TOWARD SOVEREIGN DATA EXCHANGE THROUGH A META-PLATFORM FOR DATA MARKETPLACES: A PRELIMINARY EVALUATION OF THE PERCEIVED EFFICACY OF CONTROL MECHANISMS

ANTRAGAMA EWA ABBAS, WIRAWAN AGAHARI,
HOSEA OFE, ANNEKE ZUIDERWIJK, MARK DE REUVER
Delft University of Technology, Faculty of Technology, Policy and Management, Delft, Netherland
a.e.abbas@tudelft.nl, w.agahari@tudelft.nl, ofehosea@gmail.com,
a.m.g.zuiderwijkvaneijk@tudelft.nl, g.a.dereuver@tudelft.nl.

The landscape of platform ecosystems is becoming increasingly complex, with new types of platforms emerging that glue together otherwise fragmented ecosystems. One recent case is meta-platforms that can contribute to the European Data Economy by interconnecting data marketplaces; however, meta-platforms may intensify data sovereignty concerns: the inability of data providers to own and control the exchanged data. While smart contracts and certification can generally enhance data sovereignty, it is unknown whether data providers perceive these control mechanisms as valuable in the complex meta-platform setting. This study aims to evaluate the perceived efficacy of the control mechanisms to ensure data sovereignty in meta-platforms. The findings from a survey study (n=93) indicate that respondents perceive high data sovereignty. One potential explanation is that smart contracts can potentially enable providers to maintain ownership and control over their exchanged data; meanwhile, certification may signal meta-platforms' responsibility to deliver secure data exchange infrastructure and assist providers in adhering to relevant regulations. This study contributes to advancing design knowledge for meta-platforms, showcasing that meta-platforms can be designed in a way to resolve fragmentation without neglecting data sovereignty principles.

Keywords:
data economy, meta-platforms, data marketplaces, business data exchange, data sovereignty

University of Maribor Press

DOI https://doi.org/10.18690/um.fov.6.2023.18
ISBN 978-961-286-804-8

1 Introduction

The growing demand to unleash the full potential of the Data Economy has led to the emergence of data marketplaces: multi-sided platforms that facilitate business data exchange among enterprises (Spiekermann, 2019). This phenomenon is particularly evident in the European context, where efforts to strengthen the European Data Economy have accelerated the proliferation of these marketplaces (European Commission, 2020). Due to the specialized nature of data as a commodity, data marketplaces often focus on specific industries, resulting in significant fragmentation and heterogeneity (Aaltonen et al., 2021). This fragmentation is expected to continue, causing lock-in effects and data discovery challenges for data providers and consumers (Santiago & Laoutaris, 2022).

The existing platform literature recognizes meta-platforms as potential measures to reduce fragmentation and achieve critical mass (Mosterd et al., 2021; Pitt et al., 2021). A meta-platform is built on top of two or more existing platforms to connect their ecosystems (Zhang & Williamson, 2021). A typical example of a meta-platform in the tourism industry is Trivago, which federates and coordinates other platforms (e.g., Expedia, Booking, and Airbnb). Other examples in the data marketplace context include the recently developed TRUSTS[1] and i3-Market[2]. Nevertheless, while exchanging business data on a data marketplace is already difficult due to data sovereignty concerns (i.e., the inability of data providers to own and control the exchanged business data), these concerns will likely intensify in a meta-platform setting because data may flow from one data marketplace to another (Zappa et al., 2022). Additionally, complying with data sovereignty principles has recently become a prerequisite for exchanging business data within the European context (European Commission, 2020).

Smart contracts and certification are among the most-discussed control mechanisms to enhance data sovereignty in various data exchange settings (Lauf et al., 2022; Schmidt et al., 2022). For example, smart contracts have been extensively implemented in data marketplace cases to guarantee data sovereignty (Fruhwirth et al., 2020; Precht & Gómez, 2021). Likewise, certification has been implemented in

[1] https://www.trusts-data.eu/, accessed on May 11, 2023
[2] https://www.i3-market.eu/, accessed on May 11, 2023

supply chains (Bastiaansen et al., 2020; Dalmolen et al., 2019) and data ecosystem settings (Azkan et al., 2020). 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 these control mechanisms as valuable. For example, data providers may argue that certification is less valuable due to the difficulty of tracing valid and non-expired certificates in the complex constellations of data marketplaces. Against this backdrop, **this study investigates the perceived efficacy of control mechanisms, namely smart contracts and certification, to enhance data sovereignty in data marketplace meta-platforms.** This research advances design knowledge for meta-platforms to address fragmentation without compromising data sovereignty principles.

2 Research Background

2.1 Meta-platform offerings

Multiple approaches can be adopted to interconnect digital platforms. Digital platforms can create direct application programming interfaces to connect with each other (Hodapp & Hanelt, 2022). Third parties can "bridge" two platforms by creating an application (e.g., the Philips Hue case) (Hilbolling et al., 2020) or "fork" a platform by exploiting its core resources (e.g., Amazon Fire) (Karhu et al., 2018). Meta-platforms, on the other hand, are built on top of two or more existing platforms, thereby connecting their respective ecosystems (Zhang & Williamson, 2021). Because meta-platforms may act as a coordinator to enable collective actions, legitimate governance, and transparency values (Pitt et al., 2021), meta-platforms are potentially suitable for tackling the fragmentation of data marketplaces in the European context.

Trivago is an example of a *meta-platform* where Expedia, Booking, and Airbnb serve as *platform participants*. These platform participants have their provider- and consumer-side (we refer to them as *end-users*). Therefore, meta-platforms cannot exist independently (Lagutin et al., 2019). Meta-platforms have two key offerings to create value for end-users: information aggregation and a one-stop-shop portal. First, meta-platforms aggregate information from platform participants to create new services, for example, by creating a meta-search engine to manage information flow and disseminate information (Lanza et al., 2016; Pitt et al., 2021). Aggregating information often aims to give recommendations to end-users (Floetgen et al., 2021; Yang & Wang, 2019). Second, meta-platforms provide a one-stop-shop portal to enable end-users to seamlessly interact with only a single user interface to perform necessary activities (Floetgen et al., 2021; Reinartz et al., 2019). This portal mediates interoperability between platform participants by providing service or technical integration (Ulrich & Alt, 2021). While participating platforms may be reluctant to standardization (Costabile et al., 2022), a meta-platform creates a common interface or protocol for interaction within its ecosystem without requiring participating platforms to modify their internal standards.

2.2 Data sovereignty dimensions and indicators

Data sovereignty encompasses various dimensions. To maintain a focused analysis, we prioritize the dimensions most closely associated with data sovereignty: *ownership, control, responsibility*, and *security* (Hummel et al., 2021). We also investigate *compliance* as another dimension, given its recent legal prominence in contexts such as the European Data Governance Act (Duisberg, 2022). We define indicators for each dimension to provide observable measurements of data sovereignty as a multi-dimensional construct.

Data ownership is the exclusive right and authority to make decisions regarding data assets (Hummel et al., 2021). Despite the ongoing debate on who should own data assets (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 exchange, (2) be involved in determining (monetary) incentives (Dalmolen et al., 2020), (3) define the data type to exchange (Lee et al., 2017), and (4) decide which data marketplace receives the meta-data description (Abbas et al., 2022).

Control over exchanged data is among the most heavily recognized dimension of data sovereignty, referring to the ability of data providers to steer data exchange 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 exchange (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 (e.g., on the meta-platform, on its infrastructure, or the data consumer infrastructure) (Dalmolen et al., 2020). Finally, if something happens, data providers can withdraw their (meta-)data for a meta-platform and data marketplace participants (Lauf et al., 2022). Another critical data sovereignty dimension relates to *compliance*. As data exchange 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 dimension of data sovereignty due to the context novelty is the *responsibility* dimension, primarily because of the complex constellations of data marketplaces via a meta-platform. As our previous study reveals (Abbas et al., 2022), it should be clear who is responsible for what to ensure sovereign data exchange. Hence, we propose the three indicators: meta-platforms should (1) responsibly select data marketplace participants that adhere to data exchange standards, (2) clearly divide responsibilities between the meta-platform and the data marketplace participants, and (3) take responsibility if the sensitive data is misused or stolen. Finally, we include an essential data sovereignty component: *security*. 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 exchanged data to unauthorized parties, (2) prevent the alteration of the exchanged data, (3) enable data providers to execute data-sharing transactions without system failures, and (4) implement up-to-date security features. In summary, we use these five data sovereignty dimensions to evaluate the perceived efficacy of control mechanisms in the meta-platform setting.

2.3 Control mechanisms: Smart contracts and certification

Control theories explain how and why control mechanisms enacted by controllers can influence the behaviors of controlee (Saunders et al., 2020). Control mechanisms can be divided into formal (input, process, output) and informal (self and clan) control (Wiener et al., 2016). In this study, we want to examine how smart contracts (as a process control) and certification (as an input control) can diminish data sovereignty concerns of data providers. We select the combination of these two mechanisms because they may influence all sovereignty dimensions.

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). Regarding *ownership*, smart contracts offer a pre-filled template to define use cases of data exchange, which include the term of use, monetary incentives, and the data type to exchange (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). We hypothesize that smart contracts enhance the data sovereignty dimensions of *ownership* and *control* (H_1).

Certification for sovereign data exchange "…defines a standardized level for security related to technical and organizational aspects" (Menz et al., 2019). Therefore, certification aims to confirm compliance with these pre-conditions (Biegel et al., 2020). Within the meta-platform context, applying certification means that a meta-platform decides pre-conditions that must be fulfilled by data marketplace participants and their end-users (data providers and consumers). They need to, for instance, apply technical integration services such as application programming interfaces (or data ecosystem nodes) to join the meta-platform federation infrastructure. For example, compliance and security can be achieved by incorporating the International Data Space certification, demonstrating compliance with ISO/IEC 27001 (international standard for information security management) and IEC 62443 (cybersecurity for operational technology in automation and control systems). Related to the clarity of responsibility, certification can distinguish actors' roles and responsibilities (Lansing et al., 2018). For example, a meta-platform and data marketplaces can only access the meta-data, not actual business data themselves; a meta-platform and an external third party will act as evaluators to assess certification compliances. We hypothesize that certification can advance the *compliance*, *security*, and *responsibility* dimensions of data sovereignty (H_2). To sum up, Figure 1 summarizes the research model.

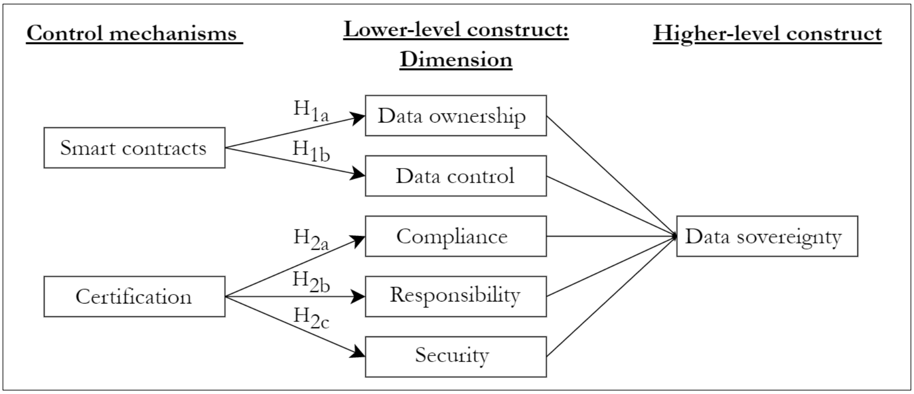

Figure 1: The research model

3 Research approach

This research is part of a larger design science project. We first explored state-of-the-art data marketplaces as federation objects and defined meta-platform boundary conditions. With a focus on data sovereignty concerns, we established metrics to evaluate artifact efficacy. We then examined control mechanisms in various business data exchange contexts, prioritizing smart contracts and certification. We developed a prototype to address data sovereignty concerns in collaboration with an EU project consortium. This paper concentrates explicitly on the final step, evaluating the perceived efficacy of control mechanisms in addressing data sovereignty concerns. We define efficacy as "the ability to produce a desired or intended result."[3] While objective measures of data sovereignty (e.g., Firdausy et al., 2022), smart contracts (e.g., Hai & Liu, 2022), and certifications (e.g., Menz et al., 2019) technically exist, they do not always reflect the subjective experience of data providers interacting with these control mechanisms. The level of control that smart contracts offer may not always match the perceived level of control due to various factors, including the complexity of the smart contracts or the ability to interpret how smart contracts work. Obtaining feedback on the perception of control mechanisms can help

[3] http://www.oxforddictionaries.com/definition/english/efficacy, accessed on 06 April 2023.

identify gaps beyond the technical aspects, which can inform the design of control mechanisms.

We conducted a survey study to achieve our objective, recruiting 93 participants residing in Europe through the Prolific platform (47 female, 46 male). The sample size was determined using G*Power statistical calculations. The majority of 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 exchanges, 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. The video explained a hypothetical scenario where users play the role of a data provider, a telecommunication company so-called TELCO.[4] Data providers will exchange 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 meta-data 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. Because the measurement of data sovereignty does not yet exist, we mostly self-developed the indicators of each dimension, as elaborated in Section 2.2. For example, in the data control dimension, we asked the following question for the first indicator (DC_1): *If I would share sensitive data, I believe the meta-platform offers me technical means to enforce data usage policies.* We also employed generic indicators such as (DS_G) "*I believe the meta-platform enables sovereignty for the sensitive data that I would share.*" These generic indicators were utilized as an enabler to check the convergent validity of the data sovereignty dimensions; for a detailed view of these indicators, please

[4] The video can be accessed here: https://www.youtube.com/watch?v=9b7iKM3BiMs.
[5] The prototype can be accessed here: https://www.figma.com/proto/KJUcfObwTZp8GaOrTyVhNi/TRUSTS-meta-platform?page-id=2506%3A47793&node-id=2506-50925&viewport=-444%2C-564%2C0.19&scaling=min-zoom&starting-point-node-id=2506%3A50925.

refer to the online supplementary material.[6] Participants answered the questions on a 5-point Likert scale.

Because we have five dimensions contributing to data sovereignty, our model can be seen as a Hierarchical Component Model (HCM). HCM offers several benefits, for example, minimizing the quantity of path model connections, overcoming the bandwidth-fidelity dilemma, and decreasing collinearity among dimensions (Sarstedt et al., 2019). 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 dimension and evaluated their convergent validity, collinearity issues, and relevance (Hair et al., 2021). Following this, we conducted a one-sample t-test in SPSS to assess the extent to which the perceived efficacy of control mechanisms, as reported by participants, is significantly better than the midpoint of our Likert scale.

4 Results

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 aspect 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 for all aspects surpasses 0.5. Consequently, we opted against removing any indicators. As for discriminant validity, the Heterotrait-monotrait ratio (HTMT) for all dimensions 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 final model comprises five data sovereignty dimensions. Specifically, the dimension 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,

[6] The online supplementary material can be accessed here: https://doi.org/10.4121/e4cacfac-31f0-4523-81f4-35383ba958a8.

S_3). We also confirm the validity of a generic data sovereignty construct measured by six indicators.

Next, we calculated the Latent Variable (LV) score for each data sovereignty dimension from the Hierarchical Component Model (HCM) of data sovereignty (Figure 2). The convergent validity is established as ($\beta = 0.713$, $p = 0.00$) and $R^2 >$ 0.5, indicating data these dimensions well represent data sovereignty. The HCM exhibits no collinearity issue, as all dimensions 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 dimensions (OW = 0.38, $p =$ 0.00), we retain the other dimensions since their outer loadings are greater than 0.5, as suggested by Hair et al. (2021).

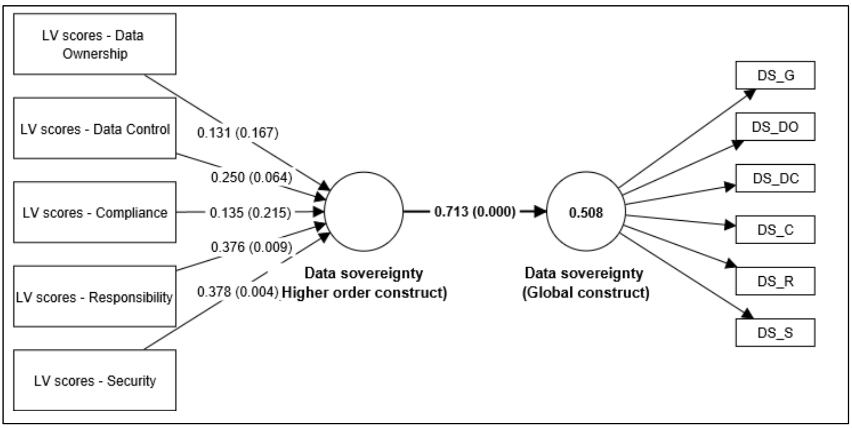

Figure 2: Hierarchical component model of data sovereignty

After validating the HCM measurement model, we conducted a one-sample t-test to compare the mean score of all data sovereignty dimensions against the benchmark value of three. Respondents perceive high data sovereignty when faced with our control mechanisms, as the mean of ownership [$t(92) = 16.1$, $p < 0.01$], control [$t(92) = 16.48$, $p < 0.01$], compliance [$t(92) = 12.41$, $p < 0.01$], security [$t(92) = 9.89$, $p <$ 0.01], and responsibility [$t(92) = 9.06$, $p < 0.01$] are all significantly greater than the benchmark value of three (see Table 1). Detailed elaboration, including raw data, survey indicators, and the complete analytical statistic, is available in the online supplementary material.

Table 1: One-sample t-test calculation (n = 93, test value = 3)

	Descriptive statistic		One-sample t-test		
Dimension	**Mean**	**SD**	**Mean dif.**	***t* value**	***p***
Ownership	4.07	0.64	1.07	16.10	<0.01
Control	4.15	0.67	1.15	16.48	<0.01
Compliance	4.04	0.80	1.04	12.41	<0.01
Security	3.78	0.76	0.78	9.89	<0.01
Responsibility	3.74	0.79	0.74	9.06	<0.01

5 Discussions and conclusions

This research aims to evaluate the perceived efficacy of control mechanisms, namely smart contracts and certification, in enhancing data sovereignty within the context of a meta-platform for data marketplaces. Our findings indicate that the meta-platform prototype containing the control mechanisms is evaluated positively on all data sovereignty dimensions. One possible explanation can be reflected in the proposed hypotheses: smart contracts may play a role in impacting data ownership and control dimensions (H_1); meanwhile, certification may influence compliance, security, and responsibility dimensions (H_2).

We primarily contribute to two streams of literature: 1) multiplatform constellations (or platform ecologies) and 2) data exchange. Specifically, we do so by advancing design knowledge for meta-platforms by providing an initial assessment of the perceived efficacy of control mechanisms in addressing data sovereignty concerns. We are among the first that showcase data sovereignty is evaluated positively in meta-platforms, meaning that, even though meta-platforms exponentially amplify the risks of data exchange, they may still be designed in ways that do not harm data sovereignty.

Considering design knowledge in the problem space, measuring data sovereignty efficacy remains ambiguous and complex. Existing research often equates data sovereignty with control (e.g., Jarke et al., 2019; Otto & Jarke, 2019) while overlooking other dimensions (cf. Hummel et al., 2021). Our findings resolve this tension by offering an alternative approach that captures the multifaceted nature of data sovereignty. To do so, we advance Hummel et al.'s (2021) work in three key aspects: first, by incorporating an added dimension of *responsibility* due to the unique context of meta-platforms with increased governance complexity among data marketplace participants; second, by offering empirical evidence on the collective influence of the five dimensions (ownership, control, security, compliance, and responsibility) on data sovereignty; and third, by enhancing granularity through the introduction of data sovereignty measurement models employed as survey instruments.

Regarding design knowledge in the solution space, our study offers valuable insights into how data providers perceive control mechanisms as valuable for ensuring data sovereignty within the unique context of meta-platforms. Our findings align with existing literature on data exchange, which suggests that smart contracts can technically enable ownership and control (e.g., Saini et al., 2020; Zhang et al., 2018), and certifications can enhance compliance, security, and responsibility (Lansing et al., 2018). However, our contribution extends beyond this general understanding by opening up future discussions for their applicability in distinctive meta-platform characteristics. For instance, smart contracts in meta-platforms are distinct from those in supply chains due to the requirement for seamless interoperability among multiple interconnected marketplaces. This interoperability demands the development of smart contracts that automatically enforce data usage policies and agreements between individual marketplaces and across varied legal and regulatory environments. As a result, smart contracts that leverage interoperable "side chains" emerge as a potential solution to explore (Singh et al., 2020). Alternatively, meta-platforms can offer shared services for data marketplace participants, serving as a backbone infrastructure to facilitate smart contract deployment and alleviate interoperability challenges.

This study has some limitations. First, this study employed a one-sample t-test, thus constraining our comparison to the Likert scale's mid-point. To further improve the validity of the finding, we will continue this research by conducting a between-subject 2x2 factorial experiment. In doing so, we can compare the effect of the presence of these control mechanisms and identify potential interaction effects to confirm the proposed H_1 and H_2. Second, while our study focuses on the most critical dimension 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. Finally, the technical aspects of smart contracts and certification are beyond the scope of our work. To what extent these two control mechanisms can be implemented in a large-scale setting needs further research.

This paper has important policy implications as it suggests ways forward to a single European Data Market while allowing specialized data marketplaces (or data spaces) to exist. This resolves tensions in the European policy to promote a single market for data and interoperable data sharing (e.g., in EU Data strategy, Data Act) and promote verticals/sector-specific data platforms (e.g., the eight verticals in the Digital Europe program), while at the same time, adhere to data sovereignty principles.

Acknowledgments

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–Trusted Secure Data Sharing Space (TRUSTS) and No 825225–Safe Data-Enabled Economic Development (Safe-DEED).

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., 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.

Azkan, C., Möller, F., Meisel, L., & Otto, B. (2020). Service dominant Logic Perspective on Data Ecosystems-a Case Study based Morphology. ECIS 2020 Research Papers, Marrakesh, Morocco.

Bastiaansen, H., Dalmolen, S., Kollenstart, M., & van Engers, T. M. (2020). User-Centric Network-Model for Data Control with Interoperable Legal Data Sharing Artefacts. PACIS 2020 Proceedings, Dubai, the United Arab Emirates.

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).

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

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.

Dalmolen, S., Bastiaansen, H., Somers, E., Djafari, S., Kollenstart, M., & Punter, M. (2019). Maintaining control over sensitive data in the Physical Internet: Towards an open, service oriented, network-model for infrastructural data sovereignty. 6th International Physical Internet Conference (IPIC), London, the United Kingdom.

Duisberg, A. (2022). Legal Aspects of IDS: Data Sovereignty—What Does It Imply? Designing Data Spaces, 61.

European Commission. (2020). A European Strategy for Data. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

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, the Netherlands.

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, 1-18. https://doi.org/10.1080/0960085x.2021.1884009

Fruhwirth, M., Rachinger, M., & Prlja, E. (2020). Discovering Business Models of Data Marketplaces. Proceedings of the 53rd Hawaii International Conference on System Sciences, Hawaii, the United States.

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(4), 377-409. https://doi.org/10.1007/s10506-018-9223-3

Hai, X., & Liu, J. (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.

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.

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

Hodapp, D., & Hanelt, A. (2022). Interoperability in the era of digital innovation: An information systems research agenda. Journal of Information Technology, 0(0), 1-21. https://doi.org/10.1177/02683962211064304

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

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, the United States.

Jarke, M., Otto, B., & Ram, S. (2019). Data sovereignty and data space ecosystems. Business & Information Systems Engineering, 61(5), 549-550.

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, 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.

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.

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), 3.

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.

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.

Menz, N., Resetko, A., & Winkel, J. (2019). IDS Certification explained.

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, 102331. 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.

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

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).

Precht, H., & Gómez, J. M. (2021). Towards GDPR Enforcing Blockchain Systems. Wirtschaftsinformatik 2021 Proceedings, Essen, Germany.

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.

Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's comments: a critical look at the use of PLS-SEM in" MIS Quarterly". MIS quarterly, iii-xiv.

Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system. IEEE Internet of Things Journal, 8(7), 5914-5925.

Santiago, & Laoutaris, N. (2022). A Survey of Data Marketplaces and Their Business Models. SIGMOD Record, 51(3), 18-29.

Sarstedt, M., Hair Jr, J. F., Cheah, J.-H., Becker, J.-M., & Ringle, C. M. (2019). How to specify, estimate, and validate higher-order constructs in PLS-SEM. Australasian marketing journal, 27(3), 197-211.

Saunders, C., Benlian, A., Henfridsson, O., & Wiener, M. (2020). MIS Quarterly Research Curation: IS Control & Governance. MIS quarterly.

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.

Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., & Choo, K.-K. R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. Journal of Network and Computer Applications, 149, 102471.

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

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, 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, Timişoara, Romania.

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.

Yang, F., & Wang, Y. (2019). Research Status and Trend Analysis of Learning Resource Aggregation in the Era of Big Data. Moscow, Russia.

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

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, 121128. https://doi.org/10.1016/j.techfore.2021.121128

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the internet of things. IEEE Internet of Things Journal, 6(2), 1594-1605.