literature proposes design principles to advance certification presentations (e.g., Lins et al., 2023; Lins & Sunyaev, 2022), they do not yet explore data sharing platforms. Therefore, another primary contribution to the existing literature involves formulating design principles, being among the first to provide prescriptive knowledge for developing smart contracts and certifications in meta-platforms for the data marketplace setting. This advancement is significant as it provides data sharing researchers with previously unavailable prescriptive knowledge.

3) Defining goodness criteria to enhance data sovereignty. Contrary to current literature that predominantly links data sovereignty to data control (see a review by Hellmeier & von Scherenberg, 2023), we proposed a conceptual framework that takes a multi-faceted perspective on data sovereignty drawing from social contract theory. This conceptual framework incorporates contextual conditions that contribute to the difficulty of realizing data sovereignty facets.

The conceptual framework offers researchers and practitioners enhanced precision when developing (and claiming) data sovereignty solutions. For instance, while Pedreira et al. (2021) explore security mechanisms, their claims about exploring sovereignty solutions are not misguided. This is because, in fact, security is one of the facets of data sovereignty. Our framework helps make more accurate claims on which sovereignty facets are targeted when designing solutions. In doing so, we guide researchers in developing prescriptive theory, which offers principles for designing artifacts (Gregor et al., 2020). Data sovereignty facets can serve as goodness criteria (i.e., requirements and evaluation indicators) to design future data sovereignty solutions, e.g., in design science research (Hevner et al., 2004).

The conceptual framework *provides empirical evidence of the descriptive knowledge of data sovereignty*. Hummel et al. (2021) identify sixteen *notions* correlated with sovereignty, with the leading themes encompassing control, security, and ownership. This aligns with our empirical findings, emphasizing the centrality of these facets in data sovereignty discourses in business data sharing. Interestingly, although the responsibility facet ranks low regarding its co-occurrence with data sovereignty in Hummel et al.'s (2021) study, suggesting lesser importance, our research highlights its critical role in data sharing. Moreover, the facet of compliance emerges as another significant consideration in our study, which is yet to receive its deserved prominence in the existing literature. Thus, our finding not only supports the importance of these notions as data sovereignty facets but also elevates the importance of responsibility and compliance in contemporary data sovereignty discussions.

In addition, the conceptual framework *highlights potential causal mechanisms between data sovereignty (higher-level) facets.* We go beyond Hummel et al.'s (2021) works that correlate data sovereignty with certain notions. As shown in our framework, we propose a causal mechanism to explain how data sovereignty (higher-level) facets may correlate to each other's. These causal mechanisms provide clearer hypotheses for empirical investigations, directing future studies toward understanding the forces that drive changes in data sovereignty facets rather than just observing that changes occur. In experimental research, awareness of facets that co-vary with treatment and the selected facet can help researchers avoid drawing misleading conclusions based on correlations that may not reflect causality.

Finally, *we highlighted contextual conditions for specifying boundary conditions for data sovereignty.* Prior to this study, the data sovereignty literature did not explore the contextual conditions that influence the difficulty of realizing its facets. Consequently, boundary conditions for theorizing data sovereignty are unexplored. Therefore, we contribute to the literature by identifying three contextual conditions that serve as boundary conditions: data type, business data sharing setting, and organizational size. This is particularly important for future studies that aim to select facets of data sovereignty relevant to their study context, ensuring that they focus on the aspects that are both contextually significant and challenging to achieve; otherwise, data sovereignty may be incorrectly deemed unimportant. Moreover, investigating facets and contextual conditions could further clarify inconsistencies in studies on data sovereignty, for instance, why the control facet is sometimes considered unimportant (e.g., Shah et al., 2019) or crucial (e.g., van den Broek & van Veenstra, 2015).

4) Advancing context understanding of a meta-platform as a business data sharing setting. We consider two main issues of digital platforms to elaborate our contribution to advancing context understanding: *conceptual ambiguity* and *scoping* (de Reuver et al., 2018). Regarding conceptual ambiguity, prior investigations do not conceptually define and structure meta-platforms but instead jump in to discuss their value creation (e.g., Floetgen et al., 2021; Pitt & Cranefield, 2021). As a result, what a meta-platform is remains subject to individual interpretation. Regarding the scoping issue, the primary stream of existing literature often portrays meta-platforms as singular entities primarily focused on leveraging metadata aggregation for recommendations and comparisons (e.g., Hein et al., 2019; Lanza et al., 2016; Pitt et al., 2021). While this is true, a smaller body of literature (e.g., Fontana et al., 2007; Pon et al., 2015) finds that meta-platforms can go even further by providing standardized architecture. This means we are unsure what exactly a meta-platform can and cannot do. In summary, neglecting these two issues results in a deficiency of a descriptive theory on meta-platforms, obstructing more advanced theoretical development (e.g., as in design theories). Considering these two issues, our theoretical contributions to the digital platform literature are as follows.

First, we contribute to the literature by *clarifying the conceptual ambiguity of meta-platforms.* We further identify four interaction scenarios between supply and demand-side users on meta-platforms. Previous studies focus on a sole scenario of *demand-side users directly connecting with a meta-platform* (e.g., Cure et al., 2022; Ulrich & Alt, 2021), as exemplified by the Trivago case where individuals use a meta-platform to search for hotels. Hence, our findings broaden existing literature on meta-platforms by expanding the scope of user interactions by revealing three other scenarios: *a) supply-side users directly connect to a meta-platform*, *b) dual-sided direct access,* and *c) cross-marketplace connections* (refer to Chapter 4). This contribution is significant, as it allows scholars to reflect on the definition, structure, and interaction scenarios of meta-platforms, providing a foundation to specify the meta-platform being referred to in their research.

Second, we contribute to *resolving the scoping issue of meta-platforms by identifying two key value creation archetypes: discovery aggregators and one-stop shops.* Each archetype exhibits unique characteristics. For instance, discovery aggregators exert minimal influence on participating data marketplaces, focusing their value proposition on aggregation. In contrast, one-stop shops have a high influence, enabling them to expand their core value proposition beyond aggregation, such as standardizing architecture to provide a unified user interface. This distinction enables scholars to identify the type of meta-platform they discuss, thereby enhancing the accuracy of theorizing meta-platforms.

10.2.2 Secondary contributions

We make secondary contributions to the intersection between data sharing and digital platform literature in Information Systems by 1) providing evidence on the potential impact of data sovereignty on the broader data economy and 2) extending the applicability of theories employed in this research in the market-based data sharing context.

1) Providing evidence on the potential impact of data sovereignty on the broader data economy. Our study is among the first to provide evidence of the impact of data sovereignty on the broader data economy. Specifically, we contribute to the existing literature on digital platforms and data sharing in two ways: exploring the constructs and providing justificatory mechanisms.

First, we explored three key constructs to assess the impact of data sovereignty on the broader data economy: trust, perceived risk, and willingness to share data. For the first two constructs, we draw from the data sharing literature that suggests data sovereignty potentially impacts trust (Balan et al., 2023; Scheider, Lauf, Möller, et al., 2023) and perceived risk (Opriel et al., 2021). However, these two constructs are not enough, as they do not consider the behavioral attention of data providers. Hence, we incorporate the third construct frequently discussed as a key antecedent to the data economy: willingness to share data (e.g., Rantanen & Koskinen, 2020; Richter & Slowinski, 2019).

Second, our findings extend the existing literature by providing justificatory mechanisms on how data sovereignty impacts the data economy. We discovered a direct positive effect of data sovereignty on the willingness of data providers to share data. Interestingly, while perceived risk partially mediates this relationship, trust in operators and data consumers does not play a mediating role. Hence, this finding challenges the prevailing assumption in data sharing research that views trust as a major driver of willingness to share data (e.g., Dahlberg & Nokkala, 2019; Holler et al., 2019), revealing that this is not always the case when data providers exercise sovereignty over their data.

Besides being the first to consider data sovereignty impacts on the broader data economy, our work thus shows that their behavioral intentions of data sharing can be explained by considering data sovereignty. According to our findings, the extent to which data providers have sovereignty over their data significantly affects their intentions to share data. Hence, we suggest that data sovereignty should be considered a core antecedent of data sharing in the context of meta-platform for data marketplaces.

2) Extending the applicability of theories employed in this research in the market-based data sharing context. Through this process, we gained insights that deepen our understanding of these theories. We specifically outline our contribution to the 1) holon and holarchy lens and 2) control theory.

We contribute to the holon and holarchy lens by introducing the notion of spectrum specificity—that is, determining the degree (high or low) of holon interactions. We found that, for instance, minimal influence from a higher-level holon corresponds to minimal integration needs at lower levels, leading to only slight alignment within the holarchy structure. This finding is essential for scholars applying the holon and holarchy lens as it highlights the nature of holon relationships and the consequent impact on system coherence and functionality. For example, when discussing digital innovation (e.g., Wang, 2021), the resulting innovation may be influenced by the configuration of these holon interactions. Hence, we suggest considering the spectrum specificity of holon interactions as moderating variables when theorizing using the holon and holarchy lens.

We also contribute to the holon and holarchy lens by offering an alternative principle of holon interactions. So far, a holon is restricted to interacting with other holons at the same level within a single upper-level holon (e.g., Huang et al., 2002; Zekhnini et al., 2023). For example, data providers (holons) can interact only with data consumers (other holons at the same level) within a data marketplace (the upper-level holon). Our study finds scenarios where data providers interact uniquely within a meta-platform employing the holarchy structure. Here, data providers can interact not only with peers at the same level through a data marketplace (an upper-level holon) but also directly with the meta-platform itself (a holon two levels up). This finding is important for researchers as it may reshape the holarchy structure-based architecture we employ to build a digital system. For instance, in digital platforms, it may now be possible to have third-party developers as complementors not only at a platform level but also at a meta-platform level.

Considering the control theory, we added evidence to a few studies that found process control does not have significant outcomes compared to expected outcomes. This contrasts with the major stream of literature that finds positive impacts of process control (Cram et al., 2022; Srivastava & Thompson, 2012; Venkatesh et al., 2018; Zhang et al., 2023). Hence, our findings highlight the need for further exploration of control theory, particularly in the recently developed aspects of control theories such as control degree, control style, and control objective, beyond merely focusing on control mode (Cram & Wiener, 2018; Wiener et al., 2023). *Additionally, we observed a new analysis emerging from our exploration: platform users that operate control mechanisms themselves.* We called this unit of analysis a *user-enacted mechanism.* Research in digital platform control theories commonly portrays platform operators as *controllers*, both *offering* and *operating* control mechanisms. For instance, platform operators as controllers use Application Programming Interfaces (APIs) to direct third-party application development as controlees, enhancing quality (Ghazawneh & Henfridsson, 2013) and encouraging their continued participation as complementors (Goldbach et al., 2014). Thus, in behavioral studies examining platform control impact, the primary focus is often the controlees (e.g., Glaser, 2020; Staub et al., 2022). However, decentralized control mechanisms, such as smart contracts, empower supply-side platform users to operate these mechanisms themselves, facilitating direct bilateral agreements with demand-side users (e.g., Maass, 2022). In other words, the operation of control mechanisms can shift from platform providers to platform users. This shift highlights a previously underexamined unit of analysis for behavioral studies in platform control: a user-enacted mechanism. Table 10.1 summarizes the scientific contribution of this research.

Table 10.1. The summary of the scientific contribution of this research

Contribution level	Contribution
Primary contribution	• Theorizing the potential impact of control mechanisms on data sovereignty • Outlining design options and principles as prescriptive knowledge • Defining goodness criteria to enhance data sovereignty • Advancing context understanding of a meta-platform as a business data sharing setting
Secondary contribution	• Providing evidence on the potential impact of data sovereignty on the broader data economy • Extending the applicability of theories employed in this research in the market-based data sharing context

10.3 Implications for practitioners and policymakers

This study has implications for practitioners, especially (meta-)platform operators and policymakers focused on developing data economy-related policies.

First, (meta-)platform operators can view data sovereignty enhancement as an alternative to trust-building strategies for promoting data sharing. Chapter 9 found the influence of data sovereignty in the data economy. These findings stress the need for practitioners to keep advancing data sovereignty solutions. However, we found that trust does not significantly mediate the relationship between data sovereignty and willingness to share data. In other words, when data providers have data sovereignty, they are more willing to share data, irrespective of their trust level in the meta-platform operator and data consumers. This suggests that enhancing data sovereignty can be an alternative to trust-building strategies for promoting data sharing. Such strategies, such as building a reputation through repeated partnerships, generally require a longer time to take effect (Gelhaar & Otto, 2020).

Second, (meta-)platform operators should approach smart contract implementations cautiously, especially in scenarios where ownership and control are critical factors for data sovereignty. Likewise, they must be equally careful in developing certifications, especially when aiming to enhance security in data sharing. Chapter 8 revealed a disparity between technical capabilities and the perceived efficacy of two control mechanisms (i.e., smart contracts and certifications) in enhancing data sovereignty. Specifically, we found no evidence that data providers perceive smart contracts as having a high efficacy in enhancing the sovereignty facets of ownership and control. We also found certifications lacking efficacy in enhancing the sovereignty facet of security. Therefore, we recommend reassessing the current technical development approaches of these two control mechanisms by reflecting on our proposed design principles as a starting point. For example, suppose smart contract developments aim to retain ownership of data providers. In that case, (meta-) platform operators need to reflect on whether their developments incorporate (one of) our proposed design principles: terms-of-use templates, automated metadata generation, and flexible data ownership settings. They may not be sufficient because, despite integrating these principles into smart contract design, data providers remain unconvinced of their ability to retain data ownership. Consequently, operators should consider alternative principles in their smart contract developments.

Third, (meta-)platform operators can leverage the prototype developed in Chapter 7. Given the growing emphasis on openness between data marketplaces (e.g., Valkokari, 2023; Zappa et al., 2022), this prototype illustrates interactions between such marketplaces, providing practical insights into how data sharing processes work in an interoperable setting. Therefore, (meta-)platform operators can use our prototype as a starting point for further developments. For instance, they can use this prototype to identify usability gaps, develop their prototypes, and retest such prototypes with meta-platform users.

Fourth, (meta-)platform operators now have various design options to select control mechanisms to enhance data sovereignty (Chapter 6). Combined with our insight into data sovereignty facets discussed in Chapter 5, operators can select control mechanisms tailored to specific facets of interest. For instance, data control measures are in high demand (e.g., usage and access control), but their implementation is generally still in its infancy and challenging to realize (Tao et al., 2022). Thus, a more expansive viewpoint on data sovereignty allows us to analyze the potential trade-off and complex interplay between facets. For instance, (meta-)platform operators can explore potential solutions by weighing the trade-off between data type, ownership, and control. In cases where data is used for training machine learning models via a federated approach (Li et al., 2020), control over the data may not be required if the data is anonymized and used only for training purposes. When involving personal data, Multi-Party Computation (MPC) enables data sharing actors to collaboratively compute a function over their inputs without revealing private data (Agahari & de Reuver, 2022; Agahari et al., 2022). Hence, MPC may make data control less relevant because data providers cannot lose ownership. These examples illustrate how, paradoxically, data sovereignty may become easier to achieve when addressing non-control-related facets.

For policymakers developing data economy-related policies, **first, our findings provide empirical evidence and explanations about the paradox of meta-platform implications in the data economy.** While meta-platforms have the potential to reconcile highly heterogeneous data marketplaces (Section 4), they also, indeed, make data sovereignty problematic (Section 5). Meta-platforms are already complex solutions, and adding control mechanisms to tackle sovereignty issues complicates them further (Section 7). Yet, such complexity may be worth it because addressing sovereignty can increase the willingness of data providers to share data (Section 9), which potentially increases meta-platform adoptions. If this is the case, meta-platforms can contribute to resolving long-standing issues in data marketplaces: high transaction and multi-homing costs.

Thus, it is therefore vital for the policy-making agenda to stimulate the exploration of control mechanisms to capitalize on meta-platform potentials. This may include providing research funding for examining control mechanisms or giving tax incentives for businesses engaging in data sharing to use these mechanisms to reduce sovereignty concerns. Alternatively, policymakers can contribute by adopting aspects of meta-platform offerings, such as providing widely acknowledged standardization (e.g., via upper ontology).

Second, the findings related to data sovereignty facets (Chapter 5) also offer insights for these policymakers, shedding light on how specific regulations influence various sovereignty facets. For instance, the Digital Services Act directly targets the Provision facet, ensuring the accountability of digital service operators to equip data providers with robust control and compliance mechanisms. On the other hand, the Data Governance Act (DGA) shapes the Participation facet. By instituting a framework for neutral data intermediaries, DGA clarifies the division of data responsibilities (e.g., what platform operators and third-party providers can do) that is vital in complex scenarios in the data economy. While these regulations address all three higher-level facets of data sovereignty, there may be areas of overlap between these regulations that future policies need to recognize. Hence, future research is advised. In addition, policymakers should be aware that focusing on a single facet may inadvertently create unintended consequences for other facets, potentially hindering the overall effectiveness of the regulation. Moreover, when regulation aims to be context-independent, the contextual conditions affect whether businesses can realistically deal with the regulations regarding sovereignty.

In summary, this study has implications for practitioners, especially (meta-) platform operators, by 1) proposing data sovereignty enhancement as an alternative to trust-building strategies for promoting data sharing, 2) advising caution in smart contract and certification developments, highlighting a gap between technical capabilities and behavioral perceptions, 3) showcasing a prototype to facilitate data sharing across data marketplaces, and 4) highlighting various design options for control mechanisms to enhance data sovereignty. For policymakers developing data economy-related policies, we 1) provide empirical evidence and explanations about the paradox of meta-platform implications in the data economy and 2) offer insights for these policymakers, shedding light on how specific regulations influence various sovereignty facets.

10.4 Limitations and future research

This section discusses limitations and future research considering the research approach and the scope of the research.

10.4.1 Limitations related to the research approach

Similar to other design science research studies (e.g., Pumplun et al., 2023; Scheider et al., 2023), *we did not directly evaluate how design principles for smart contracts and certifications influence a specific data sovereignty facet.* For instance, we hypothesized that smart contracts enhanced data sovereignty by enabling data ownership retention. We compared the presence and absence of smart contracts to help retain data ownership of data providers. Yet, we did not explicitly test how design principles, such as *customizable ownership settings*, contribute to the ownership facet of data sovereignty. Put differently, we indirectly tested the collective efficacy of the design principles. This approach is justifiable, as a detailed experimental evaluation of each principle would result in an impractical number of experimental groups. However, it limits our ability to fully explain the observed discrepancy between the technical capabilities and perceived effectiveness of smart contracts and certifications in promoting data sovereignty, though we offer potential explanations in Chapter 10. Hence, a closer examination of the design principles detailed in Chapter 7 through experiments at the principle level could provide insights into how exactly each principle impacts a facet of sovereignty. In doing so, we can refine the design principles, improve the prototype, and conduct a new evaluation. Despite this limitation, the study already contributes in many ways to the intersection between digital platforms and data sharing literature (see Section 10.2).

We used a behavioral attention variable (i.e., willingness to share data by data providers) and self-reported measures (i.e., participants filling out a survey) rather than the actual transaction of data sharing in a meta-platform. Despite being commonly employed in an exploratory study to understand emerging phenomena (c.f., Agahari, 2023; Liang et al., 2023), this approach is susceptible to biases such as subjectivity and social desirability (Dimoka et al., 2011). While we rely on behavioral intention and self-reported measures, some previous studies (e.g., Dodds et al., 2018; Shirokova et al., 2022) report no significant difference between intentions and actions in natural settings, although this finding is challenged by others (e.g., Ableitner et al., 2018). Despite this limitation, we set a stage for future comparative studies examining data sovereignty impacts on the data economy when meta-platforms advance to the commercialization stage, allowing for the collection and analysis of actual data sharing transactions.

Like typical studies on early adoption stages of emerging phenomena (e.g., Fecho & Zöll, 2023; Zöll et al., 2022), *we employed a presentation and a prototype exploration to demonstrate the functioning of control mechanisms in business data sharing through a meta-platform.* This means that we evaluated visual representations rather than actual implementations of control mechanisms in a real-world context. Consequently, participants might not fully understand how control mechanisms work in enhancing data sovereignty in meta-platforms for data marketplaces. Even though we made efforts to ensure understanding, such as encouraging interviewees to challenge the concepts and checking the knowledge of survey participants, participants only interacted with the prototype for approximately 30 minutes. Therefore, we should view our findings within the early adoption phase of meta-platforms. Hence, this study serves as a foundation for future research, enabling comparisons and deeper analysis when meta-platforms gain broader business adoption.

We controlled certain contextual conditions to examine the data sovereignty's impact on the data economy to enhance internal validity. Although this is a common practice (Sekaran & Bougie, 2016), it indicates that our results may primarily apply to scenarios where data providers: a) are large organizations possessing the necessary technical skills to share highly sensitive data using control mechanisms and 2) receive sufficient monetary compensation for their data products. Future studies can explore the potential moderating effects of these contextual conditions. For example, following the logic of social exchange theory (e.g., Cropanzano & Mitchell, 2005), high payments for data might incentivize data providers to accept greater risks. This suggests that the mediating effect of perceived risk is lower in situations where data payments are high. Therefore, we suggest future research testing our model under varied contextual conditions.

Finally, we did not claim that our sample was representative in our Structural Equation Modeling (SEM) analysis of data sovereignty's impacts on the broader data economy, particularly considering data providers as an organizational unit of analysis. However, our sample mainly consisted of business managers or employees with specialized training. Furthermore, our sample has a balanced representation, with approximately 50% of participants knowledgeable about data marketplaces and the remaining 50% not, thereby ensuring diversity in perspectives. Additionally, there is an equitable gender distribution, with approximately a 50:50 ratio of males to females. More importantly, we compared our SEM results in Chapter 9 to SEM results in Chapter 8 when we developed our measurement model for data sovereignty (refer to Online Appendix 4). We observed consistent conclusions, meaning our SEM model remains robust when applied to varied data samples. Despite this, we recommend further research to test our model with a representative sample.

10.4.2 Limitations related to the scope of the research

We focus on market-mode data sharing, specifically from the perspective of business data sharing. Future studies can empirically confirm the applicability of data sovereignty facets, control mechanisms, and data sovereignty's influence on the data economy in two other settings: the hierarchy (e.g., supply chains) and network mode (e.g., data ecosystems). For example, let us consider our data sovereignty conceptual framework developed in Chapter 5. Considering the responsibility division, for instance, focal partners in supply chains generally must provide provision mechanisms, dictating the infrastructure for data control, which low-power partners must comply with (Ke & Wei, 2007). In contrast, the responsibility for provisioning data ecosystem infrastructure becomes the joint responsibility of its members (Otto & Jarke, 2019). Because data ecosystems are still in their infancy, the proven value of developing such ecosystems is unclear (Otto & Jarke, 2019). To speed up the emergence of a data ecosystem, data providers and consumers are often involved in the development; thus, allocating extra money to engage with these processes is required (Martin et al., 2021). This example illustrates how data sharing settings influence the difficulty of responsibility division.

Another example of the influence of the business data sharing setting is illustrated in defining data ownership in the supply chain context. Low-power partners often depend on focal partners who may unilaterally change data sharing agreements (Hewage, 2018; Kembro et al., 2017). Consequently, despite the risk of disclosing too much information and potential exploitation, low-power partners might feel compelled to comply with data sharing requests to maintain their relationships with focal partners (Ke & Wei, 2007). Likewise, power dynamics also happen in the network mode, where keystone members coordinate data ecosystem developments. These keystone members can influence data ownership, such as monetary incentives (Otto & Jarke, 2019). Consequently, non-keystone actors may have limited negotiating power (Scaria et al., 2018), further complicating their ability to define ownership within the ecosystem. The above examples show that the conceptual framework of data sovereignty is relevant and can be extended to other data sharing settings, although there may be slight differences in the influence specification of each facet.

Future research could also *explore the connection between data sovereignty and broader political issues*, such as state surveillance of data subject activities via sharing global telecommunication systems (e.g., Lashmar, 2017). The potential for state surveillance (e.g., Sweden's Tidö Agreement) might compel data providers to report data subjects who violate state regulations. This scenario indicates that the sovereignty of data providers in a business data sharing context, typically maintained through protection, provision, and participation, might be overtaken by state-imposed mandates.

Our study focuses specifically on meta-platforms as a market-based data sharing setting. However, beyond data sovereignty, the meta-platforms themselves face other adoption challenges. For instance, a meta-platform must consider that well-performing, operationalized data marketplaces may keep their platform closed, or what Hodapp and Hanelt (2022) termed *planned low interoperability* due to strategic motives to avoid direct competition. Data marketplace pursuing this competitive strategy is likely not always welcome with the idea of joining a meta-platform: they want to protect their market share. Another issue is that not every data marketplace is commercially viable at the moment (see a review by Spiekermann, 2019); hence, marketplaces may potentially *piggyback* the network effects without sufficiently contributing to the development of meta-platforms. A meta-platform must also consider (and prepare for) various impacts of increased network effects. In addition to antitrust regulation (Mosterd et al., 2021), a concentrated network effect in a single digital ecology negatively impacts privacy, security, homogeneity, and reliability (Hodapp & Hanelt, 2022).

Considering homogeneity (i.e., innovation stagnancy), for instance, if a meta-platform becomes too big with massive network effects, new entrances of data marketplaces (even with the newest technological superiority) may not be sufficiently adopted. Finally, Márton (2021) argues that every digital ecology has its limit, and platform designers must respect that limit. For example, standardization can be helpful to improve compliance but, at the same time, make the platform participants too dependent on the focal platform. Consequently, they may lose their capability and competitive advantage in the long run. Hence, exploring these issues is advised to contribute to our understanding of meta-platform realization as a data sharing context.

In addition, we focus on the most relevant data sovereignty facets and contextual conditions. Although they emerged from our empirical data and signaled their importance, we did not claim them to be exhaustive. They serve as a foundational basis, and we see an opportunity for future research to explore other conditions and possibly conduct prioritization studies. For example, while our study focuses on the most critical facets of data sovereignty, we are aware of the potential significance of other dimensions (e.g., justice). To account for this, we considered the justice dimension as a control variable in the prototype development by suggesting appropriate data pricing to ensure fair revenue distributions.

These sovereignty facets emerged mainly from the data provider perspective. Therefore, future work can explore the data consumers' perspective to provide a more balanced standpoint, possibly leading to new insights in, e.g., the relation between data sovereignty facets. For instance, when data consumers have more purchasing power, data providers may have less influence in creating data sharing agreements. This could require providers to give up some ownership rights. Table 10.2 summarizes the research limitations and future research.

Table 10.2. Limitations and further research

Category	Limitation	Further research
Research approach	Did not directly evaluate how design principles for smart contracts and certifications influence a specific data sovereignty facet	Evaluating the prescriptive knowledge at the design principle level
	Selecting a behavioral attention variable (i.e., willingness to share data by data providers) and self-reported measures (i.e., participants filling a survey) rather than the actual transaction of data sharing in meta-platforms	Comparing the finding of data sovereignty's influence on the data economy by using the behavioral attention variable vs. actual data sharing transactions when meta-platforms reach the adoption phase
	Employing a presentation and a prototype exploration to demonstrate the functioning of control mechanisms in business data sharing through a meta-platform	Comparing the findings from meta-platform value creations, data sovereignty facets, perceived efficacy of control mechanisms, and data sovereignty influence on the data economy when meta-platforms reach the adoption phase
	Controlling contextual conditions to enhance internal validity	Examining the moderating effect of contextual conditions
	Using non-representative samples in the Structural Equation Modeling (SEM) for investigating data sovereignty impacts on the broader data economy	Testing our SEM model with a representative sample
Scope	Focusing on the market-mode data sharing setting from the business data sharing perspective	• Exploring the data sovereignty facets, control mechanisms, and data sovereignty's influence on the data economy on the two other business data sharing settings: the hierarchy and network mode • Connecting data sovereignty to the broader political issues • Exploring the strategy to tackle planned low interoperability by data marketplace operators, piggybacking issues, and innovation stagnancy
	Focusing on the most relevant aspect of data sovereignty facets for data sharing	• Exploring the relevance of other data sharing facets and contextual conditions • Exploring the data consumer perspective

In conclusion, this study created design knowledge for developing and evaluating control mechanisms for business data sharing through meta-platforms for data marketplaces, focusing on investigating their efficacy in enhancing data sovereignty in the societal context of the data economy. In doing so, this study resolves the tensions in the European policy-making agendas that promote a single market for data (e.g., in EU Data strategy, Data Act) while, at the same time, pushing sector-specific data marketplaces to exist (e.g., the eight verticals in the Digital Europe program). Furthermore, policy agendas also emphasize adherence to data sovereignty principles. As data sovereignty is vital for data providers to share their data via meta-platforms, addressing this concern may increase meta-platform adoptions. Hence, we hope a meta-platform can realize its potential to be one distinguished instrument to fulfill what we hope (and are optimistic) for in a Data Economy: a single European Data Market in 2030.

References

Aaltonen, A., Alaimo, C., & Kallinikos, J. (2021). The Making of Data Commodities: Data Analytics as an Embedded Process. *Journal of management information systems, 38*(2), 401-429. https://doi.org/10.1080/07421222.2021.1912928

Abbas, A. E. (2021). *Designing Data Governance Mechanisms for Data Marketplace Meta-Platforms*. Proceedings 34th Bled eConference – Digital Support from Crisis to Progressive Change, Online.

Abbas, A. E., Agahari, W., Ofe, H., Zuiderwijk, A., & de Reuver, M. (2023). *Toward Sovereign Data Exchange Through a Meta-Platform for Data Marketplaces: A Preliminary Evaluation of the Perceived Efficacy of Control Mechanisms*. 36th Bled eConference – Digital Economy and Society: The Balancing Act for Digital Innovation in Times of Instability, Bled, Slovenia.

Abbas, A. E., Agahari, W., van de Ven, M., Zuiderwijk, A., & de Reuver, M. (2021). Business Data Sharing through Data Marketplaces: A Systematic Literature Review. *Journal of Theoretical and Applied Electronic Commerce Research, 16*(7), 3321-3339. https://doi.org/10.3390/jtaer16070180

Abbas, A. E., Ofe, H., Zuiderwijk, A., & de Reuver, M. (2022). *Preparing Future Business Data Sharing via a Meta-Platform for Data Marketplaces: Exploring Antecedents and Consequences of Data Sovereignty*. 35th Bled eConference - Digital Restructuring and Human (Re-Action), Bled, Slovenia.

Abbas, A. E., Ofe, H., Zuiderwijk, A., & de Reuver, M. (2023). *Toward Business Models for a Meta-Platform: Exploring Value Creation in the Case of Data Marketplaces*. The 56th Hawaii International Conference on System Sciences (HICSS), Honolulu, Hawaii, the United States.

Abbasi, A., Sarker, S., & Chiang, R. H. (2016). Big Data Research in Information Systems: Toward an Inclusive Research Agenda. *Journal of the Association for Information Systems, 17*(2), 3. https://doi.org/10.17705/1jais.00423

Abdullah, N. S., Sadiq, S., & Indulska, M. (2010). *Information Systems Research: Aligning to Industry Challenges in Management of Regulatory Compliance*. PACIS 2010 Proceedings, Taipei, Taiwan.

Ableitner, L., Tiefenbeck, V., Fleisch, E., & Staake, T. (2018). *Eco-Feedback Interventions: Selective Attention and Actual Behavior Change*. AMCIS 2018 Proceedings, New Orleans, Louisiana, the United States.

Abraham, R., Schneider, J., & vom Brocke, J. (2023). A Taxonomy of Data Governance Decision Domains in Data Marketplaces. *Electronic Markets, 33*(1), 1-13. https://doi.org/10.1007/s12525-023-00631-w

Adam, M., Croitor, E., Werner, D., Benlian, A., & Wiener, M. (2022). Input Control and Its Signalling Effects for Complementors' Intention to Join Digital Platforms. *Information Systems Journal, 33*(3). https://doi.org/10.1111/isj.12408

Agahari, W. (2020). *Platformization of Data Sharing: Multi-Party Computation (MPC) as Control Mechanism and Its Effect on Firms' Participation in Data Sharing via Data Marketplaces*. 33rd Bled eConference—Enabling Technology for a Sustainable Society, Bled, Slovenia.

Agahari, W. (2023). *Multi-Party Computation as a Privacy-Enhancing Technology: Implications for Data Sharing by Businesses and Consumers* [Dissertation, Delft University of Technology]. Delft.

Agahari, W., & de Reuver, M. (2022). *Rethinking Consumers' Data Sharing Decisions With the Emergence of Multi-Party Computation: An Experimental Design For Evaluation*. The 30th European Conference on Information Systems, Timişoara, Romania.

Agahari, W., Ofe, H., & de Reuver, M. (2022). It Is Not (Only) About Privacy: How Multi-Party Computation Redefines Control, Trust, and Risk in Data Sharing. *Electronic Markets, 32*(3), 1577-1602. https://doi.org/10.1007/s12525-022-00572-w

Aiken, K. D. (2006). Trustmarks, Objective-Source Ratings, and Implied Investments in Advertising: Investigating Online Trust and the Context-Specific Nature of Internet Signals. *Journal of the Academy of Marketing Science, 34*(3), 308-323. https://doi.org/10.1177/0092070304271004

Alqahtani, M., & Erfani, E. (2021). *Impact of Technical Controls, Accountability, and Monitoring on the Job Performance of Employees: Assessing the Mediating Role of Stress*. ACIS 2021 Proceedings, Sydney, Australia.

Alt, R., & Zimmermann, H.-D. (2019). Electronic Markets on Platform Competition. *Electronic Markets, 29*(2), 143-149. https://doi.org/10.1007/s12525-019-00353-y

Ansah, E. O., Kaplowitz, M. D., Lupi, F., & Kerr, J. (2020). Smallholder Participation and Procedural Compliance With Sustainable Cocoa Certification Programs. *Agroecology and Sustainable Food Systems, 44*(1), 54-87. https://doi.org/10.1080/21683565.2019.1579776

Arp, R., Smith, B., & Spear, A. D. (2015). *Building Ontologies With Basic Formal Ontology*. MIT Press.

Asare, A. K., Brashear-Alejandro, T. G., & Kang, J. (2016). B2B Technology Adoption in Customer Driven Supply Chains. *Journal of Business & Industrial Marketing, 31*(1), 1-12. https://doi.org/10.1108/JBIM-02-2015-0022

Assarroudi, A., Heshmati Nabavi, F., Armat, M. R., Ebadi, A., & Vaismoradi, M. (2018). Directed Qualitative Content Analysis: The Description and Elaboration of Its Underpinning Methods and Data Analysis Process. *Journal of research in nursing, 23*(1), 42-55.

Azcoitia, S. A., & Laoutaris, N. (2022). A Survey of Data Marketplaces and Their Business Models. *SIGMOD Record, 51*(3), 18-29. https://doi.org/10.1145/3572751.3572755

Baker, J. B. (2021). Protecting and Fostering Online Platform Competition: The Role of Antitrust Law. *Journal of Competition Law & Economics*. https://doi.org/10.1093/joclec/nhaa032

Balan, A., Gabriel Tan, A., Kourtit, K., & Nijkamp, P. (2023). Data-Driven Intelligent Platforms—Design of Self-Sovereign Data Trust Systems. *Land, 12*(6), 1-21. https://doi.org/10.3390/land12061224

Banerjee, A. V., & Duflo, E. (2000). Reputation Effects and the Limits of Contracting: A Study of the Indian Software Industry. *The Quarterly Journal of Economics, 115*(3), 989-1017. https://doi.org/10.1162/003355300554962

Basaure, A., Vesselkov, A., & Töyli, J. (2020). Internet of Things (IoT) Platform Competition: Consumer Switching Versus Provider Multihoming. *Technovation, 90*, 102101. https://doi.org/10.1016/j.technovation.2019.102101

Batubara, F. R., Ubacht, J., & Janssen, M. (2018). *Challenges of Blockchain Technology Adoption for E-government*. Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, Delft, The Netherlands. https://dx.doi.org/10.1145/3209281.3209317

Batubara, F. R., Ubacht, J., & Janssen, M. (2019). *Unraveling Transparency and Accountability in Blockchain*. Proceedings of the 20th Annual International Conference on Digital Government Research, New York, NY, the United States. https://dx.doi.org/10.1145/3325112.3325262

Bauer, J., Helmke, R., Bothe, A., & Aschenbruck, N. (2019). CAN't Track Us: Adaptable Privacy for ISOBUS Controller Area Networks. *Computer Standards & Interfaces, 66*, 103344. https://doi.org/10.1016/j.csi.2019.04.003

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems, 19*(10), 1020-1034. https://doi.org/10.17705/1jais.00518

Beese, J., Haki, K., Schilling, R., Kraus, M., Aier, S., & Winter, R. (2023). Strategic Alignment of Enterprise Architecture Management – How Portfolios of Control Mechanisms Track a Decade of Enterprise Transformation at Commerzbank. *European Journal of Information Systems, 32*(1), 92-105. https://doi.org/10.1080/0960085X.2022.2085200

Bernstein, L. (1996). Foreword: Importance of Software Prototyping. *Journal of Systems Integration, 6*(1), 9-14. https://doi.org/10.1007/BF02262748

Bider, I., Johannesson, P., & Perjons, E. (2013). Design Science Research as Movement Between Individual and Generic Situation-Problem–Solution Spaces. In (pp. 35-61). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-33371-2_3

Biegel, F., Bongers, A., Chidambaram, R., Feld, T., Garloff, K., & Ingenrieth, F. (2020). GAIA-X: Driver of Digital Innovation in Europe. *Germany's Federal Ministry for Economic Affairs and Energy (BMWi)*.

Biehs, S., & Stilling, J. (2024). *Identification of Key Requirements for the Application of Data Sovereignty in the Context of Data Exchange*. Proceedings of the 57th Hawaii International Conference on System Sciences, Honolulu, Hawaii, the United States.

Bodin, J. (1576). *Les six livres de la Republique*. Chez Iacques du Puys.

Brechtel, M., Petrik, D., & Hölzle, K. (2023). *From Challenges to Solution Pathways for Industrial Data Ecosystems-A Socio-Technical Perspective*. Wirtschaftsinformatik 2023 Proceedings, Paderborn, Germany.

Carter, S. M. (2006). The Interaction of Top Management Group, Stakeholder, and Situational Factors on Certain Corporate Reputation Management Activities. *Journal of Management Studies, 43*(5), 1145-1176. https://doi.org/https://doi.org/10.1111/j.1467-6486.2006.00632.x

Carvalho, A., & Karimi, M. (2020, 2020). How Blockchain Can Bring Trust and Transparency to the Payment of Crowd Forecasters. ICIS 2020 Proceedings, Hyderabad, India.

Casadesus-Masanell, R., & Ricart, J. E. (2010). From Strategy to Business Models and Onto Tactics. *Long Range Planning, 43*(2-3), 195-215. https://doi.org/10.1016/j.lrp.2010.01.004

Chang, H. H., & Chen, S. W. (2008). The Impact of Online Store Environment Cues on Purchase Intention: Trust and Perceived Risk as a Mediator. *Online Information Review, 32*(6), 818-841. https://doi.org/10.1108/14684520810923953

Chen, Y., Chen, S., Liang, J., Feagan, L. W., Han, W., Huang, S., & Wang, X. S. (2020). Decentralized Data Access Control Over Consortium Blockchain. *Information Systems, 94*(1), 1-15. https://doi.org/10.1016/j.is.2020.101590

Chiquito, E., Chiquito, A., Bodin, U., & Synnes, K. (2022). *Automated Usage Control for Secure Data Sharing Based on Ricardian Contracts*. IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society, Brussels, Belgium.

Choi, J. P. (2010). Tying in Two-Sided Markets With Multi-Homing. *The Journal of Industrial Economics, 58*(3), 607-626. https://doi.org/10.1111/j.1467-6451.2010.00426.x

Chown, J. (2021). The Unfolding of Control Mechanisms inside Organizations: Pathways of Customization and Transmutation. *Administrative science quarterly*, *66*(3), 711-752. https://doi.org/10.1177/0001839220980015

Cichy, P., Salge, T.-O., & Kohli, R. (2021). Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars. *MIS quarterly*, *45*(4), 1863-1892.

Clack, C. D. (2018). Smart Contract Templates: Legal Semantics and Code Validation. *Journal of Digital Banking, 2*(4), 338-352.

Clausen, S., Brünker, F., Jung, A.-K., & Stieglitz, S. (2022). *The Impact of Signaling Commitment to Ethical AI on Organizational Attractiveness*. Wirtschaftsinformatik 2022 Proceedings, Nuremberg, Germany.

Clegg, B., & Shaw, D. (2008). Using Process-Oriented Holonic (PrOH) Modelling to Increase Understanding of Information Systems. *Information Systems Journal*, *18*(5), 447-477. https://doi.org/10.1111/j.1365-2575.2008.00308.x

Cohen, J. (2013). *Statistical Power Analysis for the Behavioral Sciences*. Academic press.

Colwell, S. R., Zyphur, M. J., & Schminke, M. (2011). When Does Ethical Code Enforcement Matter in the Inter-Organizational Context? The Moderating Role of Switching Costs. *Journal of Business Ethics, 104*(1), 47-58. https://doi.org/10.1007/s10551-011-0888-8

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling Theory: A Review and Assessment. *Journal of Management, 37*(1), 39-67. https://doi.org/10.1177/014920631038841

Constantinides, P., Chiasson, M. W., & Introna, L. D. (2012). The Ends of Information Systems Research: A Pragmatic Framework. *MIS quarterly, 36*(1), 1-20. https://doi.org/10.2307/41410403

Costabile, C., Iden, J., & Bygstad, B. (2022). Building Digital Platform Ecosystems Through Standardization: An Institutional Work Approach. *Electronic Markets*, *32*(4), 1877-1889. https://doi.org/10.1007/s12525-022-00552-0

Cram, W. A., Brohman, K., & Gallupe, R. B. (2016). Information Systems Control: A Review and Framework for Emerging Information Systems Processes. *Journal of the Association for Information Systems, 17*(4), 216 – 266. https://doi.org/10.17705/1jais.00427

Cram, W. A., & Wiener, M. (2018). Perceptions of control legitimacy in information systems development. *Information Technology & People, 31*(3), 712-740. https://doi.org/10.1108/ITP-11-2016-0275

Cram, W. A., Wiener, M., Tarafdar, M., & Benlian, A. (2022). Examining the Impact of Algorithmic Control on Uber Drivers' Technostress. *Journal of management information systems*, *39*(2), 426-453. https://doi.org/10.1080/07421222.2022.2063556

Croitor, E., Adam, M., & Benlian, A. (2021). Perceived Input Control on Digital Platforms: A Mixed-Methods Investigation of Web-Browser Platforms. *Journal of Decision Systems*, *30*(1), 50-71. https://doi.org/10.1080/12460125.2020.1815440

Cropanzano, R., & Mitchell, M. S. (2005). Social Exchange Theory: An Interdisciplinary Review. *Journal of Management*, *31*(6), 874-900. https://doi.org/10.1177/0149206305279602

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Applied Innovation Review*, *1*(2), 1-16.

Crotty, M. J. (1998). *The Foundations of Social Research: Meaning and Perspective in the Research Process*. Sage Publications Ltd.

Cuno, S., Bruns, L., Tcholtchev, N., Lämmel, P., & Schieferdecker, I. (2019). Data Governance and Sovereignty in Urban Data Spaces Based on Standardized ICT Reference Architectures. *Data*, *4*(1), 1-24. https://doi.org/10.3390/data4010016

Cure, M., Hunold, M., Kesler, R., Laitenberger, U., & Larrieu, T. (2022, 2022/12/01). Vertical integration of platforms and product prominence. *Quantitative Marketing and Economics*, *20*(4), 353-395. https://doi.org/10.1007/s11129-022-09255-4

D'Hauwers, R., & Walravens, N. (2022). *Do You Trust Me? Value and Governance in Data Sharing Business Models*. Proceedings of Sixth International Congress on Information and Communication Technology, Singapore.

Dahlberg, T., & Nokkala, T. (2019). *Willingness to Share Supply Chain Data in an Ecosystem Governed Platform–An Interview Study*. BLED 2019 Proceedings, Bled, Slovenia.

Dahlman, C. J. (1979). The Problem of Externality. *The journal of Law and Economics*, *22*(1), 141-162. https://doi.org/10.1086/466936

Dai, H., & Luo, X. (2011). *The Role of Risk Perception, Trust, Innovativeness and Emotion in Developing Consumer's Satisfaction in Electronic Mediated Environment (EME)*. ICIS 2011 Proceedings, Shanghai, China.

Dalmolen, S., Bastiaansen, H., Kollenstart, M., & Punter, M. (2020). *Infrastructural Sovereignty Over Agreement and Transaction Data ('Metadata') in an Open Network-Model for Multilateral Sharing of Sensitive Data*. 40th International Conference on Information Systems, ICIS 2019, Munich, Germany

Danylak, P., Lins, S., Hsu, C., & Sunyaev, A. (2022). *Making Sense of Certification Internalization: A Process Model for Implementing Information Security and Data Protection Certifications*. Proceedings of the 17th Pre-ICIS Workshop on Information Security and Privacy (WISP 2022), Copenhagen, Denmark.

De Filippi, P., & McCarthy, S. (2012). Cloud Computing: Centralization and Data Sovereignty. *European Journal of Law and Technology, 3*(2), 1-18.

De Mooy, M. (2017). *Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data: Considerations for Future Policy Regimes in the United States and the European Union*. Bertelsmann Stiftung.

de Reuver, M., Sørensen, C., & Basole, R. C. (2018). The Digital Platform: A Research Agenda. *Journal of Information Technology*, *33*(2), 124-135. https://doi.org/10.1057/s41265-016-0033-3

Dellermann, D., Lipusch, N., Ebel, P., & Leimeister, J. M. (2019). Design Principles for a Hybrid Intelligence Decision Support System for Business Model Validation. *Electronic Markets, 29*, 423-441. https://doi.org/10.1007/s12525-018-0309-2

Demichev, A., Kryukov, A., & Prikhod'Ko, N. (2021). Business Process Engineering for Data Storing and Processing in a Collaborative Distributed Environment Based on Provenance Metadata, Smart Contracts and Blockchain Technology. *Journal of Grid Computing, 19*(1), 1-30. https://doi.org/10.1007/s10723-021-09544-4

Dillon, D. R., O'Brien, D. G., & Heilman, E. E. (2000). Literacy Research in the Next Millennium: From Paradigms to Pragmatism and Practicality. *Reading Research Quarterly, 35*(1), 10-26.

Dimoka, A., Pavlou, P. A., & Davis, F. D. (2011). Research Commentary—NeuroIS: The Potential of Cognitive Neuroscience for Information Systems Research. *Information Systems Research, 22*(4), 687-702. https://doi.org/10.1287/isre.1100.0284

Dixit, A., Deval, V., Dwivedi, V., Norta, A., & Draheim, D. (2022). Towards User-Centered and Legally Relevant Smart-Contract Development: A Systematic Literature Review. *Journal of Industrial Information Integration*, *26*. https://doi.org/10.1016/j.jii.2021.100314

Djamasbi, S., & Strong, D. (2019). User Experience-Driven Innovation in Smart and Connected Worlds. *AIS Transactions on Human-Computer Interaction, 11*(4), 215-231. https://doi.org/10.17705/1thci.00121

Dodds, R., Jenkins, B., Smith, W., & Pitts, R. E. (2018). Willingness-To-Pay vs Actual Behavior: Sustainable Procurement at Festivals. In T. Ohnmacht, J. Priskin, & J. Stettler (Eds.), *Contemporary Challenges of Climate Change, Sustainable Tourism Consumption, and Destination Competitiveness* (Vol. 15, pp. 67-78). Emerald Publishing Limited. https://doi.org/10.1108/S1871-317320180000015009

Driessen, S. W., Monsieur, G., & Van Den Heuvel, W. (2022). Data Market Design: A Systematic Literature Review. *IEEE Access*, *10*, 33123-33153. https://doi.org/10.1109/access.2022.3161478

Du, W., & Atallah, M. J. (2001). *Secure Multi-Party Computation Problems and Their Applications: A Review and Open Problems*. Proceedings of the 2001 workshop on New security paradigms, New York, New York, the United States.

Duan, Y., Mullins, R., Hamblin, D., Stanek, S., Sroka, H., Machado, V., & Araujo, J. (2002). Addressing ICTs Skill Challenges in SMEs: Insights From Three Country Investigations. *Journal of European Industrial Training, 26*(9), 430-441. https://doi.org/10.1108/03090590210451524

Duisberg, A. (2022). Legal Aspects of IDS: Data Sovereignty—What Does It Imply? *Designing Data Spaces*, 61.

Eladhari, M. P., & Ollila, E. M. (2012). Design for Research Results: Experimental Prototyping and Play Testing. *Simulation & Gaming, 43*(3), 391-412. https://doi.org/10.1177/1046878111434255

Elkjaer, B., & Simpson, B. (2011). Pragmatism: A Lived and Living Philosophy. What Can It Offer to Contemporary Organization Theory? In *Philosophy and organization theory* (pp. 55-84). Emerald Group Publishing Limited.

Ellis, E. (2006). Citizenship and Property Rights: A New Look at Social Contract Theory. *The Journal of Politics, 68*(3), 544-555. https://doi.org/10.1111/j.1468-2508.2006.00444.x

Elo, S., & Kyngäs, H. (2008). The Qualitative Content Analysis Process. *Journal of Advanced Nursing, 62*(1), 107-115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Esposito, C., Castiglione, A., & Choo, K. K. R. (2016). Encryption-Based Solution for Data Sovereignty in Federated Clouds. *IEEE Cloud Computing, 3*(1), 12-17. https://doi.org/10.1109/MCC.2016.18

Esposito, C., Castiglione, A., Frattini, F., Cinque, M., Yang, Y., & Choo, K. K. R. (2019). On Data Sovereignty in Cloud-Based Computation Offloading for Smart Cities Applications. *IEEE Internet of Things Journal, 6*(3), 4521-4535. https://doi.org/10.1109/JIOT.2018.2886410

Ethikrat, D. (2017). *Big Data and Health–Data Sovereignty as the Shaping of Informational Freedom*. (Opinion – Executive Summary & Recommendations).

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American journal of theoretical and applied statistics, 5*(1), 1-4. https://doi.org/10.11648/j.ajtas.20160501.11

Eurich, M., Oertel, N., & Boutellier, R. (2010). The Impact of Perceived Privacy Risks on Organizations' Willingness to Share Item-Level Event Data Across the Supply Chain. *Electronic Commerce Research, 10*(3), 423-440. https://doi.org/10.1007/s10660-010-9062-0

European Commission. (2024). *The European Data Market Monitoring Tool*. (European Data Market Study 2021–2023. https://ec.europa.eu/newsroom/dae/redirection/document/105189

Fadler, M., & Legner, C. (2022). Data Ownership Revisited: Clarifying Data Accountabilities in Times of Big Data and Analytics. *Journal of Business Analytics, 5*(1), 123-139. https://doi.org/10.1080/2573234x.2021.1945961

Falcão, R., Matar, R., Rauch, B., Elberzhager, F., & Koch, M. (2023). A Reference Architecture for Enabling Interoperability and Data Sovereignty in the Agricultural Data Space. *Information, 14*(3), 197. https://doi.org/10.3390/info14030197

Fassnacht, M., Benz, C., Heinz, D., Leimstoll, J., & Satzger, G. (2023). *Barriers to Data Sharing among Private Sector Organizations*. Proceedings of the 56th Hawaii International Conference on Systems Sciences, Honolulu, Hawaii, the United States.

Fazi, M. A. (2022). A Contextual Study of Regulatory Framework for Blockchain. In *Regulatory Aspects of Artificial Intelligence on Blockchain* (pp. 40-51). IGI Global.

Featherman, M. (2001). *Extending the Technology Acceptance Model by Inclusion of Perceived Risk*. AMCIS 2001 Proceedings, Boston, Massachusetts, the United States.

Featherman, M., & Fuller, M. (2003). *Applying TAM to E-services Adoption: The Moderating Role of Perceived Risk*. 36th Annual Hawaii International Conference on System Sciences, Honolulu, Hawaii, the United States.

Fernqvist, F., & Ekelund, L. (2014). Credence and the Effect on Consumer Liking of Food – A Review. *Food Quality and Preference, 32*(1), 340-353. https://doi.org/10.1016/j.foodqual.2013.10.005

Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics*. Sage.

Field, A., & Hole, G. (2002). *How to design and report experiments*. Sage. https://doi.org/DOI: 10.17705/1jais.00787

Filatotchev, I., & Bishop, K. (2002). Board Composition, Share Ownership, and 'Underpricing' of U.K. IPO Firms. *Strategic Management Journal, 23*(10), 941-955. https://doi.org/10.1002/smj.269

Fink, L. (2022). Why and How Online Experiments Can Benefit Information Systems Research. *Journal of the Association for Information Systems, 23*(6), 1333-1346.

Firdausy, D. R., De Alencar Silva, P., Van Sinderen, M., & Iacob, M.-E. (2022). *Towards a Reference Enterprise Architecture to Enforce Digital Sovereignty in International Data Spaces*. 2022 IEEE 24th Conference on Business Informatics (CBI), Amsterdam, Netherlands.

Floetgen, R. J., Mitterer, N., Urmetzer, F., & Böhm, M. (2021). *Platform Ecosystem Structures: Leveraging Platform-based Technology and the Finance Ecosystem for the New Normal*. PACIS 2021 Proceedings, Online.

Floetgen, R. J., Strauss, J., Weking, J., Hein, A., Urmetzer, F., Böhm, M., & Krcmar, H. (2021). Introducing Platform Ecosystem Resilience: Leveraging Mobility Platforms and Their Ecosystems for the New Normal During COVID-19. *European Journal of Information Systems, 30*(3), 1-18. https://doi.org/10.1080/0960085x.2021.1884009

Fontana, F., D'Arcangelo, D., Di Domenico, M., & Vannicelli, D. (2007). *MATRIX MULTI-PLATFORM an e-Learning Environment to Manage Distributed Platforms and Heterogeneous Contents*. E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, Quebec, Canada.

Foss, N. J., & Saebi, T. (2017). Fifteen Years of Research on Business Model Innovation. *Journal of Management, 43*(1), 200-227. https://doi.org/10.1177/0149206316675927

Friend, C. (2004). *Social Contract Theory*. Internet Encyclopedia of Philosophy.

Fruhwirth, M., Breitfuss, G., & Pammer-Schindler, V. (2020). *The Data Product Canvas: A Visual Collaborative Tool for Designing Data-Driven Business Models*. 33rd Bled eConference—Enabling Technology for a Sustainable Society, Bled, Slovenia.

Fruhwirth, M., Rachinger, M., & Prlja, E. (2020). *Discovering Business Models of Data Marketplaces*. Proceedings of the 53rd Hawaii International Conference on System Sciences, Honolulu, Hawaii, the United States.

Furness, M., & Trautner, B. (2020). Reconstituting Social Contracts in Conflict-Affected Mena Countries: Whither Iraq and Libya? *World Development, 135*(1), 1-12. https://doi.org/10.1016/j.worlddev.2020.105085

Gantz, J., & Reinsel, D. (2012). The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East. *IDC iView: IDC Analyze the future*, 1-16.

Garbuio, M., & Lin, N. (2019). Artificial Intelligence as a Growth Engine for Health Care Startups: Emerging Business Models. *California Management Review, 61*(2), 59-83. https://doi.org/10.1177/00081256188119

Gelhaar, J., & Otto, B. (2020). *Challenges in the Emergence of Data Ecosystems*. PACIS 2020 Proceedings, Dubai, the United Arab Emirates.

Gentry, C. (2009). *Fully Homomorphic Encryption Using Ideal Lattices*. Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, New York, New York, the United States.

Gerald, P., & Suzanne, W. (2010). Consumer Perception of Web Site Security Attributes. *Journal of Information Privacy and Security, 6*(4), 3-27. https://doi.org/10.1080/15536548.2010.10855897

Ghazawneh, A., & Henfridsson, O. (2010). *Governing Third-Party Development Through Platform Boundary Resources*. ICIS 2010 Proceedings, St. Louis, Missouri, the United States.

Ghazawneh, A., & Henfridsson, O. (2013). Balancing Platform Control and External Contribution in Third-Party Development: The Boundary Resources Model. *Information Systems Journal, 23*(2), 173-192. https://doi.org/10.1111/j.1365-2575.2012.00406.x

Gil, G., Arnaiz, A., Diez, F. J., & Higuero, M. V. (2020). *Evaluation Methodology for Distributed Data Usage Control Solutions*. 2020 Global Internet of Things Summit (GIoTS), Dublin, Ireland.

Glaser, K. (2020). *Governance of Internal Complementors in Platform Ecosystems*. ICIS 2020 Proceedings, Hyderabad, India.

Glennon, M., Kolding, M., Sundbland, M., Croce, C. L., Micheletti, G., Raczko, N., Freitas, L., Moise, C., & Osimo, D. (2023). *D2.4 Second Report on Facts and Figures*. (European DATA Market Study 2021–2023).

Glesne, C. (2016). *Becoming Qualitative Researchers: An Introduction* (Fifth ed.). Pearson Boston.

Goldbach, T., Benlian, A., & Buxmann, P. (2018). Differential Effects of Formal and Self-Control in Mobile Platform Ecosystems: Multi-Method Findings on Third-Party Developers' Continuance Intentions and Application Quality. *Information & Management, 55*(3), 271-284. https://doi.org/10.1016/j.im.2017.07.003

Goldbach, T., Kemper, V., & Benlian, A. (2014). *Mobile Application Quality and Platform Stickiness under Formal vs. Self-Control — Evidence from an Experimental Study*. ICIS 2014 Proceedings, Auckland, New Zealand.

Goldkuhl, G. (2012). Pragmatism vs Interpretivism in Qualitative Information Systems Research. *European Journal of Information Systems, 21*(2), 135-146. https://doi.org/10.1057/ejis.2011.54

Gong, Y., van Engelenburg, S., & Janssen, M. (2021). A Reference Architecture for Blockchain-Based Crowdsourcing Platforms. *Journal of Theoretical and Applied Electronic Commerce Research, 16*(4), 937-958. https://doi.org/10.3390/jtaer16040053

Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain Systems. *Artificial Intelligence and Law, 26*, 377-409. https://doi.org/10.1007/s10506-018-9223-3

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS quarterly, 37*(2), 337-355.

Gregor, S., Kruse, L. C., & Seidel, S. (2020). The Anatomy of a Design Principle. *Journal of the Association for Information Systems, 21*(6), 1622-1652. https://doi.org/10.17705/1jais.00649

Gu, H., Zhang, T., Lu, C., & Song, X. (2021). Assessing Trust and Risk Perceptions in the Sharing Economy: An Empirical Study. *Journal of Management Studies, 58*(4), 1002-1032. https://doi.org/10.1111/joms.12678

Guo, Y., Bao, Y., Stuart, B. J., & Le-Nguyen, K. (2018). To Sell or Not to Sell: Exploring Sellers' Trust and Risk of Chargeback Fraud in Cross-Border Electronic Commerce. *Information Systems Journal, 28*(2), 359-383. https://doi.org/10.1111/isj.12144

Gupta, A., Lanteigne, C., & Kingsley, S. (2020). SECure: A Social and Environmental Certificate for AI Systems. *arXiv preprint arXiv:2006.06217*.

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R Package and Shiny App for Producing PRISMA 2020-Compliant Flow Diagrams, With Interactivity for Optimised Digital Transparency and Open Synthesis. *Campbell Systematic Reviews, 18*(2), 1-12. https://doi.org/https://doi.org/10.1002/cl2.1230

Hai, X., & Liu, J. (2022, 2022). *PPDS: Privacy Preserving Data Sharing for AI applications Based on Smart Contracts*. 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, the United States.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications.

Hann, I.-H., Roberts, J., Slaughter, S., & Fielding, R. (2002). *Economic Incentives for Participating in Open Source Software Projects*. ICIS 2002 Proceedings, Barcelona, Spain.

Hart, P., & Saunders, C. (1997). Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange. *Organization Science, 8*(1), 23-42. https://doi.org/10.1287/orsc.8.1.23

Hartono, E., Holsapple, C. W., Kim, K.-Y., Na, K.-S., & Simpson, J. T. (2014). Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Respecification and Validation. *Decision Support Systems, 62*, 11-21. https://doi.org/10.1016/j.dss.2014.02.006

Hasan, M. R., & Legner, C. (2023). *Understanding Data Products: Motivations, Definition, and Categories*. ECIS 2023 Research Papers, Kristiansand, Norway.

Hauser, D. J., Ellsworth, P. C., & Gonzalez, R. (2018). Are Manipulation Checks Necessary? *Frontiers in psychology, 9*, 998. https://doi.org/10.3389/fpsyg.2018.00998

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The Limits of Trust-Free Systems: A Literature Review on Blockchain Technology and Trust in the Sharing Economy. *Electronic Commerce Research and Applications, 29*, 50-63. https://doi.org/10.1016/j.elerap.2018.03.005

He, Y., Chen, Y. C., Guo, Z. Y., Tso, R., & Ye, S. (2019). *SCDP: Smart Contract-based Decentralized Privacy System for Securing Data Ownership Management*. 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan.

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital Platform Ecosystems. *Electronic Markets, 30*(1), 87-98. https://doi.org/10.1007/s12525-019-00377-4

Hein, A., Setzke, D. S., Hermes, S., & Weking, J. (2019). *The Influence of Digital Affordances and Generativity on Digital Platform Leadership*. ICIS 2019 Proceedings, Munich, Germany.

Hellmeier, M., Pampus, J., Qarawlus, H., & Howar, F. (2023). *Implementing Data Sovereignty: Requirements & Challenges from Practice*. Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy.

Hellmeier, M., & von Scherenberg, F. (2023). *A Delimitation of Data Sovereignty from Digital and Technological Sovereignty*. ECIS 2023 Research Papers, Kristiansand, Norway.

Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015, 2015/09/01/). A Taxonomy for Privacy Enhancing Technologies. *Computers & Security, 53*(1), 1-17. https://doi.org/10.1016/j.cose.2015.05.002

Hevner, A., & Chatterjee, S. (2010). Design Science Research in Information Systems. In *Design research in information systems* (pp. 9-22). Springer.

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian journal of information systems, 19*(2), 87-92.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS quarterly, 28*(1), 75-105. https://doi.org/10.2307/25148625

Hewage, U. (2018). *Factors Influencing the Effective Information Sharing in Sri Lankan Export-Led Manufacturing Supply Chains*. 2018 International Conference on Production and Operations Management Society (POMS), Rio de Janeiro, Brazil.

Hickey, S. (2011). The Politics of Social Protection: What Do We Get From a 'Social Contract' Approach? *Canadian Journal of Development Studies/Revue canadienne d'études du développement, 32*(4), 426-438. https://doi.org/10.1080/02255189.2011.647447

Hilbolling, S., Berends, H., Deken, F., & Tuertscher, P. (2020). Complementors as Connectors: Managing Open Innovation Around Digital Product Platforms. *R&D Management, 50*(1), 18-30. https://doi.org/10.1111/radm.12371

Hinsley, F. H. (1986). *Sovereignty* (Second ed.). Cambridge University Press.

Hochwarter, W. A., Witt, L., & Kacmar, K. M. (2000). Perceptions of Organizational Politics as a Moderator of the Relationship Between Consciousness and Job Performance. *Journal of applied psychology, 85*(3), 472-478. https://doi.org/10.1037/0021-9010.85.3.472

Hodapp, D., & Hanelt, A. (2022). Interoperability in the Era of Digital Innovation: An Information Systems Research Agenda. *Journal of Information Technology, 37*(4), 407-427. https://doi.org/10.1177/02683962211064304

Hofman, W., Rukanova, B., Tan, Y. H., Bharosa, N., Ubacht, J., & Rietveld, E. (2024). Digital Infrastructures for Compliance Monitoring of Circular Economy: Requirements for Interoperable Data Spaces. In K. Arai (Ed.), *Advances in Information and Communication* (pp. 332-351). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-54053-0_24

Holler, M., Vogt, H., & Barth, L. (2019). *Exploring the Willingness-To-Share Data of Digitized Products in B2B Manufacturing Industries*. 32nd Bled eConference-Humanizing Technology for a Sustainable Society, Bled, Slovenia.

Hong, S., & Kim, H. (2020). VaultPoint: A Blockchain-Based SSI Model that Complies with OAuth 2.0. *Electronics*, *9*(8), 1-20. https://doi.org/10.3390/electronics9081231

Hong, Y., & Pavlou, P. (2012). *An Empirical Investigation on Provider Pricing in Online Crowdsourcing Markets for It Services*. ICIS 2012 Proceedings, Orlando, Florida, the United States.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What It Is and What It Means. *Information and Communications Technology Law*, *28*(1), 65-98. https://doi.org/10.1080/13600834.2019.1573501

Houde, S., & Hill, C. (1997). What do Prototypes Prototype? In (pp. 367-381). Elsevier. https://doi.org/10.1016/b978-044481862-1.50082-0

Hu, M. (2020). Cambridge Analytica's Black Box. *Big Data & Society*, *7*(2), 1-6. https://doi.org/10.1177/2053951720938091

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The Effects of Web Assurance Seals on Consumers' Initial Trust in an Online Vendor: A Functional Perspective. *Decision Support Systems*, *48*(2), 407-418. https://doi.org/10.1016/j.dss.2009.10.004

Huang, B., Gou, H., Liu, W., Li, Y., & Xie, M. (2002). A Framework for Virtual Enterprise Control With the Holonic Manufacturing Paradigm. *Computers in Industry*, *49*(3), 299-310. https://doi.org/10.1016/S0166-3615(02)00098-2

Huang, L.-T., Farn, C.-K., & Yin, K.-L. (2005). *On Initial Trust Building for Ecommerce: Revisiting From the Perspective of Signal Theory and Trust Transference*. ECIS 2005 Proceedings, Regensburg, Germany.

Hummel, P., Braun, M., Augsberg, S., & Dabrock, P. (2018). Sovereignty and Data Sharing. *ITU Journal: ICT Discoveries*, *2*.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data Sovereignty: A Review. *Big Data & Society*, *8*(1), 1–17. https://doi.org/10.1177/2053951720982012

Hutterer, A. (2023). *Introduction of Data Spaces–Status and Recommendations for Action*. Proceedings of The International Conference on Electronic Business, Chiayi, Taiwan.

Irion, K. (2012). Government Cloud Computing and National Data Sovereignty. *Policy &amp; Internet*, *4*(3-4), 40-71. https://doi.org/10.1002/poi3.10

Jagals, M., Karger, E., Ahlemann, F., & Brée, T. (2021). Enhancing Inter-Organizational Data Governance via Blockchain–Shaping Scopes and Research Avenues. Forty-Second International Conference on Information Systems, Texas, Texas, the United States.

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

Jaworski, B. J. (1988). Toward a Theory of Marketing Control: Environmental Context, Control Types, and Consequences. *Journal of marketing*, *52*(3), 23-39. https://doi.org/10.1177/002224298805200303

Jiang, D., Jiang, L. D., Jackie Jr, J., Grover, V., & Sun, H. (2022). Everything Old Can Be New Again: Reinvigorating Theory Borrowing for the Digital Age. *MIS quarterly*, *46*(4), 1833-1850.

Jung, C., & Dörr, J. (2022). Data Usage Control. In B. Otto, M. ten Hompel, & S. Wrobel (Eds.), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (pp. 129-146). Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_8

Jussen, I., Schweihoff, J., Dahms, V., Möller, F., & Otto, B. (2023). *Data Sharing Fundamentals: Characteristics and Definition*. Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS), Honolulu, Hawaii, the United States.

Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the Blockchain Technology Adoption in Supply Chains-Indian Context. *International journal of production research*, *57*(7), 2009-2033. https://doi.org/10.1080/00207543.2018.1518610

Kampling, H., Klesel, M., & Niehaves, B. (2016). *On Experiments in Design Science Research and Theory Development: A Literature Review*. 49th Hawaii International Conference on System Sciences (HICSS), Honolulu, Hawaii, the United States.

Kang, Y., & Zhou, L. (2019). Helpfulness Assessment of Online Reviews. *ACM TRANSACTIONS ON MANAGEMENT INFORMATION SYSTEMS*, *10*(3), 1-18. https://doi.org/10.1145/3365538

Kannengießer, N., Lins, S., Sander, C., Winter, K., Frey, H., & Sunyaev, A. (2022). Challenges and Common Solutions in Smart Contract Development. *IEEE Transactions on Software Engineering*, *48*(11), 4291-4318. https://doi.org/10.1109/TSE.2021.3116808

Karger, E. (2020). Combining Blockchain and Artificial Intelligence-Literature Review and State of the Art. ICIS 2020 Proceedings, Hyderabad, India.

Karger, E., Jagals, M., & Ahlemann, F. (2021). Blockchain for AI Data–State of the Art and Open Research. Forty-Second International Conference on Information Systems, Texas, Texas, the United States.

Karhu, K., Gustafsson, R., & Lyytinen, K. (2018). Exploiting and Defending Open Digital Platforms with Boundary Resources: Android's Five Platform Forks. *Information Systems Research*, *29*(2), 479-497. https://doi.org/10.1287/isre.2018.0786

Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015, 2015/02/01). Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks. *European Journal of Human Genetics*, *23*(2), 141-146. https://doi.org/10.1038/ejhg.2014.71

Ke, W., & Wei, K. K. (2007). Factors Affecting Trading Partners' Knowledge Sharing: Using the Lens of Transaction Cost Economics and Socio-Political Theories. *Electronic Commerce Research and Applications*, *6*(3), 297-308. https://doi.org/10.1016/j.elerap.2006.06.006

Kembro, J., Näslund, D., & Olhager, J. (2017). Information Sharing Across Multiple Supply Chain Tiers: A Delphi Study on Antecedents. *International Journal of Production Economics*, *193*, 77-86. https://doi.org/10.1016/j.ijpe.2017.06.032

Kim, G., & Koo, H. (2016). The Causal Relationship Between Risk and Trust in the Online Marketplace: A Bidirectional Perspective. *Computers in Human Behavior*, *55*, 1020-1029. https://doi.org/10.1016/j.chb.2015.11.005

Kim, H.-W., Xu, Y., & Koh, J. (2004). A Comparison of Online Trust Building Factors Between Potential Customers and Repeat Customers. *Journal of the Association for Information Systems*, *5*(10), 13. https://doi.org/10.17705/1jais.00056

Kim, K., & Kim, J. (2011). Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust. *Journal of Interactive Marketing*, *25*(3), 145-158. https://doi.org/10.1016/j.intmar.2010.09.003

Kim, L. (2018). *The Lessons of Google Glass: Aligning Key Benefits and Sociability*. Human Interface and the Management of Information. Interaction, Visualization, and Analytics: 20th International Conference, HIMI 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA.

Kim, S. S. (2020). The 'Relatedness' Perspective in Compliance Management of Multi-business Firms. *Asia Pacific Journal of Information Systems*, *30*(2), 353-373. https://doi.org/10.14329/apjis.2020.30.2.353

Kirsch, L. J. (1996). The Management of Complex Tasks in Organizations: Controlling the Systems Development Process. *Organization Science*, *7*(1), 1-21. https://doi.org/10.1287/orsc.7.1.1

Kirsch, L. S. (1997). Portfolios of Control Modes and IS Project Management. *Information Systems Research*, *8*(3), 215-239. https://doi.org/10.1287/isre.8.3.215

Klang, D., Wallnöfer, M., & Hacklin, F. (2014). The Business Model Paradox: A Systematic Review and Exploration of Antecedents. *International Journal of Management Reviews*, *16*(4), 454-478. https://doi.org/10.1111/ijmr.12030

Klein, A., Sørensen, C., de Freitas, A. S., Pedron, C. D., & Elaluf-Calderwood, S. (2020). Understanding Controversies in Digital Platform Innovation Processes: The Google Glass Case. *Technological Forecasting and Social Change*, *152*, 119883.

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS quarterly*, 67-93.

Knoppers, B. M., Harris, J. R., Tassé, A. M., Budin-Ljøsne, I., Kaye, J., Deschênes, M., & Zawati, M. n. H. (2011). Towards a Data Sharing Code of Conduct for International Genomic Research. *Genome Medicine*, *3*(46), 1-4. https://doi.org/10.1186/gm262

Komninos, N., Kakderi, C., Collado, A., Papadaki, I., & Panori, A. (2021). Digital Transformation of City Ecosystems: Platforms Shaping Engagement and Externalities across Vertical Markets. *Journal of Urban Technology*, *28*(1-2), 93-114. https://doi.org/10.1080/10630732.2020.1805712

Koukoularis, E., Markopoulos, V., & Voutsinas, N. (2023). *A Self-Sovereign Way to Exchange Educational Credentials*. Proceedings of European University Information Systems, Vigo, Spain.

Koutroumpis, P., Leiponen, A., & Thomas, L. (2019). The nature of data. *Innovation and Entrepreneurship Working Papers, Imperial College Business School: London, UK*.

Koutroumpis, P., Leiponen, A., & Thomas, L. D. W. (2020). Markets for Data. *Industrial and Corporate Change*, *29*(3), 645-660. https://doi.org/10.1093/icc/dtaa002

Kretschmer, T., Leiponen, A., Schilling, M., & Vasudeva, G. (2022). Platform Ecosystems as Meta-Organizations: Implications for Platform Strategies. *Strategic Management Journal*, *43*(3), 405-424. https://doi.org/https://doi.org/10.1002/smj.3250

Kuechler, B., & Vaishnavi, V. (2008). On Theory Development in Design Science Research: Anatomy of a Research Project. *European Journal of Information Systems*, *17*(5), 489-504. https://doi.org/10.1057/ejis.2008.40

Lagutin, D., Bellesini, F., Bragatto, T., Cavadenti, A., Croce, V., Kortesniemi, Y., Leligou, H. C., Oikonomidis, Y., Polyzos, G. C., Raveduto, G., Santori, F., Trakadas, P., & Verber, M. (2019). *Secure Open Federation of IoT Platforms Through Interledger Technologies - The SOFIE Approach*. 2019 European Conference on

Networks and Communications (EuCNC), Valencia, Spain. https://dx.doi.org/10.1109/EuCNC.2019.8802017

Lansing, J., Benlian, A., & Sunyaev, A. (2018). "Unblackboxing" Decision Makers' Interpretations of IS Certifications in the Context of Cloud Service Certifications. *Journal of the Association for Information Systems*, *19*(11), 1064-1096. https://doi.org/10.17705/1jais.00520

Lansing, J., Schneider, S., & Sunyaev, A. (2013). *Cloud Service Certifications: Measuring Consumers' Preferences for Assurances*. ECIS 2013 Completed Research, Utrecht, The Netherlands.

Lansing, J., Siegfried, N., Sunyaev, A., & Benlian, A. (2019). Strategic Signaling Through Cloud Service Certifications: Comparing the Relative Importance of Certifications' Assurances to Companies and Consumers. *The Journal of Strategic Information Systems, 28*(4), 1-23. https://doi.org/10.1016/j.jsis.2019.101579

Lansing, J., & Sunyaev, A. (2013). Does Pain Result in Gain? Assessing Cloud Service Certifications' Effectiveness.

Lanza, J., Sanchez, L., Gomez, D., Elsaleh, T., Steinke, R., & Cirillo, F. (2016). A Proof-of-Concept for Semantically Interoperable Federation of IoT Experimentation Facilities. *Sensors*, *16*(7), 1006. https://doi.org/10.3390/s16071006

Lauf, F., Scheider, S., Bartsch, J., Herrmann, P., Radic, M., Rebbert, M., Nemat, A. T., Schlueter Langdon, C., Konrad, R., & Sunyaev, A. (2022). *Linking Data Sovereignty and Data Economy: Arising Areas of Tension*. Wirtschaftsinformatik 2022 Proceedings, Nuremberg, Germany.

Lăzăroiu, G., Neguriţă, O., Grecu, I., Grecu, G., & Mitran, P. C. (2020). Consumers' Decision-Making Process on Social Commerce Platforms: Online Trust, Perceived Risk, and Purchase Intentions. *Frontiers in Psychology*, *11*, 890. https://doi.org/10.3389/fpsyg.2020.00890

Lazouski, A., Martinelli, F., & Mori, P. (2010). Usage Control in Computer Security: A Survey. *Computer Science Review*, *4*(2), 81-99. https://doi.org/10.1016/j.cosrev.2010.02.002

Lee, S. U. (2019). *Data Governance for Platform Ecosystem* The University of New South Wales]. Kensington, Australia.

Lee, S. U., Zhu, L., & Jeffery, R. (2017). *Data Governance for Platform Ecosystems: Critical Factors and the State of Practice*. PACIS 2017 Proceedings, Langkawi Island, Malaysia.

Levy, Y., & Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science*, *9*(1), 181-212. https://doi.org/10.28945/479

Li, L., Fan, Y., Tse, M., & Lin, K.-Y. (2020). A Review of Applications in Federated Learning. *Computers & Industrial Engineering*, *149*(1), 1-15. https://doi.org/10.1016/j.cie.2020.106854

Lian, Y. (2021). *Data Rights Law 3.0*. Peter Lang Verlag. https://doi.org/10.3726/b18421

Liang, C., Peng, J., Hong, Y., & Gu, B. (2023). The Hidden Costs and Benefits of Monitoring in the Gig Economy. *Information Systems Research*, *34*(1), 297-318. https://doi.org/10.1287/isre.2022.1130

Lins, S., Becker, J.-M., Lyytinen, K., & Sunyaev, A. (2023). A Design Theory for Certification Presentations. *SIGMIS Database*, *54*(3), 75–118. https://doi.org/10.1145/3614178.3614183

Lins, S., Kromat, T., Löbbers, J., Benlian, A., & Sunyaev, A. (2020). Why Don't You Join In? A Typology of Information System Certification Adopters. *Decision Sciences*, *0*(0), 1–34. https://doi.org/10.1111/deci.12488

Lins, S., Schneider, S., Szefer, J., Ibraheem, S., & Sunyaev, A. (2019). Designing Monitoring Systems for Continuous Certification of Cloud Services: Deriving Meta-Requirements and Design Guidelines. *Communications of the Association for Information Systems*, *44*(1), 460-510. https://doi.org/10.17705/1CAIS.04425

Lins, S., & Sunyaev, A. (2017). Unblackboxing IT Certifications: A Theoretical Model Explaining IT Certification Effectiveness. ICIS 2017 Proceedings, Seoul, South Korea.

Lins, S., & Sunyaev, A. (2022). Advancing the Presentation of IS Certifications: Theory-Driven Guidelines for Designing Peripheral Cues to Increase Users' Trust Perceptions. *Behaviour & Information Technology*, *42*(13), 2255-2278. https://doi.org/10.1080/0144929x.2022.2113432

Loewe, M., Zintl, T., & Houdret, A. (2021). The Social Contract as a Tool of Analysis: Introduction to the Special Issue on "Framing the Evolution of New Social Contracts in Middle Eastern and North African Countries." *World Development*, *145*(1), 1-16. https://doi.org/10.1016/j.worlddev.2020.104982.

Lonati, S., Quiroga, B. F., Zehnder, C., & Antonakis, J. (2018). On Doing Relevant and Rigorous Experiments: Review and Recommendations. *Journal of Operations Management*, *64*, 19-40. https://doi.org/10.1016/j.jom.2018.10.003

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., & Wells, T. (2012). Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers. *Journal of the American Society for Information Science and Technology*, *63*(4), 755-776. https://doi.org/10.1002/asi.21705

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society, 1*(2), 1-13. https://doi.org/10.1177/2053951714541861

Maass, W. (2022). *Contract-based Data-Driven Decision Making in Federated Data Ecosystems*. Proceedings of the 55th Hawaii International Conference on System Sciences, Maui, Hawaii, the United States.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. *MIS Quarterly, 35*(2), 293-334. https://doi.org/10.2307/23044045

Malsa, N., Vyas, V., Gautam, J., Shaw, R. N., & Ghosh, A. (2021). Framework and Smart Contract for Blockchain Enabled Certificate Verification System Using Robotics. *Machine Learning for Robotics Applications*, 125-138.

Mannhardt, F., Koschmider, A., Baracaldo, N., Weidlich, M., & Michael, J. (2019). Privacy-Preserving Process Mining. *Business & Information Systems Engineering, 61*(5), 595-614. https://doi.org/10.1007/s12599-019-00613-3

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *The Internet of Things: Mapping the Value Beyond the Hype*. https://globaltrends.thedialogue.org/publication/the-internet-of-things-mapping-the-value-beyond-the-hype/

Mariani, M. M., Ek Styven, M., & Teulon, F. (2021). Explaining the Intention to Use Digital Personal Data Stores: An Empirical Study. *Technological Forecasting and Social Change, 166*, 120657. https://doi.org/10.1016/j.techfore.2021.120657

Martens, B., De Streel, A., Graef, I., Tombal, T., & Duch-Brown, N. (2020). *Business-To-Business Data Sharing: An Economic and Legal Analysis*. (JRC Digital Economy Working Paper 2020-05). https://joint-research-centre.ec.europa.eu/publications/business-business-data-sharing-economic-and-legal-analysis_en

Martin, M. P. (2003). Prototyping. In H. Bidgoli (Ed.), *Encyclopedia of Information Systems* (pp. 565-573). Elsevier. https://doi.org/10.1016/B0-12-227240-4/00140-4

Martin, S., Gautier, P., Turki, S., & Kotsev, A. (2021). *Establishment of Sustainable Data Ecosystems: Recommendations for the Evolution of Spatial Data Infrastructures*. https://publications.jrc.ec.europa.eu/repository/handle/JRC124148

Márton, A. (2021). Steps Toward a Digital Ecology: Ecological Principles for the Study of Digital Ecosystems. *Journal of Information Technology, 37*(3), 250-265. https://doi.org/10.1177/02683962211043222

Mascalzoni, D., Melotti, R., Pattaro, C., Pramstaller, P. P., Gögele, M., De Grandi, A., & Biasiotto, R. (2022, 2022/12/01). Ten Years of Dynamic Consent in the Chris Study: Informed Consent as a Dynamic Process. *European Journal of Human Genetics, 30*(12), 1391-1397. https://doi.org/10.1038/s41431-022-01160-4

Maschewski, J. (2023). *Patient Centricity in Is Healthcare–a Framework Proposing Enablement, Empowerment, and Engagement of Patients as Individual IS Users*. Wirtschaftsinformatik 2023 Proceedings, Paderborn, Germany.

Matar, A., Hansson, M., Slokenberga, S., Panagiotopoulos, A., Chassang, G., Tzortzatou, O., Pormeister, K., Uhlin, E., Cardone, A., & Beauvais, M. (2023). Proposal for an International Code of Conduct for Data Sharing in Genomics. *Developing World Bioethics, 23*(4), 344-357. https://doi.org/https://doi.org/10.1111/dewb.12381

Mattila, J., Seppälä, T., Valkama, P., Hukkinen, T., Främling, K., & Holmström, J. (2021). Blockchain-based deployment of product-centric information systems. *Computers in Industry, 125*(1), 1-15. https://doi.org/10.1016/j.compind.2020.103342

Mavlanova, T., Benbunan-Fich, R., & Lang, G. (2016). The Role of External and Internal Signals in E-commerce. *Decision Support Systems, 87*, 59-68. https://doi.org/10.1016/j.dss.2016.04.009

Mawere, M., & Van Stam, G. (2020, 2020). Data Sovereignty: A Perspective From Zimbabwe. WebSci ’20 Companion, Southampton, United Kingdom.

McLain, D. L., & Hackman, K. (1999). Trust, Risk, and Decision-Making in Organizational Change. *Public Administration Quarterly*, 152-176.

Meier, P., Beinke, J. H., Fitte, C., Schulte To Brinke, J., & Teuteberg, F. (2021). Generating Design Knowledge for Blockchain-Based Access Control to Personal Health Records. *Information Systems and e-Business Management, 19*(1), 13-41. https://doi.org/10.1007/s10257-020-00476-2

Melero, R., & Navarro-Molina, C. (2020). Researchers' Attitudes and Perceptions Towards Data Sharing and Data Reuse in the Field of Food Science and Technology. *Learned Publishing, 33*(2), 163-179. https://doi.org/https://doi.org/10.1002/leap.1287

Melnyk, S. A., Sroufe, R. P., & Calantone, R. J. (2003). A Model of Site-Specific Antecedents of ISO 14001 Certification. *Production and Operations Management, 12*(3), 369-385. https://doi.org/10.1111/j.1937-5956.2003.tb00209.x

Menz, N., Resetko, A., & Otto, B. (2019). *Framework for the IDS Certification Scheme 2.0*.

Menz, N., Resetko, A., & Winkel, J. (2019). *IDS Certification Explained*.

Mettler, T., Eurich, M., & Winter, R. (2014). On the Use of Experiments in Design Science Research: A Proposition of an Evaluation Framework. *Communications of the Association for Information Systems, 34*(1), 10. https://doi.org/10.17705/1CAIS.03410

Mezquita, Y., Valdeolmillos, D., González-Briones, A., Prieto, J., & Corchado, J. M. (2019). *Legal Aspects and Emerging Risks in the Use of Smart Contracts Based on Blockchain*. 14th International Conference of Knowledge Management in Organizations, Zamora, Spain.

Mik, E. (2017). Smart Contracts: Terminology, Technical Limitations and Real World Complexity. *Law, Innovation and Technology, 9*(2), 269-300. https://doi.org/10.1080/17579961.2017.1378468

Mikołajewska-Zając, K., Márton, A., & Zundel, M. (2021). Couchsurfing With Bateson: An Ecology of Digital Platforms. *Organization Studies*, 1-21. https://doi.org/10.1177/01708406211058628

Mnif, E., Mouakhar, K., & Jarboui, A. (2021). Blockchain Technology Awareness on Social Media: Insights From Twitter Analytics. *The Journal of High Technology Management Research, 32*(2), 100416.

Mohammadi, M., Hofman, W., & Tan, Y.-H. (2020). Seamless Interoperability in Logistics by Ontology Alignment. *Journal of Supply Chain Management Science, 104-117*. https://doi.org/10.18757/jscms.2020.5444

Möhring, M., Keller, B., Schmidt, R., Rippin, A.-L., Schulz, J., & Brückner, K. (2018). *Empirical Insights in the Current Development of Smart Contracts*. PACIS 2018 Proceedings, Yokohama, Japan.

Möller, F., Schoormann, T., Strobel, G., & Hansen, M. R. P. (2022). *Unveiling the Cloak: Kernel Theory Use in Design Science Research*. ICIS 2022 Proceedings, Copenhagen, Denmark.

Morlok, T. N., Constantiou, I., & Hess, T. (2018). *Gone for Better or for Worse? Exploring the Dual Nature of Ephemerality on Social Media Platforms*. ECIS 2018 Proceedings, Portsmouth, England, the United Kingdom.

Mosterd, L., Sobota, V. C. M., Van De Kaa, G., Ding, A. Y., & De Reuver, M. (2021). Context Dependent Trade-Offs Around Platform-To-Platform Openness: The Case of the Internet of Things. *Technovation, 108*(1), 1-15. https://doi.org/10.1016/j.technovation.2021.102331

Moyano, J. P., Avital, M., Bühler, M., & Schmedders, K. (2021). *Fostering Peer-to-Peer Blockchain-based Data Markets*. The 25th Pacific Asia Conference on Information Systems, Dubai, the United Arab Emirates.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A Survey on Essential Components of a Self-Sovereign Identity. *Computer Science Review, 30*(1), 80-86. https://doi.org/10.1016/j.cosrev.2018.10.002

Mukhopadhyay, S., De Reuver, M., & Bouwman, H. (2016). Effectiveness of Control Mechanisms in Mobile Platform Ecosystem. *Telematics and Informatics, 33*(3), 848-859. https://doi.org/10.1016/j.tele.2015.12.008

Munoz-Arcentales, A., López-Pernas, S., Pozo, A., Alonso, Á., Salvachúa, J., & Huecas, G. (2019). An Architecture for Providing Data Usage and Access Control in Data Sharing Ecosystems. *Procedia Computer Science, 160*(1), 590-597. https://doi.org/10.1016/j.procs.2019.11.042

Nagel, L., & Lycklama, D. (2021). *Design Principles for Data Spaces - Position Paper*. https://dx.doi.org/10.5281/zenodo.5105744

Naik, N., & Jenkins, P. (2020, 3-6 Aug 2020). *Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet Using Blockchain Technology*. 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud),

Nast, M., Rother, B., Golatowski, F., Timmermann, D., Leveling, J., Olms, C., & Nissen, C. (2020). *Work-In-Progress: Towards an International Data Spaces Connector for the Internet of Things*. 2020 16th IEEE International Conference on Factory Communication Systems (WFCS), Porto, Portugal.

Nickerson, J., Seidel, S., Yepes, G., & Berente, N. (2022). *Design Principles for Coordination in the Metaverse*. Academy of Management Annual Meeting, Seattle, Washington, the United States.

Nielsen, J. (1994). *Usability engineering*. Morgan Kaufmann.

Niles, I., & Pease, A. (2001). *Towards a Standard Upper Ontology*. Proceedings of the International Conference on Formal Ontology in Information Systems - Volume 2001, Ogunquit, Maine, the United States. https://doi.org/10.1145/505168.505170

Ofe, H., Abbas, A. E., van de Ven, M., Bergman, R., Zuiderwijk, A., Reuver, M. d., Utermark, B., Markopoulos, I., Avgousti, G., Rosam, G., Fribus, M., & Brockob, A. (2021). *D7.1 "Sustainable Business Model for TRUSTS Data Marketplace I."* https://www.trusts-data.eu/wp-content/uploads/2021/07/TRUSTS_D7.1_Sustainable-Business-Model_Taxonomies.pdf

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems, 37*(1), 43. https://doi.org/10.17705/1CAIS.03743

Opriel, S., Möller, F., Burkhardt, U., & Otto, B. (2021). *Requirements for Usage Control based Exchange of Sensitive Data in Automotive Supply Chains*. Proceedings of the 54th Hawaii International Conference on System Sciences, Honolulu, Hawaii, the United States.

Orlikowski, W. J. (1991). Integrated Information Environment or Matrix of Control? The Contradictory Implications of Information Technology. *Accounting, management and information technologies*, *1*(1), 9-42. https://doi.org/10.1016/0959-8022(91)90011-3

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, *2*(1), 1-28.

Óskarsdóttir, M., Bravo, C., Sarraute, C., Vanthienen, J., & Baesens, B. (2019). The Value of Big Data for Credit Scoring: Enhancing Financial Inclusion Using Mobile Phone Data and Social Network Analytics. *Applied Soft Computing*, *74*(1), 26-39. https://doi.org/10.1016/j.asoc.2018.10.004

Osterwalder, A., & Pigneur, Y. (2010). *Business model generation: a handbook for visionaries, game changers, and challengers*. John Wiley & Sons.

Otto, B. (2011). Organizing Data Governance: Findings from the Telecommunications Industry and Consequences for Large Service Providers. *Communications of the Association for Information Systems*, *29*(3), 45-66. https://doi.org/10.17705/1cais.02903

Otto, B. (2022). The Evolution of Data Spaces. In B. Otto, M. ten Hompel, & S. Wrobel (Eds.), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (pp. 3-15). Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_1

Otto, B., & Burmann, A. (2021, 2021/08/01). Europäische Dateninfrastrukturen. *Informatik Spektrum*, *44*(4), 283-291. https://doi.org/10.1007/s00287-021-01386-4

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

Ouchi, W. G. (1979). A Conceptual Framework for the Design of Organizational Control Mechanisms. *Management Science*, *25*(9), 833-848.

Palmié, M., Boehm, J., Friedrich, J., Parida, V., Wincent, J., Kahlert, J., Gassmann, O., & Sjödin, D. (2021). Tartups Versus Incumbents in 'Green' Industry Transformations: A Comparative Study of Business Model Archetypes in the Electrical Power Sector. *Industrial Marketing Management*, *96*, 35-49. https://doi.org/10.1016/j.indmarman.2021.04.003

Panitz, J. C., Wiener, M., & Amberg, M. (2011). *Factors Facilitating Compliance Implementation–Case Study Results From Multinational Enterprises*. ECIS 2011 Proceedings, Helsinki, Finland.

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing Information Systems Knowledge: A Typology of Literature Reviews. *Information & Management*, *52*(2), 183-199. https://doi.org/10.1016/j.im.2014.08.008

Park, J., & Sandhu, R. (2004). The UCONABC Usage Control Model. *ACM Transactions on Information and System Security*, *7*(1), 128-174. https://doi.org/10.1145/984334.984339

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, *7*(3), 101-134. https://doi.org/10.1080/10864415.2003.11044275

Pavlou, P. A., & Gefen, D. (2004). Building Effective Online Marketplaces With Institution-Based Trust. *Information Systems Research*, *15*(1), 37-59. https://doi.org/10.1287/isre.1040.0015

Pedreira, V., Barros, D., & Pinto, P. (2021). A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. *Sensors*, *21*(15), 1-21. https://doi.org/10.3390/s21155189

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Petersen, D. (2022). Automating Governance: Blockchain Delivered Governance for Business Networks. *Industrial Marketing Management*, *102*(1), 177-189. https://doi.org/10.1016/j.indmarman.2022.01.017

Pettenpohl, H., Spiekermann, M., & Both, J. R. (2022). International Data Spaces in a Nutshell. In B. Otto, M. ten Hompel, & S. Wrobel (Eds.), *Designing Data Spaces The Ecosystem Approach to Competitive Advantage* (pp. 29-40). Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_3

Piccoli, G., & Pigni, F. (2013). Harvesting External Data: The Potential of Digital Data Streams. *MIS Quarterly Executive*, *12*(1).

Pinto, P., Sousa, C., & Cardeiro, C. (2023). Data Spaces Based Approach for B2B Data Exchange: A Footwear Industry Case. *Procedia Computer Science*, *219*, 933-940.

Pitt, J., & Cranefield, S. (2021). A Conceptual Model and Metaplatform for Public Interest Technology Design. *IEEE Transactions on Technology and Society*, *2*(2), 71-82. https://doi.org/10.1109/tts.2021.3075189

Pitt, J., Rychwalska, A., Roszczynska-Kurasinska, M., & Nowak, A. (2019). Democratizing Platforms for Social Coordination. *IEEE Technology and Society Magazine*, *38*(1), 43-50. https://doi.org/10.1109/mts.2019.2894459

Pitt, S., van Meelis Lacey, M., Scaife, E., & Pitt, J. (2021). No App is an Island: Collective Action and Sustainable Development Goal-Sensitive Design. *International Journal of Interactive Multimedia & Artificial Intelligence*, *6*(5).

Plateaux, A., Lacharme, P., Rosenberger, C., & Murty, K. (2013). *A Contactless E-health Information System With Privacy*. 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), Sardinia, Italy.

Pon, B., Seppälä, T., & Kenney, M. (2015). One Ring to Unite Them All: Convergence, the Smartphone, and the Cloud. *Journal of Industry, Competition and Trade*, *15*(1), 21-33. https://doi.org/10.1007/s10842-014-0189-x

Ponte, E. B., Carvajal-Trujillo, E., & Escobar-Rodríguez, T. (2015). Influence of Trust and Perceived Value on the Intention to Purchase Travel Online: Integrating the Effects of Assurance on Trust Antecedents. *Tourism Management*, *47*(1), 286-302. https://doi.org/10.1016/j.tourman.2014.10.009

Porter, M. (2001). Strategy and the Internet. *Harvard Business Review*, *79*(3), 62-78.

Precht, H., & Gómez, J. M. (2021, 2021//). *Towards GDPR Enforcing Blockchain Systems*. Innovation Through Information Systems, Cham.

Pumplun, L., Peters, F., Gawlitza, J. F., & Buxmann, P. (2023). Bringing Machine Learning Systems into Clinical Practice: A Design Science Approach to Explainable Machine Learning-Based Clinical Decision Support Systems. *Journal of the Association for Information Systems*, *24*(4), 953-979. https://doi.org/10.17705/1jais.00820

Rainie, S. C., Kukutai, T., Walter, M., Figueroa-Rodríguez, O. L., Walker, J., & Axelsson, P. (2019). Indigenous Data Sovereignty. In *The State of Open Data: Histories and Horizons*. African Minds and the International Development Research Centre (IDRC).

Rammert, M., Kindermann, B., & Strese, S. (2023). *Get the Crypto Crowd Going: Evaluating the Signaling Effect of Motivational Cues on Crowd Involvement*. ICIS 2023 Proceedings, Hyderabad, India.

Rantanen, M. M., & Koskinen, J. (2020a). *Humans of the European Data Economy Ecosystem - What Do They Demand from a Fair Data Economy?* Human-Centric Computing in a Data-Driven Society, Cham.

Rantanen, M. M., & Koskinen, J. (2020b). 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.

Reimsbach-Kounatze, C. (2021). Enhancing Access to and Sharing of Data: Striking the Balance Between Openness and Control Over Data. In *Data Access, Consumer Interests and Public Welfare* (pp. 25-68). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748924999-25

Reinartz, W., Wiegand, N., & Imschloss, M. (2019). The Impact of Digital Transformation on the Retailing Value Chain. *International Journal of Research in Marketing*, *36*(3), 350-366. https://doi.org/10.1016/j.ijresmar.2018.12.002

Reyman, J. (2013). User Data on the Social Web: Authorship, Agency, and Appropriation. *College English*, *75*(5), 513-533.

Richter, H., & Slowinski, P. R. (2019). The Data Sharing Economy: On the Emergence of New Intermediaries. *IIC - International Review of Intellectual Property and Competition Law*, *50*(1), 4-29. https://doi.org/10.1007/s40319-018-00777-7

Riss, U. V., Maier, E., & Doerk, M. (2022). *Perceived Risks of the Data Economy: Autonomy and the Case of Voice Assistants*. Proceedings of the ETHICOMP, Turku, Finland.

Rosillo-Díaz, E., Blanco-Encomienda, F. J., & Crespo-Almendros, E. (2019). A Cross-Cultural Analysis of Perceived Product Quality, Perceived Risk and Purchase Intention in E-commerce Platforms. *Journal of Enterprise Information Management*, *33*(1), 139-160. https://doi.org/10.1108/jeim-06-2019-0150

Ruparelia, N. B. (2016). *Cloud Computing*. The MIT Press.

Sabt, M., Achemlal, M., & Bouabdallah, A. (2015). *Trusted Execution Environment: What It is, and What It is Not*. 2015 IEEE Trustcom/BigDataSE/Ispa, Helsinki, Finland.

Sahoo, S., & Halder, R. (2021). Traceability and Ownership Claim of Data on Big Data Marketplace Using Blockchain Technology. *Journal of Information and Telecommunication*, *5*(1), 35-61. https://doi.org/10.1080/24751839.2020.1819634

Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2021). A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. *IEEE Internet of Things Journal*, *8*(7), 5914-5925. https://doi.org/10.1109/JIOT.2020.3032997

Saldaña, J. (2016). *The Coding Manual for Qualitative Researchers* (Third edition ed.). Sage Publications Los Angeles, California.

Salviotti, G., De Rossi, L. M., & Abbatemarco, N. (2018). *A Structured Framework to Assess the Business Application Landscape of Blockchain Technologies*. Proceedings of the 51st Hawaii International Conference on System Sciences, Hawaii, HI, the United States.

Sánchez-Guerrero, R., Mendoza, F. A., Díaz-Sánchez, D., Cabarcos, P. A., & López, A. M. (2017). Collaborative eHealth Meets Security: Privacy-Enhancing Patient Profile Management. *IEEE Journal of Biomedical and Health Informatics, 21*(6), 1741-1749. https://doi.org/10.1109/JBHI.2017.2655419

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), Limerick, Ireland.

Saunders, C., Benlian, A., Henfridsson, O., & Wiener, M. (2020). MIS Quarterly Research Curation: IS Control & Governance. *MIS Quarterly*.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (Eighth edition ed.). Pearson Harlow, United Kingdom.

Scaria, E., Berghmans, A., Pont, M., Arnaut, C., & Leconte, S. (2018). *Study on Data Sharing Between Companies in Europe*. (A study prepared for the European Commission Directorate-General for Communications Networks, Content and Technology). https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en

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

Schäfer, F., Rosen, J., Zimmermann, C., & Wortmann, F. (2023). *Unleashing The Potential of Data Ecosystems: Establishing Digital Trust through Trust-enhancing Technologies*. ECIS 2023 Research Papers, Kristiansand, Norway.

Scheider, S., Lauf, F., & Geller, S. (2023). *Data Sovereign Humans and the Information Economy: Towards Design Principles for Human Centric B2C Data Ecosystems*. Proceedings of the 56th Hawaii International Conference on System Sciences, Honolulu, Hawaii, the United States.

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*(1), 577–595. https://doi.org/10.1007/s12599-023-00816-9

Schilling, R., Aier, S., & Winter, R. (2019). *Designing an Artifact for Informal Control in Enterprise Architecture Management*. ICIS 2019 Proceedings, Munich, Germany.

Schinle, M., Erler, C., & Stork, W. (2021). *Data Sovereignty in Data Donation Cycles-Requirements and Enabling Technologies for the Data-driven Development of Health Applications*. Proceedings of the 54th Hawaii International Conference on System Sciences, Kauai, Hawaii, the United States.

Schlehahn, E., Murmann, P., Karegar, F., & Fischer-Hübner, S. (2020). Opportunities and Challenges of Dynamic Consent in Commercial Big Data Analytics. In M. Friedewald, M. Önen, E. Lievens, S. Krenn, & S. Fricker (Eds.), *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers* (pp. 29-44). Springer International Publishing. https://doi.org/10.1007/978-3-030-42504-3_3

Schmidt, K., Munilla Garrido, G., Mühle, A., & Meinel, C. (2022). *Mitigating Sovereign Data Exchange Challenges: A Mapping to Apply Privacy-and Authenticity-Enhancing Technologies*. International Conference on Trust and Privacy in Digital Business, Vienna, Austria.

Schöbel, S. M., & Leimeister, J. M. (2023). Metaverse Platform Ecosystems. *Electronic Markets, 33*(1). https://doi.org/10.1007/s12525-023-00623-w

Schomm, F., Stahl, F., & Vossen, G. (2013). Marketplaces for Data: An Initial Survey. *ACM SIGMOD Record, 42*(1), 15-26. https://doi.org/10.1145/2481528.2481532

Schumann, F., & Döring, M. (2022). *The Impact of Digital Transformation on Top Management Teams: A Systematic Literature Review and Analysis on the Role Delineation of the Chief Digital Officer and the Chief Information Officer*. PACIS 2022 Proceedings, Online.

Segars, A. H., & Grover, V. (1999). Profiles of Strategic Information Systems Planning. *Information Systems Research, 10*(3), 199-232.

Sekaran, U., & Bougie, R. (2016). *Research Methods for Business: A Skill Building Approach*. John Wiley & Sons.

Sestino, A., Kahlawi, A., & De Mauro, A. (2023). Decoding the Data Economy: A Literature Review of Its Impact on Business, Society and Digital Transformation. *European Journal of Innovation Management, ahead-of-print*(ahead-of-print), 1-26. https://doi.org/10.1108/EJIM-01-2023-0078

Shah, M. H., Peikari, H. R., & Yasin, N. M. (2014). The Determinants of Individuals' Perceived E-security: Evidence From Malaysia. *International Journal of Information Management, 34*(1), 48-57. https://doi.org/10.1016/j.ijinfomgt.2013.10.001

Shah, N., Coathup, V., Teare, H., Forgie, I., Giordano, G. N., Hansen, T. H., Groeneveld, L., Hudson, M., Pearson, E., Ruetten, H., & Kaye, J. (2019). Motivations for Data Sharing—Views of Research Participants From Four European Countries: A DIRECT study. *European Journal of Human Genetics, 27*(5), 721-729. https://doi.org/10.1038/s41431-019-0344-2

Shanks, G., Tansley, E., Nuredini, J., Tobin, D., & Weber, R. (2008). Representing Part-Whole Relations in Conceptual Modeling: An Empirical Evaluation. *MIS Quarterly*, 553-573.

Sharma, R., Wingreen, S., Kshetri, N., & Hewa, T. (2019). *Design principles for use cases of blockchain in food supply chains*. 25th Americas Conference on Information Systems (AMCIS 2019), Cancun, Mexico.

Shin, S. I., Kim, J. B., Hall, D., & Lang, T. (2019). *What Information Propagates Among the Public When an Initial Coin Offering (ICO) Is Initiated? A Theory-Driven Approach*. Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, Hawaii, the United States.

Shirokova, G., Osiyevskyy, O., Bogatyreva, K., Edelman, L. F., & Manolova, T. S. (2022). Moving from Intentions to Actions in Youth Entrepreneurship: An Institutional Perspective. *Entrepreneurship Research Journal, 12*(1), 25-69. https://doi.org/10.1515/erj-2019-0201

Siddiqui, M. S., Syed, T. A., Nadeem, A., Nawaz, W., & Alkhodre, A. (2022). Permission and Usage Control for Virtual Tourism using Blockchain-based Smart Contracts. *International Journal of Advanced Computer Science and Applications, 13*(11), 231-240. https://doi.org/10.14569/IJACSA.2022.0131126

Silva, D., Guerreiro, S., & Sousa, P. (2019). Decentralized Enforcement of Business Process Control Using Blockchain. In (pp. 69-87). Springer International Publishing. https://doi.org/10.1007/978-3-030-06097-8_5

Skaggs, B. C., & Snow, C. C. (2004). The Strategic Signaling of Capabilities by Service Firms in Different Information Asymmetry Environments. *Strategic Organization, 2*(3), 271-291. https://doi.org/10.1177/1476127004045253

Sobhy, H. (2021). The Lived Social Contract In Schools: From Protection to the Production of Hegemony. *World Development, 137*(1), 1-15. https://doi.org/10.1016/j.worlddev.2020.104986

Søgaard, J. S. (2021). A Blockchain-Enabled Platform for VAT Settlement. *International Journal of Accounting Information Systems, 40*(1), 1-18. https://doi.org/10.1016/j.accinf.2021.100502

Spiekermann, M. (2019). Data Marketplaces: Trends and Monetisation of Data Goods. *Intereconomics, 54*(4), 208-216. https://doi.org/10.1007/s10272-019-0826-z

Srivastava, S., & Thompson, T. (2012). Contract Performance in Offshore Systems Development: Role of Control Mechanisms. *Journal of Management Information Systems, 29*(1), 115-158. https://doi.org/10.2753/mis0742-1222290104

Srivastava, S. C., & Teo, T. S. (2012). *Aligning Control Structures With Control Processes For Effective Offshore Contract Performance*. PACIS 2012 Proceedings, Ho Chi Minh City, Vietnam.

Stachon, M., Möller, F., Guggenberger, T., Tomczyk, M., & Henning, J.-L. (2023). *Understanding Data Trusts*. ECIS 2023 Research-in-Progress Papers, Kristiansand, Norway.

Stahl, B. C. (2007). Positivism or Non-Positivism — Tertium Non Datur. In *Ontologies: A Handbook of Principles, Concepts and Applications in Information Systems* (pp. 115-142). Springer US. https://doi.org/10.1007/978-0-387-37022-4_5

Stahl, F., Schomm, F., Vomfell, L., & Vossen, G. (2017). Marketplaces for Digital Data: Quo Vadis? *Computer and Information Science, 10*(4), 22. https://doi.org/10.5539/cis.v10n4p22

Stahl, F., Schomm, F., & Vossen, G. (2014). *Data Marketplaces: An Emerging Species*. IOS Press.

Stahl, F., Schomm, F., Vossen, G., & Vomfell, L. (2016). A classification framework for data marketplaces. *Vietnam Journal of Computer Science, 3*(3), 137-143. https://doi.org/10.1007/s40595-016-0064-2

Stahl, F., & Vossen, G. (2017). Name Your Own Price on Data Marketplaces. *Informatica, 28*(1), 155-180. https://doi.org/10.15388/Informatica.2017.124

Staub, N., Haki, K., Aier, S., & Winter, R. (2022). Governance Mechanisms in Digital Platform Ecosystems: Addressing the Generativity-Control Tension. *Communications of the Association for Information Systems, 51*(1), 906 – 939. https://doi.org/10.17705/1CAIS.05137

Sturm, B., Lansing, J., & Sunyaev, A. (2014). *Moving in the Right Direction?: Mapping Literature on Cloud Service Certifications' Outcomes With Practitioners' Perceptions*. Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel.

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy of Management Review, 20*(3), 571-610. https://doi.org/10.5465/amr.1995.9508080331

Sultana, S. A., Rupa, C., Malleswari, R. P., & Gadekallu, T. R. (2023). IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field. *Information, 14*(8), 446. https://doi.org/10.3390/info14080446

Sun, J., Xu, D., & Karanasios, S. (2023). *How Parts Connect to Whole in Building Digital Generativity in Digital Platform Ecosystems*. ECIS 2023 Research-in-Progress Papers, Kristiansand, Norway. https://aisel.aisnet.org/ecis2023_rip/37

Sun, Y., & Li, Y. (2021). The Impact of Risk-Aware Consumer Trust on Cb E-commerce Platforms and Purchase Intention. *Journal of Global Information Management (JGIM), 30*(3), 1-13. https://doi.org/10.4018/JGIM.20220701.oa10

Susha, I., Janssen, M., & Verhulst, S. (2017). Data Collaboratives as “Bazaars”? A Review of Coordination Problems and Mechanisms to Match Demand for Data With Supply. *Transforming Government: People, Process and Policy, 11*(1), 157-172. https://doi.org/10.1108/TG-01-2017-0007

Tan, K.-L., Chi, C.-H., & Lam, K.-Y. (2023). Survey on Digital Sovereignty and Identity: From Digitization to Digitalization. *ACM Computing Surveys, 56*(3), 1-36. https://doi.org/10.1145/3616400

Tao, Y., Yang, S., & Ge, H. (2022). *Comparative Study on Data Sovereignty Guarantee Technology*. 2022 IEEE 13th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Beijing, China.

Tapia, A. H., Blodgett, B., Ocker, R., & Rosson, M. B. (2011). *Ownership and Control Over Data Resources in a Virtual Scientific Collaboratory*. Proceedings of International Association for the Development of the Information Society: IADIS 2011, Shanghai, China.

Tateishi, T., Yoshihama, S., Sato, N., & Saito, S. (2019). Automatic Smart Contract Generation Using Controlled Natural Language and Template. *IBM Journal of Research and Development, 63*(2/3), 6:1-6:12. https://doi.org/10.1147/JRD.2019.2900643

Taylor, R. D. (2020). “Data Localization”: The Internet in the Balance. *Telecommunications Policy, 44*(8), 1-15. https://doi.org/10.1016/j.telpol.2020.102003

Teece, D. J. (2010). Business Models, Business Strategy and Innovation. *Long Range Planning, 43*(2-3), 172-194. https://doi.org/10.1016/j.lrp.2009.07.003

Thapa, D., & Haj-Bolouri, A. (2023). *Demystifying Philosophy for Information Systems Researcher*. 2023 Americas Conference on Information Systems, Panama City, Panama.

Thies, F., Wessel, M., & Benlian, A. (2018). Network effects on crowdfunding platforms: Exploring the implications of relaxing input control. *Information Systems Journal, 28*(6), 1239-1262. https://doi.org/10.1111/isj.12194

Tiwana, A. (2013). *Platform Ecosystems: Aligning Architecture, Governance, and Strategy*. Newnes.

Tiwana, A., & Keil, M. (2009). Control in Internal and Outsourced Software Projects. *Journal of Management Information Systems, 26*(3), 9-44. https://doi.org/10.2753/mis0742-1222260301

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research Commentary—Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. *Information Systems Research, 21*(4), 675-687. https://doi.org/10.1287/isre.1100.0323

Tuler De Oliveira, M., Reis, L. H. A., Verginadis, Y., Mattos, D. M. F., & Olabarriaga, S. D. (2022). SmartAccess: Attribute-Based Access Control System for Medical Records Based on Smart Contracts. *IEEE Access, 10*(1), 117836-117854. https://doi.org/10.1109/access.2022.3217201

Ulrich, D., & Alt, R. (2021). Social Networking Platforms to Close the Gender Gap: An Analysis of Female Doctoral Students in Information Systems. ECIS 2021 Research Papers, Timișoara, Romania.

Vacca, A., Di Sorbo, A., Visaggio, C. A., & Canfora, G. (2021). A Systematic Literature Review of Blockchain and Smart Contract Development: Techniques, Tools, and Open Challenges. *Journal of Systems and Software, 174*(1), 1-19. https://doi.org/10.1016/j.jss.2020.110891

Vaishnavi, V., Kuechler, W., & Petter, S. (2004). *Design Science Research in Information Systems*. http://www.desrist.org/design-research-in-information-systems/

Valkokari, K. (2023). How to Enable Data-Sharing Ecosystems in the Context of Urban Mobility? *Network Industries Quarterly, 25*(2), 13-16.

van den Broek, T., & van Veenstra, A. F. (2015). Modes of Governance in Inter-Organizational Data Collaborations. ECIS 2015, Münster, Germany.

van Den Broek, T., & van Veenstra, A. F. (2018). Governance of Big Data Collaborations: How to Balance Regulatory Compliance and Disruptive Innovation. *Technological Forecasting and Social Change, 129*(1), 330-338. https://doi.org/10.1016/j.techfore.2017.09.040

Van Der Burg, S., Wiseman, L., & Krkeljas, J. (2021). Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing. *Ethics and Information Technology, 23*(3), 185-198. https://doi.org/10.1007/s10676-020-09543-1

van der Wielen, G., van Hattum, M., Mosterd, L., de Reuver, M., & Janssen, M. (2022). *More Than One Way to Solve the Healthcare Innovation Crisis With Digital Platforms: Various Forms of Platform Openness Impacting Primary Healthcare*. 35th Bled eConference Digital Restructuring and Human (Re) action, Bled, Slovenia.

van Velzen, T. (2022). *Business-To-Business Data Sharing via Data Marketplace Meta-Platforms: Exploring Governance Mechanisms to Enhance Data Sovereignty* Delft University of Technology]. Delft, the Netherlands. http://resolver.tudelft.nl/uuid:f6e34396-8038-47dc-a92a-ce4a6fd3e027

Vanderhulst, G., Schreiber, D., Luyten, K., Muhlhauser, M., & Coninx, K. (2009, 2009). *Edit, Inspect and Connect Your Surroundings*. Proceedings of the 1st ACM SIGCHI Symposium on Engineering Interactive Computing Systems, New York, New York, the United States.

Velikovsky, J. T. (2016). *Communication, Creativity and Consilience in Cinema* Faculty of Science and Information Technology, University of Newcastle].

Venable, J. (2006). *The Role of Theory and Theorising in Design Science Research*. Proceedings of the 1st International Conference on Design Science in Information Systems and Technology (DESRIST 2006), Claremont, California, the United States.

Venkatesh, V., Rai, A., & Maruping, L. M. (2018). Information Systems Projects and Individual Developer Outcomes: Role of Project Managers and Process Control. *Information Systems Research, 29*(1), 127-148. https://doi.org/10.1287/isre.2017.0723

Venkatesh, V., Thong, J. Y. L., Chan, F. K. Y., Hu, P. J.-H., & Brown, S. A. (2011). Extending the Two-Stage Information Systems Continuance Model: Incorporating UTAUT Predictors and the Role of Context. *Information Systems Journal, 21*(6), 527-555. https://doi.org/10.1111/j.1365-2575.2011.00373.x

Vesselkov, A., Hämmäinen, H., & Töyli, J. (2019). Design and Governance of mHealth Data Sharing. *Communications of the Association for Information Systems*, 299-321. https://doi.org/10.17705/1cais.04518

Virkar, S., Viale Pereira, G., & Vignoli, M. (2019). Investigating the Social, Political, Economic and Cultural Implications of Data Trading. In I. Lindgren, et al. (Ed.), *Electronic Government. EGOV 2019. Lecture Notes in Computer Science* (pp. 215-229). Springer, Cham. https://doi.org/10.1007/978-3-030-27325-5_17

Vom Brocke, J., Winter, R., Hevner, A., & Maedche, A. (2020). Special Issue Editorial–Accumulation and Evolution of Design Knowledge in Design Science Research: A Journey Through Time and Space. *Journal of the Association for Information Systems, 21*(3), 520-544. https://doi.org/10.17705/1jais.00611

Walter, M., Lovett, R., Maher, B., Williamson, B., Prehn, J., Bodkin-Andrews, G., & Lee, V. (2021). Indigenous Data Sovereignty in the Era of Big Data and Open Data. *Australian Journal of Social Issues, 56*(2), 143-156. https://doi.org/https://doi.org/10.1002/ajs4.141

Wan, Y., Poon, S., & Hu, N. (2004). *Tracking the Mindset of Open Source Participation: a Research in Progress*. AMCIS 2004 Proceedings, New York, New York, the United States.

Wang, P. (2021). Connecting the Parts with the Whole: Toward an Information Ecology Theory of Digital Innovation Ecosystems. *MIS Quarterly, 45*(1), 397-422. https://doi.org/10.25300/misq/2021/15864

Wang, Y., Min, Q., & Han, S. (2016). Understanding the Effects of Trust and Risk on Individual Behavior Toward Social Media Platforms: A Meta-Analysis of the Empirical Evidence. *Computers in Human Behavior, 56*, 34-44. https://doi.org/https://doi.org/10.1016/j.chb.2015.11.011

Weber, R. (2004). Editor's Comments: The Rhetoric of Positivism versus Interpretivism: A Personal View. *MIS Quarterly, 28*(1), iii-xii. https://doi.org/10.2307/25148621

Wells, J. D., Valacich, J. S., & Hess, T. J. (2011). What Signal Are You Sending? How Website Quality Influences Perceptions of Product Quality and Purchase Intentions. *MIS Quarterly*, 373-396.

Wiener, M., Cram, W. A., Remus, U., & Mähring, M. (2023). Control-Style Choices and Performance Impacts: How Should Senior IS Managers Enact Control Over Uncertain IS Projects? *Decision Support Systems, 167*(1), 1-12. https://doi.org/10.1016/j.dss.2022.113915

Wiener, M., Mähring, M., Remus, U., & Saunders, C. (2016). Control Configuration and Control Enactment in Information Systems Projects: Review and Expanded Theoretical Framework. *MIS Quarterly, 40*(3), 741-774.

Wiengarten, F., Humphreys, P., Onofrei, G., & Fynes, B. (2017). The Adoption of Multiple Certification Standards: Perceived Performance Implications of Quality, Environmental and Health & Safety Certifications. *Production Planning & Control, 28*(2), 131-141. https://doi.org/10.1080/09537287.2016.1239847

Wiesche, M., Bodner, J., & Schermann, M. (2013). *Antecedents of It-Enabled Organizational Control Mechanisms*. 20th European Conference on Information Systems (ECIS 2012), Barcelona, Spain.

Winandy, M. (2012). *A Note on the Security in the Card Management System of the German E-health Card*. Electronic Healthcare: Third International Conference, Casablanca, Morocco.

Wiseman, L., Pesce, V., Zampati, F., Sullivan, S., Addison, C., & Drolet, J. (2019). Review of Codes of Conduct, Voluntary Guidelines and Principles Relevant for Farm Data Sharing. *CTA Working Paper*.

Xia, H., Lu, D., Lin, B., Nord, J. H., & Zhang, J. Z. (2023). Trust in Fintech: Risk, Governance, and Continuance Intention. *Journal of Computer Information Systems, 63*(3), 648-662. https://doi.org/10.1080/08874417.2022.2093295

Xiao, S., Tan, X., Dong, M., & Qi, J. (2014). *How to Design Your Project in the Online Crowdfunding Market? Evidence From Kickstarter*. ICIS 2014 Proceedings, Auckland, New Zealand.

Xu, Y., & Kim, H.-W. (2003). *Trust Research in the Transactional Context and Its Implications for Online Trust*. PACIS 2003 Proceedings, Adelaide, Australia.

Yan, Y., Lv, Z., & Hu, B. (2018). Building Investor Trust in the P2P Lending Platform With a Focus on Chinese P2P Lending Platforms. *Electronic Commerce Research, 18*, 203-224. https://doi.org/10.1007/s10660-017-9255-x

Yang, Z., Keung, J., Zhang, M., Xiao, Y., Huang, Y., & Hui, T. (2020). *Smart Contracts Vulnerability Auditing with Multi-semantics*. 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain. https://dx.doi.org/10.1109/compsac48688.2020.0-153

Yong, B., Shen, J., Liu, X., Li, F., Chen, H., & Zhou, Q. (2020). An Intelligent Blockchain-Based System for Safe Vaccine Supply and Supervision. *International Journal of Information Management*, *52*(1), 1-12. https://doi.org/10.1016/j.ijinfomgt.2019.10.009

Yoo, C. W., Parameswaran, S., & Kishore, R. (2015). Knowing about Your Food From the Farm to the Table: Using Information Systems That Reduce Information Asymmetry and Health Risks in Retail Contexts. *Information & Management*, *52*(6), 692-709. https://doi.org/10.1016/j.im.2015.06.003

Zappa, A., Le, C.-H., Serrano, M., & Curry, E. (2022). Connecting Data Spaces and Data Marketplaces and the Progress Toward the European Single Digital Market with Open-Source Software. In (pp. 131-146). Springer International Publishing. https://doi.org/10.1007/978-3-030-98636-0_7

Zekhnini, K., Cherrafi, A., Bouhaddou, I., Benabdellah, A. C., & Raut, R. (2023). A Holonic Architecture for the Supply Chain Performance in Industry 4.0 Context. *International Journal of Logistics Research and Applications*, 1-28. https://doi.org/10.1080/13675567.2021.1999912

Zhai, M., Chen, Y., & Wei, M. (2022). Influence of Trust and Risk on Peer-To-Peer Investment Willingness: A Bidirectional Perspective. *Internet Research*, *32*(3), 943-966. https://doi.org/10.1108/INTR-11-2019-0444

Zhang, B., Yao, Y., Han, G., He, J., Xie, Y., & Wang, X. (2023). How Does Platform Labour Process Control Affect Courier's Employment Mobility Intentions?—The Mediating Effects of Overtime Work and Job Autonomy. *Sustainability*, *15*(13), 1-19. https://doi.org/10.3390/su151310022

Zhang, M. Y., & Williamson, P. (2021). The Emergence of Multiplatform Ecosystems: Insights From China's Mobile Payments System in Overcoming Bottlenecks to Reach the Mass Market. *Technological Forecasting and Social Change*, *173*(1), 1-14. https://doi.org/10.1016/j.techfore.2021.121128

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet of Things Journal*, *6*(2), 1594-1605. https://doi.org/10.1109/JIOT.2018.2847705

Zheng, H., Xu, B., & Lin, Z. (2019). Seller's Creditworthiness in the Online Service Market: A Study From the Control Perspective. *Decision Support Systems*, *127*, 113118. https://doi.org/10.1016/j.dss.2019.113118

Zhou, J., Kishore, R., Amo, L., & Ye, C. (2022). Description and Demonstration Signals as Complements and Substitutes in an Online Market for Mental Health Care. *MIS Quarterly*, *46*(4).

Zhu, H., & Madnick, S. E. (2009). One Size Does Not Fit All: Legal Protection for Non-copyrightable Data. *Communications of the ACM*, *52*(9), 123-128. https://doi.org/10.1145/1562164.1562196

Zou, W., Lo, D., Kochhar, P. S., Le, X. B. D., Xia, X., Feng, Y., Chen, Z., & Xu, B. (2021). Smart Contract Development: Challenges and Opportunities. *IEEE Transactions on Software Engineering*, *47*(10), 2084-2106. https://doi.org/10.1109/TSE.2019.2942301

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

Appendices

1. Interview protocols

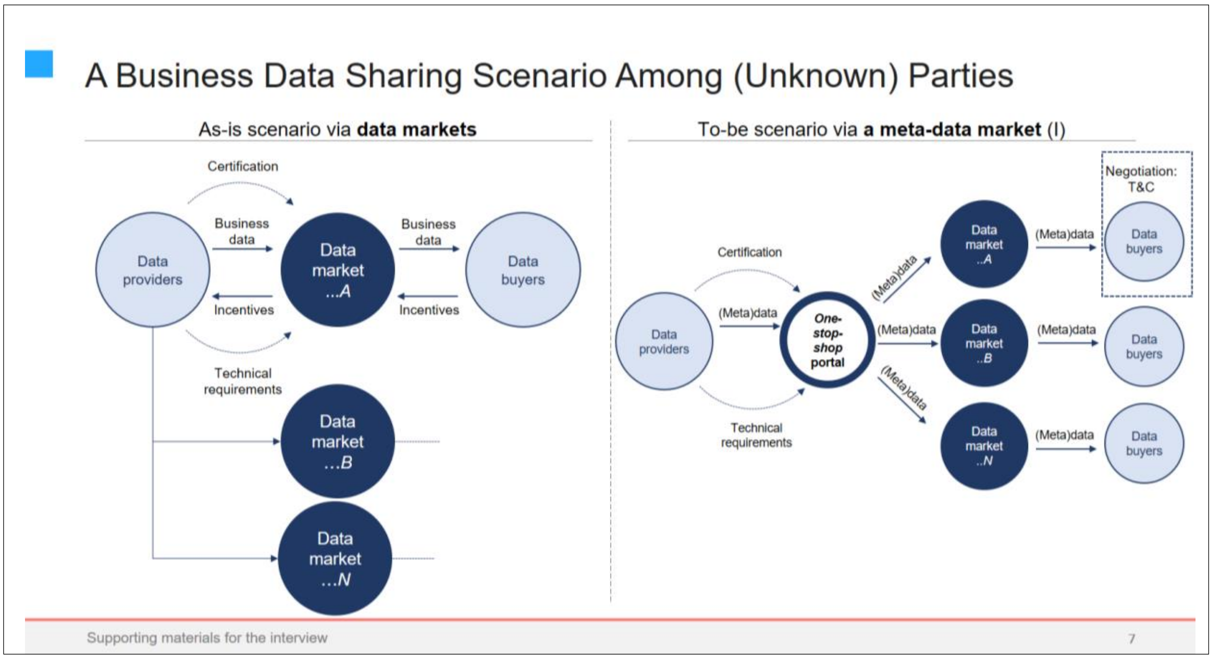
Opening segment

Questions about background information.

- **Question 1:** What position do you hold in this company now, and for how long have you been in this position?
- **Question 2:** Could you please tell me briefly the nature of your job?
- **Question 3:** How familiar is your organization with business-to-business data sharing? Has your organization known, experienced, or thought about it?
    - *[if yes, probe for]* Could you explain how your company conducts B2B data sharing?
    - *[if yes, probe for]* What is your role in decision-making about B2B data sharing?
- **Question 4:** Could you please tell me briefly about your experience related to data marketplaces?

Middle segment

Questions about exploring potential value propositions and hindrances of business data sharing via a meta-platform for data marketplaces.



A Business Data Sharing Scenario Among (Unknown) Parties

As-is scenario via **data markets**

Certification

Data providers

Business data

Incentives

Data market …A

Business data

Incentives

Data buyers

Technical requirements

Data market …B

Data market …N

To-be scenario via **a meta-data market** (I)

Negotiation: T&C

Certification

Data providers

(Meta)data

One-stop-shop portal

Technical requirements

(Meta)data

(Meta)data

(Meta)data

Data market ..A

Data market ..B

Data market ..N

(Meta)data

(Meta)data

(Meta)data

Data buyers

Data buyers

Data buyers

Supporting materials for the interview 7

- **Question 5:** Do you have any questions related to the use case of a meta-platform for data marketplaces?
- **Question 6:** To what extent do you think a meta-platform for data marketplaces can facilitate B2B data sharing among organizations?
    - *[for greater extent, probe for]* Could you explain the reasons why this is the case?
    - *[for less extent, probe for]* Could you explain why business data sharing via a meta-platform for data markets may not work?

2. Structured categorization matrix for analyzing data sovereignty facets

Higher-level facet	Facet	Second-order code	First-order Code
Protection	Data ownership	Data ownership fundamental	Data ownership as sovereignty facet Protection of data ownership
		Data possession	Data provider as owner Ownership clarification Ownership transfer Retention of intellectual property right
		Meta-data	Meta-data as data description Importance of meta-data
		Term of use	Data storage location Data usage condition
Provision	Data control	Data control fundamental	Data control as sovereignty facet Provision of data control mechanism
		Data provenance	Data flow tracking Data origin information Data tagging Data usage insight Data storage insight Knowledge about data consumer
		Data withdrawal	Data access revocation Dataset retraction
		Policy enforcement	Access condition check Legal enforcement Policy attachment Technical enforcement
	Security	Cutting-edge security mechanism specific for data sharing	Anonymization Confidential computing Distributed ledger architecture Encryption Federated learning Privacy-preserving data analysis Watermark
		Security CIAN principles	Availability Confidentiality Integrity Non-repudiation
		Security fundamental	Security as sovereignty facet Provision of security mechanism
		Verifiable credential	Authorization capability Credential verification Trusted identity
	Compliance	Compliance fundamental	Compliance as sovereignty facet Provision of compliance mechanism
		External compliance	Industry standard Regulatory compliance
		Horizontal compliance	Data usage audit Data sharing contract Dispute resolution
		Vertical compliance	Agreement with operator Technical compliance
Participation	Responsibility division	Accountable oversight	Liability chain Penalty Provision mechanism

Higher-level facet	Facet	Second-order code	First-order Code
		Interpretation of participation	Active oversight
			Membership enrollment
			Product installation
			Responsible use of platform and data
		Responsibility fundamental	Responsibility as sovereignty facet
			Responsibility division to ensure participation
Contextual condition	Data type (format variations)	Influence on data control	Complexity in data storage
			Data format
			Large data size
			Processed data withdrawal
			Real-time data
	Data type (industry-specific data)	Influence on compliance	Compliance practice maturity
			High governance standard
			Over-regulation
		Influence on ownership	Lack of capacity for data sharing
	Business data sharing setting	Influence on compliance	Cultural knowledge gap
			Different liability
			Different national law
		Influence on data control	Alignment of data marketplace architecture
			Data provenance difficulty
		Influence on ownership	Data marketplace selection
		Influence on responsibility	Data marketplace evaluation
			Domination of meta-platform
			Responsibility division
	Organizational size	Influence on compliance	Liability for large organization
			Understanding legal requirement for smaller company
		Influence on data control	Lack of capability for smaller company

3. Online appendices and datasets

The online appendices can be accessed online at https://doi.org/10.4121/785dfc19-d82b-4e46-a6d4-8a714569557b. The online appendices consist of:

1. Online Appendix 1. List of literature
2. Online Appendix 2. Prototype evaluation
3. Online Appendix 3. Prototype interfaces
4. Online Appendix 4. Developing a data sovereignty measurement model
5. Online Appendix 5. Conducting a controlled experiment

The raw datasets for the quantitative studies in this dissertation (Chapters 8 and 9) are available in the 4TU Research Data Repository. For access to these datasets, please see the following DOI:

1. Data sovereignty measurement model: https://doi.org/10.4121/e4cacfac-31f0-4523-81f4-35383ba958a8.
2. Controlled experiment and structural equation modeling: https://doi.org/10.4121/785dfc19-d82b-4e46-a6d4-8a714569557b.

Acknowledgments

I want to thank the incredible people who made my PhD journey so inspiring. **Mark,** you are the main reason why I cherished my PhD journey so much! I recall having another PhD offer on the table, but your question changed my decision: “How do you cope with stress?” At that moment, I knew I would be in good hands. So, I chose you, Anneke, and the ICT group. Mark, when we brainstormed, your insights often swiped my doubts about research directions. Your detailed, sharp, and critical feedback shaped my research outputs to the next level. I could not help but smile every time I saw that single question mark “?” in my manuscript. You throwing me into the Information System field? Best move ever. After ECIS 2022 in Timisoara, I found the “home” to which I belong. You care so much about me, not just as a PhD researcher but as a person. Starting our meetings with a simple “How is life?” means more than you might realize. You have been a guiding light in my PhD journey, much like the *moon* lighting up a dark sky.

Anneke, I could not ask for a better supervisor because I already have one. You, too, are the primary reason why my PhD journey is so rewarding. While digital platforms might not be your main literature, I was amazed by how quickly you made sense of everything! Your perspective helped me position my work for a wider audience beyond just the data economy community. Your feedback is always spot on, catching mistakes I often overlook. One word that stays with me: *consistency*. After our meetings, I came out feeling more confident and valued. It does make me wonder, though:” I have gotten used to your level of excellence. How will I find mentors like you in my next career steps?” You have been the *sun* in my PhD journey, always shining a light on the right path.

Aga, I thank you for everything. It started with your email “[PhD Vacancies] Business Models for Data Platforms,” and that set me on my journey at TU Delft. You have been the first person I would reach out to about PhD matters, and life, too! Thanks for all the discussions, the paper writing sessions, and the conference trips, among others. Knocking on your office is one of my favorite memories in my PhD journey, *my brother.*

I want to thank **Hosea** for our two years of interaction. With him, working on the Trusted Secure Data Sharing Space (TRUSTS) project (funded by the European Commission) became so much fun. He backed me up so I could work on my PhD, too. He always reminded me about theory. As a pragmatist with a consulting background, I did not always prioritize it. Over time, however, I realized: *theory is king.*

I want to extend my gratitude to our research partners from the TRUSTS project. A special thank you to those I worked closely with: **Ahmad, Alexandra, Andreas, Bert, Gerrit, Gianna, Giulia, Hannah, Ioannis M., Ioannis R., Martin, Michael, Natalia, Nina, Rosa, Silvia,** and **Stefan.**

To my dissertation committee, thank you for your invaluable contributions. **Yao-hua**, your feedback in the ICT Colloquiums was pivotal in positioning my work within the broader data sharing literature—thank you. **Hans,** your guidance during my go-no-go meeting was crucial, and your insights significantly enhanced the design of my dissertation. **Jan,** taking your design science course was one of the best decisions in my PhD journey. I am so grateful to have participated. **Christine** and **Johan,** although we have never met, you accepted the invitation without hesitation. I appreciate it immensely, and I look forward to our paths crossing again in the future.

To the ICT Group, thank you for the warm hospitality. The formal (e.g., ICT colloquiums) and social events (e.g., ICT gatherings) made me feel at home every single day. A special mention to the faculty members: **Aaron, Boriana, Caroline, Fernando, Jacobien, Jolien, Marcela, Marijn, Nadia, Nitesh, Roel, Sélinde,** and **Sepinoud**; to the postdoctoral and guest researchers: **Hong, Francesca, Marcus, Marloes, Mengying,** and **Menno**; to my fellow PhDs: **Antonia, Budi, Cathleen, Dewant, Emyana, Elyas, Esra, Eva, Gijs, Gilang, Ini, Íñigo, Jacqueline, Jeroen, Julia, Juliette, Kathleen, Lærke, Liubov, Louise, Nic, Prachi, Rachel, Reni, Ruixuan,** and **Wendy**; to the unforgettable former ICT members: **Ali, Arie, Dhata, Ilse, Lutfhi, Mannat, Olivier,** and **Jacopo.**

Christine, Ellen, Fanny, Ilse, Jolien, Laura, Minaksie, and **Olivie:** I cannot imagine navigating my PhD without you. You answered countless questions, from visas to scheduling, from ICT colloquiums to workspace arrangements. Thank you for making everything smoother!

My office mates in B3.310, **Elyas, Rijk, Sem,** and **Wiebke,** you made every day at the office lively and enjoyable. Our shared moments and discussions always made me feel connected and excited for what each new day would bring. To my TPM PhD peer group: **Aashis, Jeroen, Jessie, Maartje, Mylene,** and **Sara**, it took us two years to complete twelve meetings, but we made it! Thank you for your critical feedback on my proposal and for assisting me in testing my research instruments.

I attended Information System (IS) conferences during my PhD trajectory. At the Bled eConference, I always felt embraced and secure. A big thank you to **Andreja, Anand, Doroteja, Guido, Mirjana,** and others. At DESRIST, my knowledge of design science research was strengthened, and I am grateful to **Leona, Maung, Matti**, and **Robert** for that. The ECIS and ICIS 2022 doctoral consortiums made me fall in love (even more) with the IS field. **Hanna, Jonathan**, **Monideepa,** and **Ravis** were so helpful during ECIS. At ICIS, I owe much to **ABJ, Andrea, Anjana, Arun, Atreyi, Chee Wee, Christy, Joao, Ke-Wei, Margunn, Natalia, Youngjin,** and many others. Their insights were eye-opening.

I collaborate with many colleagues on paper writing. Special shoutouts to **Claudia, Sven, Zenlin, Geerten, Martin, Nag,** and **Saba**. Along the journey, I also connected with some of my favorite PhD peers: **Sean, Dennis, Nedo,** and **Fruhwirth.**

I want to thank the former TPM MSc students with whom I collaborated. **Montijn,** your passion for business models in the IS field is contagious, and I look forward to collaborating more in the future. **Thomas,** it is great that you are still active in data-sharing consulting after graduation. **Bisma,** your work on aggregator business models significantly helped TRUSTS. **Romy,** I hear you are doing fantastic in Switzerland! **Gio,** I enjoyed our countless discussion sessions about sovereignty. **Maureen,** I am excited to see where your excellent thesis materials will be published. I also thank **Gijs,** with whom I enjoyed critical discussions about digital platforms in the health domain. I am happy to join the supervision team in the late stage of your PhD trajectory.

Being in the Netherlands, especially Delft, the warmth and support of **the Indonesian Community** has been invaluable. Among the PhD and Postdoc Indonesian folks, I am grateful for Agung I, Agung W, Adit, Albert, Alfan, Anita, Arry, Atin, Bagas, Budi, Daniel, Dita, Eryda, Fazrul, Fira, Gagus, Iban, Ilham, Indra, Jeri, JJ, Liza, Lucas, Lutfi, Mikhta, Nasikun, Sebrian, Yana, and Wicak. From the KMD 2022/2023 batch, my thanks go to Artono, Bella, Dhoni, Endy, Fakhri, Gusti, Habbie, Hamida, Hanif, Rifki, Risang, Sasa, SASA, Satria G., Satria W., Syakal, and Widana. And for the continuous support from the PPI Delft community across the years, I appreciate Abrar, Aji, Ando, Anggi, Ardhan, Arin, Ayu, Ben, Citra, Devano, Eureka, Fadhil, Firman, Firdo, Goban, Hilman, Iqbal, Kanya, Mute, Nindy, Panji, Petra, Randana, Rasyid, Riando, Sulthon, Tofan, Wida, among others. I also thank Yurina for her tremendous help, especially during my first year navigating life in Delft.

Tom, Ajeng, and **Widya!** I could not imagine living in the Netherlands without you guys! Thank you for everything, my go-to folks. **Geng Receh** (Aldy, Barokah, Bita, Bramka, Nabriz, Kus, Retna, Tika), thank you for all the memories! I often called my friends, including **Gina, Ochi,** and **Yaski**! I am grateful for their companionship. I am also grateful for the active WhatsApp group with ***Tim Sembilan*** and ***Ayah Idaman***, where I can see my good friends thriving in their endeavors.

My parents, ***Bapak*** **Ersis** and ***Mama*** **Risna,** I know you always keep me in your prayers, wishing for my successful PhD journey. Thank you for traveling to Europe, for the countless video calls, and for all your support! I would also like to mention **Visi** and **Azta** for their tremendous support during my PhD journey, especially in taking care of the toddler during the pressing time! I am also grateful to my in-laws and (extended) families for their encouragement.

Rein, my lovely toddler, my world changed since you were born. It seems everything revolves around you now, and your mom and I could not be happier about it. I learn so much from you: the excitement in simple things, being present, slowing down, contagious smile, patience, recharging energy, and many other things. You are the reason I cannot give up, the reason I keep going, and the reminder of why I am here. Hey, do not grow up too fast! **Anni,** my darling, I reserve the last, special part of my acknowledgments for my favorite person on earth. For your unconditional love, your tremendous support, your strength on the hilly and rocky roads, and your dedication—not only am I forever thankful, but I also deeply admire you. What would I be without you? The future is always approaching, but it does not matter because I will always be in my forever home—with you, darling. Let us continue this journey and grow together. What is next? #MenjalANNIbersamaANTRA.

Curriculum vitae

Antragama Ewa Abbas was born in Banjarmasin on October 6, 1993. In 2015, he received his BEng in *Information Systems and Technology* from Bandung Institute of Technology, Indonesia. In 2017, he was awarded an MSc degree with distinction (Cum Laude) in *Information Technology with Business and Management* from Sussex University, England, the United Kingdom. Antragama joined the Information and Communication Technology (ICT) group at the Faculty of Technology, Policy, and Management at Delft University of Technology in 2020. Currently, he is working as a postdoctoral researcher in the same group. Prior to joining ICT, he was a technology consultant at Accenture Indonesia.

Antragama is interested in *data economy* research. Specifically, his primary research interest lies in exploring and designing emergent technologies that enable data sharing. In his PhD dissertation, he investigates knowledge for designing control mechanisms (i.e., smart contracts, certifications) to enhance data sovereignty (i.e., how organizations can control the exchanged data products) in the complex constellation of data marketplaces. In his postdoctoral tenure, he secured a research grant and is working on a project investigating the role of catalysts in health data ecosystems.

His PhD was part of the Trusted Secure Data Sharing Space (TRUSTS) project, funded by EU Horizon 2020. He published in Information Systems (IS) journals (i.e., Electronic Markets, Journal of Theoretical and Applied Electronic Research) and presented his works at IS conferences such as ICIS, ECIS, Bled eConference, and DESRIST. Together with his co-authors, he won the “Outstanding Paper Award” at the 36th Bled eConference and was nominated for “Best Research-in-Progress Paper” at ECIS 2021.

Antragama is supervising a PhD researcher. He also collaborated with six MSc students to assist them in completing their thesis and/or publishing their works in relevant IS outlets. He taught courses at the MSc level, including *Digital Platform Design, Information and Communication Service Design,* and *Research Methods.* He served as the colloquium chair for the ICT group from 2020 to 2021.

Antragama also serves the broader IS academic communities. He was a personal committee member of DESRIST and was invited to become a mini-track chair at AMCIS. He also reviewed manuscripts in relevant IS journals (e.g., Electronic Markets, Journal of Business Research) and conferences (e.g., ECIS).

List of publications

Articles

Published

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*(20), 1-21. https://doi.org/10.1007/s12525-024-00695-2

Bergman, R., **Abbas, A. E.,** Jung, S., Werker, C., & de Reuver, M. (2022). Business Model Archetypes for Data Marketplaces in the Automotive Industry. *Electronic Markets, 32*(2), 747–765. https://doi.org/10.1007/s12525-022-00547-x

Abbas, A. E., Agahari, W., van de Ven, M., Zuiderwijk, A., & de Reuver, M. (2021). Business Data Sharing through Data Marketplaces: A Systematic Literature Review. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(7), 3321-3339. https://doi.org/10.3390/jtaer16070180

Nominated for "Best PhD Paper of Engineering Systems and Services Department" Award

Under review

de Reuver, M., Agahari, W., **Abbas, A. E.,** Kool, F. *Adoption of B2B Data Marketplaces in Manufacturing Industries: The Impact of Perceived Control on Willingness to Share Internet-Of-Things Data* (Under review at *Technovation*).

van der Wielen, G., **Abbas, A. E.,** & de Reuver, M. Unleashing Innovation in First-line Healthcare Platforms: Breaking Down the Barriers. (Under review at *International Journal of Medical Informatics*).

Work in progress

Abbas, A. E., Agahari, W., Ofe, H., Zuiderwijk, A., & de Reuver, M. *It Does Matter! Data Sovereignty Impacts on Trust, Perceived Risk, and Willingness to Share (Business) Data* (Planned submission to *Business & Information Systems Engineering*).

Abbas, A. E., Hinrichs-Krapels, S., & de Reuver, M. *Institutional Pressures in the Birth Stage of Data Ecosystems*.

Abbas, A. E., Ofe, H., Zuiderwijk, A., & de Reuver, M. *Business Models for a Meta-Platform* (Planned submission to *Information & Management*).

van der Wielen, G., Zwart, M., **Abbas, A. E.,** de Reuver, M., & Janssen, M. *Communication is Care: Designing Platform-based Architecture for First-Line Healthcare* (Planned submission to *IEEE Transactions on Engineering Management*).

Conference papers

Published

Abbas, A. E., Agahari, W., Ofe, H., Zuiderwijk, A., & de Reuver, M. (2023). *Toward Sovereign Data Exchange Through a Meta-Platform for Data Marketplaces: A Preliminary Evaluation of the Perceived Efficacy of Control Mechanisms.* 36th Bled eConference – Digital Economy and Society: The Balancing Act for Digital Innovation in Times of Instability, Bled, Slovenia.

Winning "Outstanding Paper" award

Nominated for "Best PhD Paper of Engineering Systems and Services Department" Award

Abbas, A. E., Ofe, H., Zuiderwijk, A., & de Reuver, M. (2023). *Toward Business Models for a Meta-Platform: Exploring Value Creation in the Case of Data Marketplaces.* The 56th Hawaii International Conference on System Sciences (HICSS), Honolulu, the United States.

Abbas, A. E., Ofe, H., Zuiderwijk, A., & de Reuver, M. (2022). *Preparing Future Business Data Sharing via a Meta-Platform for Data Marketplaces: Exploring Antecedents and Consequences of Data Sovereignty.* 35th Bled eConference - Digital Restructuring and Human (Re-Action), Bled, Slovenia.

de Reuver, M., Ofe, H., Agahari, W., **Abbas, A. E.,** & Zuiderwijk, A. (2022). *The Openness of Data Platforms: A Research Agenda.* First ACM Data Economy Workshop, Rome, Italy.

Abbas, A. E. (2021). *Designing Data Governance Mechanisms for Data Marketplace Meta-Platforms*. Proceedings 34th Bled eConference – Digital Support from Crisis to Progressive Change, online.

Brehmer, M., **Abbas, A. E.,** & Vaidyanathan, N. (2021). *Towards Designing a Method to Create Sticky Information Security Training for SMEs: Identifying Design Factors.* ECIS 2021, online.

Nominated for "Best Research-in-Progress Paper" award

van de Ven, M., **Abbas, A. E.,** Kwee, Z., & de Reuver, M. (2021). *Creating a Taxonomy of Business Models for Data Marketplaces.* 34th Bled eConference - Digital Support from Crisis to Progressive Change, online.

Abstract presentation

van der Wielen, G., Zwart, M., **Abbas, A. E.,** & de Reuver, M. (2024). *Designing the Architecture of Platform Ecosystems in First-Line Healthcare: A Platform Openness Perspective.* 7th Innovation in Information Infrastructures (III) Workshop, Barcelona, Spain.

Previous publications

Abbas, A. E. (2019a). *API Integration of National Complaint Handling System in Indonesia: A State of The Art Review.* 2019 International Conference on ICT for Smart Society (ICISS), Bandung, Indonesia.

Abbas, A. E. (2019b). *Investigating 'One-Day Flies' Users in The StackOverflow: Why Do and Don't People Participate?* 2019 International Conference on ICT for Smart Society (ICISS), Bandung, Indonesia.

Abbas, A. E., Beloff, N., & Sari, G. G. P. (2018). *Toward Smart City in Indonesia: Connecting Dentist Co-assistant and Citizen.* 2018 International Conference on ICT for Smart Society (ICISS), Semarang, Indonesia.

Abbas, A. E. (2017). *Complex Project as a Knowledge Process: Conceptualizations and Examples.* 2017 International Conference on Computers, Communications, and Systems (ICCCS), Krakow, Poland.

Abbas, A. E. (2017). Literature Review of a Cashless Society in Indonesia: Evaluating the Progress. *International Journal of Innovation, Management and Technology*, 8(3), 193-196.

Abbas, A. E., Beloff, N., & Sari, G. G. P. (2017). *A Pathway Toward Smarter City: Build up the Strategic Application Requirement.* 2017 International Conference on ICT For Smart Society (ICISS), Tangerang, Indonesia.

Arman, A. A., **Abbas, A. E.,** & Hurriyati, R. (2015). *Analysis of Smart City Technology Initiatives for City Managers to Improve City Services and Quality of Life Based on ISO 37120.* Proceedings of 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia, St. Petersburg, Russia.

Doctoral consortium presentations

Abbas, A. E. (2022). *Designing Data Governance Mechanisms for Data Marketplace Meta-Platforms: Ensuring Data Sovereignty in Business Data Sharing.* 2022 International Conference on Information Systems (ICIS), Copenhagen, Denmark.

Abbas, A. E. (2022). *Designing Data Governance Mechanisms for Data Marketplace Meta-Platforms: Ensuring Data Sovereignty in Business Data Sharing.* 2022 European Conference on Information Systems (ECIS), Timisoara, Romania.

Abbas, A. E. (2021). *Designing Data Governance Mechanisms for Data Marketplace Meta-platforms*. 16th International Conference on Design Science Research in Information Systems and Technology (DESRIST 2021), Online.

Research project deliverables

- (Primary contribution) D7.1 Sustainable business model for TRUSTS data marketplace I
- (Primary contribution) D7.2 Sustainable business model for TRUSTS data marketplace II
- D2.1 Definition and analysis of the EU and worldwide data market trends and industrial needs for growth
- D2.2 Industry specific requirements analysis, definition of the vertical E2E data marketplace functionality and use cases definition I
- D7.4 Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship I

- D7.5 Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship II
- D7.6 Report on standardization activities
- D7.7 Business plan and Implementation action plan I