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

Online Appendices

by

Antragama Ewa ABBAS

Table of contents

List of figures

List of tables

Online Appendix 1. List of literature

Table 1.1 presents a list of literature reviewed in Chapter 6 to examine control mechanisms to enhance data sovereignty.

Table 1.1 List of literature

No	Source	Aim	Included?
1	(Hellmeier & von Scherenberg, 2023)	This research discusses the distinction between data, digital, and technological sovereignty.	Yes
2	(Aydin & Bensghir, 2019)	This study examines how digital technologies are reshaping the traditional notion of sovereignty and explores how the proliferation of digital data is transforming power relations between states, individuals, and non-state actors.	No
3	(Banse, 2021)	This study discusses security measures to enhance data sovereignty in the cloud context, emphasizing the utilization of confidential computing, remote attestation, and integrity verification.	Yes
4	(Bauer et al., 2019)	This research designs a privacy framework, named "CAN't," for ensuring privacy over shared data at the machinery level in the domain of smart farming.	Yes
5	(Calzada, 2021)	This article discusses data cooperatives and data sovereignty, which are closely interrelated concepts that have the potential to challenge surveillance capitalism in the smart city context.	Yes
6	(Chapdelaine & McLeod Rogers, 2021)	This research explores the complexities of regulating media content in the digital era, explicitly focusing on the Canadian context. It underscores the need for state regulation to balance personal data extraction practices, national cultural sovereignty, and citizens' interests.	No
7	(Chen et al., 2020)	This paper introduces a Decentralized Data Access Control (DDAC) framework that utilizes Atomicity, Consensus, and Confidentiality (ACC) constraints to manage access controls on consortium blockchains.	Yes
8	(Corbett & Cochrane, 2020)	This article investigates Participatory Geoweb, a tool for non-experts to provide geographically referenced information to tackle social and environmental challenges.	No
9	(Couture & Toupin, 2019)	The paper explores the concept of "sovereignty" within the digital technology context, considering the viewpoints of traditional states, indigenous peoples, and social movements. It characterizes data sovereignty as the assertion of collective authority over digital information and infrastructure.	No
10	(Cuno et al., 2019)	This paper proposes Urban Data Space (UDS) for data exchange in the smart city context based on relevant ICT reference architectures.	Yes
11	(Dabrock, 2020)	The paper presents AI ethics principles of explainability and enforceability to strengthen data sovereignty.	No
12	(Esposito et al., 2016)	This research discusses the *encryption-at-rest* approach in the cloud context to maintain data sovereignty.	Yes
13	(Esposito et al., 2019)	The study proposes a solution that uses encryption with geo-location to generate encryption and decryption keys, adding a security layer to smart city infrastructure by limiting data access to specific locations.	Yes
14	(De Filippi & McCarthy, 2012)	This paper discusses how centralization may harm the data sovereignty of individuals by decreasing their control over their resources data, threatening privacy and	Yes

No	Source	Aim	Included?
		personal freedom, and disrespecting national jurisdiction boundaries.	
15	(Ethikrat, 2017)	The German Ethics Council report discusses the role of big data in healthcare, outlining both the benefits and risks of its use. The Council advocates for a governance framework prioritizing data sovereignty by respecting personal autonomy and confidentiality, ensuring fairness, and fostering responsibility.	Yes
16	(Gupta et al., 2020)	This research proposes a novel "SECure" framework inspired by the Environment, Society, and Governance (ESG) framework to create eco-socially responsible AI systems.	Yes
17	(Hartsch et al., 2021)	The study examines the impact of legal, social, and economic elements on incorporating data from harvester production into Germany's wood supply chain.	Yes
18	(Hong & Kim, 2020)	This study introduces a self-sovereign identity (SSI) model based on blockchain technology, which is built to align with the OAuth 2.0 standard.	Yes
19	(Hummel et al., 2018)	This study identifies data sovereignty as a benchmark for managing socio-technical systems.	Yes
20	(Hummel et al., 2021)	This study reviews 341 publications to clarify the concept of data sovereignty and its implications.	No
21	(Irion, 2012)	The paper discusses data sovereignty as a promising concept in the cloud context for governments as it balances information virtualization with their continuous need for exclusive authority and control.	Yes
22	(Jarke et al., 2019)	This paper summarizes the articles in the special issue of "Data Sovereignty and Data Space Ecosystems" in *Business & Information Systems Engineering*.	Yes
23	(Kushwaha et al., 2020)	The study investigates how different nations protect their cloud-hosted government data from foreign law enforcement, particularly under international regulations like the US CLOUD Act.	Yes
24	(Lauf et al., 2022)	This research identifies several tensions in data sovereignty and recommends appropriate solutions to tackle these challenges.	Yes
25	(Lian, 2021)	This article discusses the need for swift enactment of global data rights legislation, focusing on China's potential to lead in the digital economy sector.	Yes
26	(Mannhardt et al., 2019)	This study introduces a model to safeguard the privacy of *event* data, particularly in process mining, using differential privacy techniques.	Yes
27	(Mark, 2019)	The study examines Amsterdam's DrukteRadar project, which uses smart information systems (SIS) to manage crowd levels and problem hotspots, and identifies ethical issues, including data accuracy, privacy, and data ownership. The paper reveals the project's strategies for ensuring data sovereignty, mitigating algorithmic inaccuracies, and protecting citizen privacy.	Yes
28	(Martens & Zscheischler, 2022)	Through a discourse analysis of an online conference, this study explores digital transformation governance in agriculture. Data sovereignty is discussed among the key challenges.	Yes
29	(Mawere & Van Stam, 2020)	The study explores data sovereignty from an African perspective, specifically focusing on Zimbabwean health systems.	Yes
30	(Micheli et al., 2020)	This research investigates four emerging models of data governance for the data economy.	No

No	Source	Aim	Included?
31	(De Mooy, 2017)	The study discusses the effectiveness of current data-protection regimes based on individual control and proposes approaches to data sovereignty.	Yes
32	(Munoz-Arcentales et al., 2019)	This research suggests a framework for managing access and usage in data-sharing ecosystems across various parties to maintain data sovereignty.	Yes
33	(Nagel & Lycklama, 2021)	The paper advocates for establishing “data spaces” across sectors, fostering data sharing, and creating a Data Economy.	Yes
34	(Nast et al., 2020)	The paper presents an approach for integrating Internet of Things (IoT) devices into the International Data Spaces (IDS) connector.	Yes
35	(Nugraha et al., 2015)	This research defines data sovereignty requirements from the perspective of nation-states, particularly Indonesia.	Yes
36	(Otto, 2019)	The article discusses the importance of data sovereignty in business ecosystems.	No
37	(Otto & Burmann, 2021)	The paper discusses the importance of balancing the common good and individual interests in the use of data, preventing a concentration of economic power in platform giants.	Yes
38	(Pedreira et al., 2021)	The study systematically reviews cybersecurity attacks, vulnerabilities, and defense strategies in Industry 4.0. It reveals data sovereignty as a pressing issue, with initiatives like IDS and GAIA-X aiming to address these challenges.	Yes
39	(Peterson et al., 2011)	The paper introduces data sovereignty in the cloud context by relating data authenticity to geographical location. Potential control mechanisms: provable data possession	No
40	(Plateaux et al., 2013)	This paper discusses the security and privacy concerns inherent in e-health information systems that handle large volumes of sensitive data, emphasizing the importance of data sovereignty.	Yes
41	(Polatin-Reuben & Wright, 2014)	The paper explores the implications and risks associated with various interpretations of data sovereignty.	Yes
42	(Redeker et al., 2020)	This research proposes technical infrastructure to ensure data sovereignty in the Asset Administration Shell context.	Yes
43	(Ruparelia, 2016)	This book mentions data sovereignty as an issue in the cloud computing context.	Yes
44	(Sarabia-Jácome et al., 2019)	This study presents a seaport data space to enhance interoperability among stakeholder systems leveraging the Industrial Data Space (IDS) architecture.	Yes
45	(Schleicher et al., 2011)	The study presents an approach to modeling compliant business processes, focusing on data sovereignty and compliance requirements in cloud computing.	No
46	(Singi et al., 2020)	The paper presents a framework based on knowledge graphs for governing data sovereignty, designed to categorize data and pinpoint applicable laws.	No
47	(Tan et al., 2023)	This study examines Self-Sovereign Identity, addressing its challenges and open issues such as efficient key management, scalability, and interoperability.	Yes
48	(Kukutai & Taylor, 2016)	This book discusses data sovereignty, focusing on issues of the rights of indigenous communities to manage their cultural heritage, traditional knowledge, and intellectual property.	Yes
49	(Taylor, 2020)	This article examines the global trend of “Data Localization,” which mandates data to be stored and	No

No	Source	Aim	Included?
		processed within its country of origin, potentially impacting technologies like cloud services, big data, AI, and IoT.	
50	(Vaile, 2014)	This paper examines the impact of Snowden's revelations on the understanding of data sovereignty in cloud technologies. It focuses on jurisdictional questions concerning data location and control.	Yes
51	(Zieglmeier & Pretschner, 2023)	This study designs a framework to improve the trustworthiness of software systems while providing data subjects with greater oversight over how their data is processed and used.	No
52	(Zrenner et al., 2019)	The study designs a usage control architecture to enhance data sovereignty, using a case from the German automotive industry.	Yes
53	(Schäfer et al., 2023)	This paper discusses five technologies to solve trust challenges in data exchange.	Yes
54	(Schmidt et al., 2022)	This paper reviews privacy-enhancing technologies to ensure data sovereignty.	Yes
55	(Scheider, Lauf, Möller, et al., 2023)	This article proposes reference architecture for data sovereignty.	Yes
56	(Scheider, Lauf, & Geller, 2023)	This article discusses design principles for sovereign data exchange.	Yes

Online Appendix 2. Prototype evaluation

This online appendix details the prototype evaluation conducted in Chapter 7. We improved the developed prototype through a three-step evaluation cycle. The first cycle, conducted on 28 April 2022, involved 24 MSc students in a hybrid class setting. The primary objective was to gather early feedback on usability aspects. The second cycle, held on May 13, 2022, engaged six researchers in an in-person workshop to test 2nd version of the prototype. The third cycle step occurred on 01 June 2022 and involved 39 practitioners working on a data marketplace meta-platform project. The workshop was conducted in person. This final step primarily focused on obtaining feedback concerning the two control mechanisms: smart contracts and onboarding certification. We elaborate on the details of the evaluation cycle in the following sub-sections.

2.1 Cycle 1

The first evaluation cycle occurred as part of an interactive lecture in a master's course at TU Delft. In this cycle, early feedback for usability improvement was collected through a discussion conducted in a hybrid class setting. After a short introduction to the key concept and scenario, the students explored the zero draft of a working prototype of the TRUSTS meta-platform. When exploring, they took notes about a) points for improvements and b) challenges they faced while using the prototype. Afterward, they entered their views on menti.com. From that, a follow-up discussion emerged. The researcher also implicitly observed any difficulties that occurred in the exploration. Table 2.1 summarizes the discussed improvement points and prototype adjustments after Cycle 1.

Table 2.1. Feedback from the first evaluation cycle

Category	Improvement point	Prototype adjustment
Preparation stage	The Bit.ly shortening link is case-sensitive and confusing.	Embed the link directly into the questionnaire to automatically open a new tab when clicking.
	Participants are unsure if they need to create an account in Figma to use the prototype.	Clearly state in the task introduction that creating an account is unnecessary to use the prototype.
	The prototype only works in desktop mode; uninformed participants may struggle.	▪ Inform participants to use a PC or desktop for the online experiment. ▪ Use a Qualtrics check function to ensure participants use the appropriate device.
Concept clarity	Participants do not fully understand the concepts of meta-platform and smart contracts.	Create a video instruction for self-paced learning and embed a conceptual model in the survey for reference.
Performance	Large image size slows down prototype performance.	Use compressed images to improve prototype performance.
Visual clarity	I_1.2.2 Sign in: Unfriendly color contrast and unnecessary "Chart" icon.	Improve color contrast and remove the "Chart" icon in the I_1.2.2 interface.
	I_1.2.3 View dashboard: Unrealistic line chart for continuous revenue streams.	Change the line chart into a bar chart.
	I_2.4.5 View updated dashboard: Inability to see the result of the uploaded dataset.	Incorporate the uploaded dataset on the dashboard.
	I_2.2.4 Define terms of use: Difficulty in deciding the price for the dataset.	Include a recommendation for data pricing.
	I_3.1.1 Select a request	Create better dummy information.

Category	Improvement point	Prototype adjustment
	Duplicate data consumer information.	
	I_4.1.2 View data usage: Unclear provenance graph.	Redraw the provenance graph for better visualization of data usage.
Navigation	Difficulty in finding the next page.	Develop interface I_1.1.1 to provide explicit instructions for navigating to the next page.
	Difficulty in scrolling down.	Inform data providers on interface I_1.1.1 to "scroll down to view the entire page" due to Figma's scroll-down functionality limitations.
Others	Unresponsive web display.	Fix the prototype setting in Figma.
	Spelling errors.	Correct spelling errors.

2.2 Cycle 2

After adjusting the prototype based on the improvement points from the first evaluation cycle, the second version of the TRUSTS meta-platform prototype was ready for testing. In this version, we also created a video explanation to better explain the concept of meta-platform. Therefore, we divided the evaluation activity of Cycle 2 into two parts: the video explanation and the prototype exploration.

In the beginning, participants were asked to watch a 5-minute video explanation together, giving them an overview of the prototype and its features. After watching the video, they were encouraged to take notes on any aspects that could be improved or clarified, spending another 5 minutes on this task.

Following the video explanation, participants were given 10 minutes to explore the prototype by following the task instructions. As they navigated through the prototype, they were asked to take notes and write down any suggestions. After completing the self-paced exploration, they had an additional 5 minutes to finalize their notes.

Once the feedback collection phase was completed, all the notes were displayed on a wall for all participants to review (See Figure 2.1 for the workshop activity illustration). The group then collaborated to prioritize the most critical feedback and suggestions for refining the video and prototype. This process allowed the participants to vote on which improvements should be implemented in the next iteration of the research instrument.

Figure 2.1. The illustration for the workshop activity

The participants' feedback yielded three main takeaways from the video explanation. First, they noted that the sound quality of the video explanation could be improved. For example, including subtitles would enhance clarity and accommodate participants with varying auditory processing or language proficiency levels. Second, the participants observed that the narrator in the video sometimes blocked the text and images on the interface. Adjusting the placement or size of the narrator could resolve this issue. Finally, the participants observed that the prototype's images and text were too small, potentially impeding usability and the overall user experience. Addressing these concerns by increasing images and text size would enhance readability and facilitate better engagement with the prototype.

The second evaluation cycle also revealed three key takeaways concerning the prototype itself. First, participants reported that navigation issues hindered their effective use of the platform. For instance, some only discovered the button to go to the next prototype after 10 minutes. Participants requested clearer instructions for navigating the pages, such as guidance on returning to the landing page. Providing consistent and clear instructions throughout the prototype is crucial to improve navigation. Second, unclear task descriptions contributed to difficulties in understanding the actions required from data providers. Participants reported confusion regarding Task 1, specifically the need to open another browser. Additionally, they were uncertain about the meaning of certain terms or phrases. Finally, participants felt the allocated time for exploring the prototype was insufficient. They suggested a longer duration, perhaps 15-20 minutes, would be more appropriate for fully engaging with the platform and completing the tasks.

2.3 Cycle 3

We conducted the third evaluation cycle to discuss certification and smart contracts in detail. We performed this evaluation during the TRUSTS plenary meeting held in Vienna. The workshop involved participants from multiple work packages within the broader TRUSTS consortium. To facilitate this process, they were given access to the Figma prototype and instructed to explore it for 10 minutes. After becoming familiar with the features, participants were requested to provide feedback on the Miro board.

We received some minor feedback regarding the visualization of certification in the prototype. For instance, 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 IDS components and organization 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 influence data providers or 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.

Concerning the smart contracts, one key point was clarifying and redrawing the data provenance graph to represent the data usage better. Additionally, adding the feature to verify data usage compliance is considered technically challenging. However, including this feature within the TRUSTS meta-platform prototype allows us to demonstrate the meta-platform's control mechanisms. By highlighting the smart contracts' capabilities, we emphasize the potential advantages they bring to the meta-platform—despite the complexities and challenges associated with their implementation. After revising adjusted the prototype, we came up with the final version of the prototype.

Online Appendix 3. Prototype interfaces

Online Appendix 3 details tasks for data providers, including related interfaces and their descriptions, and design principles.

3.1 Task 1: Familiarizing data providers with the prototype

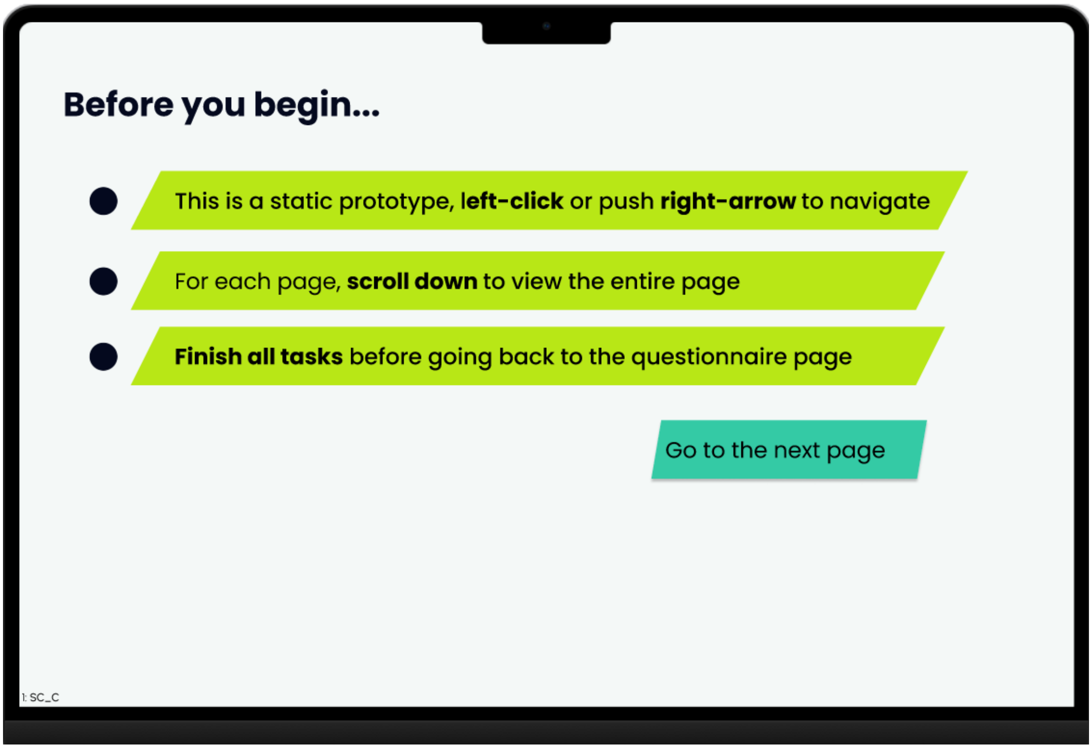
Task 1 familiarizes data providers with the prototype by providing essential information and context for interacting with the TRUSTS meta-platform. Table 3.1 shows the division of this task into three subtasks. The first subtask describes the general guidance to use the prototype. The second subtask 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 (KPIs) 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 3.1. Task 1 description

ID	Interface	Description
Subtask 1.1: Introducing Task 1		
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.

3.1.1 Introducing Task 1

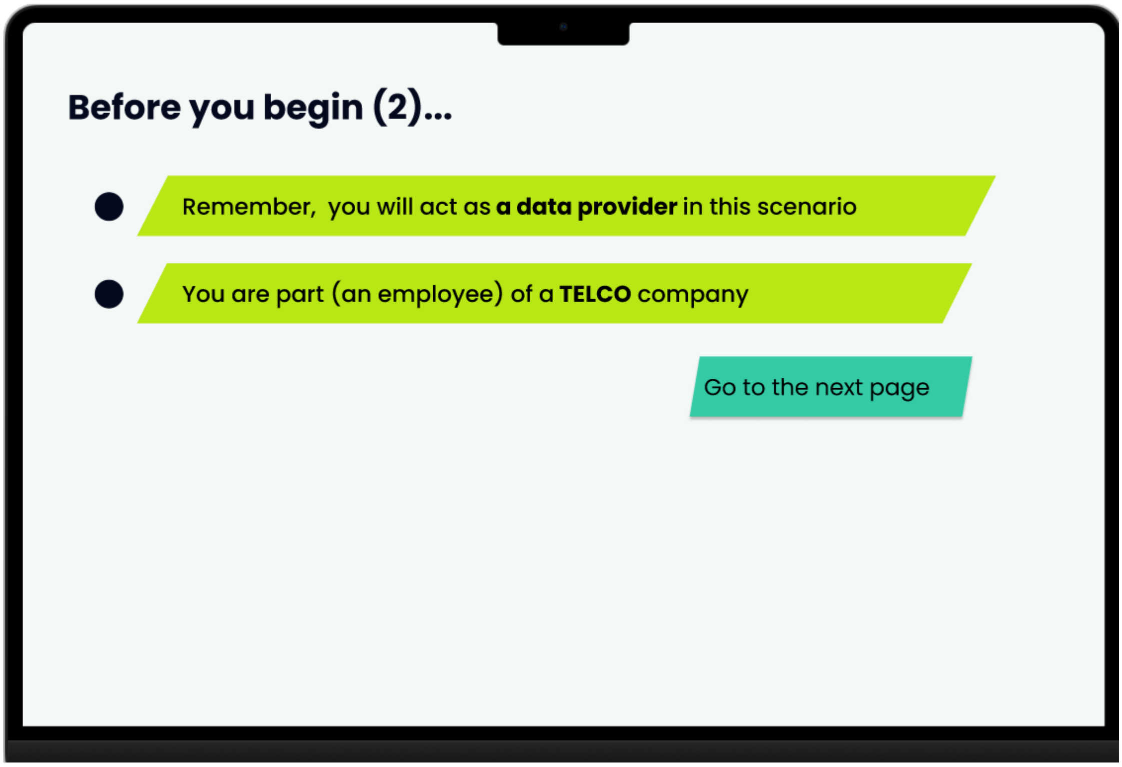
Subtask 1.1 includes three interfaces that help data providers familiarize themselves with the TRUSTS meta-platform prototype. Interface *I_1.1.1* offers guidance on navigating the static prototype, such as using left-click or right-arrow to move through the interfaces and scrolling down to view entire pages (Figure 3.1). Figure 3.2 highlights the user role as a data provider from a TELCO company, as shown in Interface *I_1.1.2*. Figure 3.3 shows Interface *I_1.2.3,* informing two other subtasks that data providers must perform: exploring the homepage and signing in as a data provider. Overall, the interfaces in Task 1 ensure that data providers understand their roles and expectations while interacting with the prototype.



Before you begin...

- This is a static prototype, **left-click** or push **right-arrow** to navigate
- For each page, **scroll down** to view the entire page
- **Finish all tasks** before going back to the questionnaire page

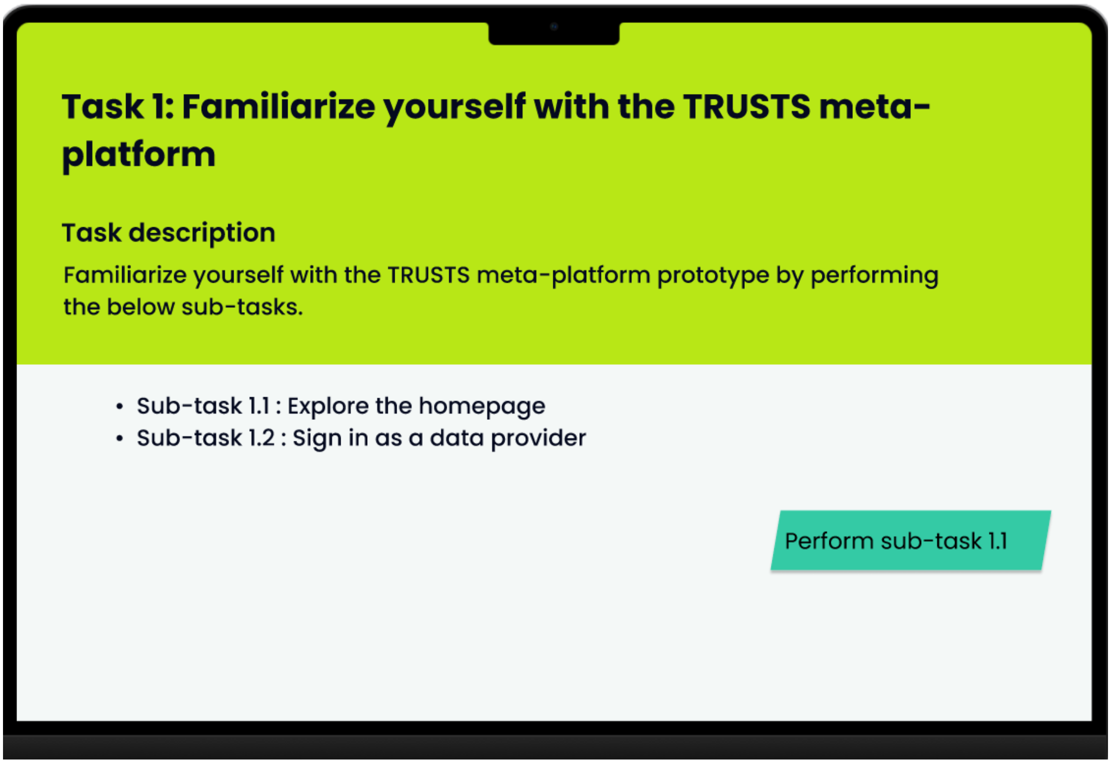
Figure 3.1. I_1.1.1: Before you begin



Before you begin (2)...

- Remember, you will act as **a data provider** in this scenario
- You are part (an employee) of a **TELCO** company

Figure 3.2. I_1.1.2: Before you begin (2)



Task 1: Familiarize yourself with the TRUSTS meta-platform

Task description

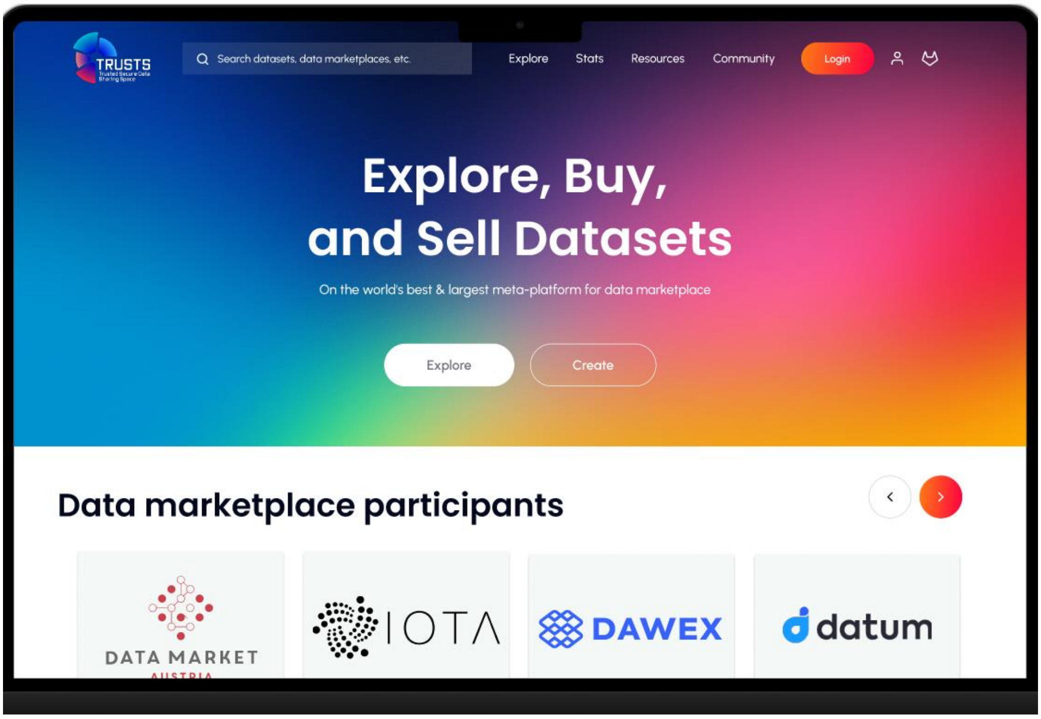
Familiarize yourself with the TRUSTS meta-platform prototype by performing the below sub-tasks.

- Sub-task 1.1 : Explore the homepage
- Sub-task 1.2 : Sign in as a data provider

Figure 3.3. I_1.2.3: Task 1 description

3.1.2 Subtask 1.2: Exploring the homepage

Subtask 1.2 requires data providers to examine the TRUSTS meta-platform homepage. The homepage (Figure 3.4) shows various data marketplace participants who joined the TRUSTS meta-platform, such as Data Market Austria, IOTA, DAWEX, and Datum. The TRUSTS business processes section informs the next steps for data providers, including uploading a dataset, selecting marketplaces, creating contracts, and controlling shared data (Figure 3.5).

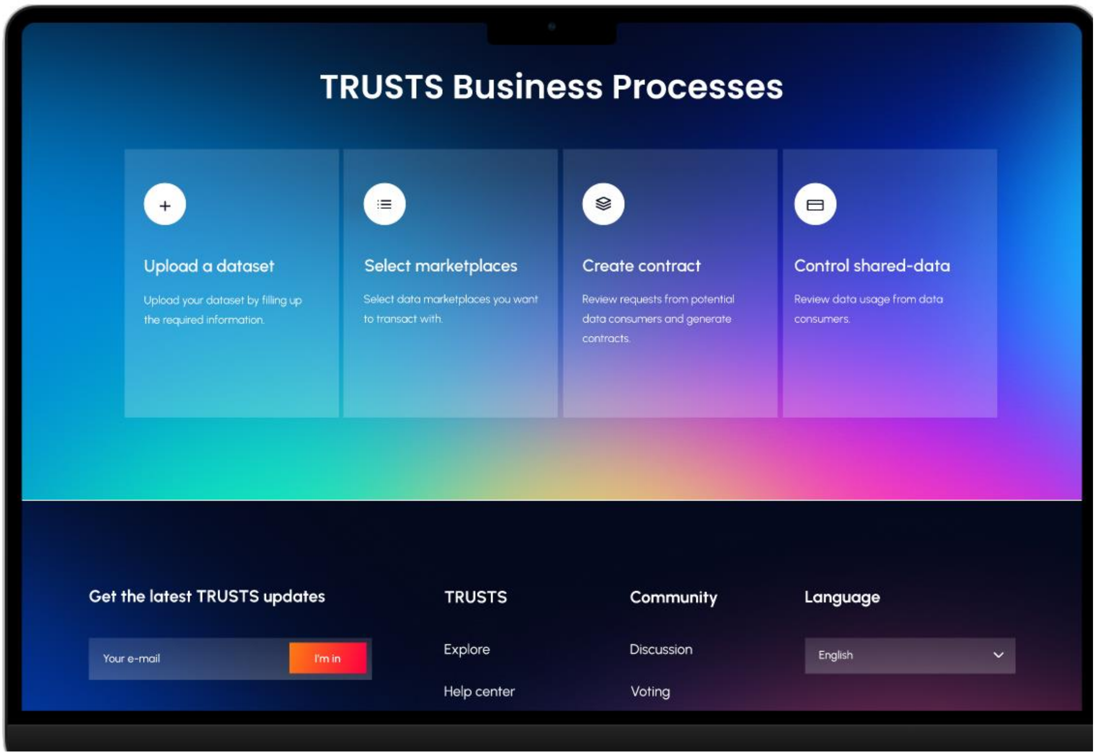


Explore, Buy, and Sell Datasets

On the world's best & largest meta-platform for data marketplace

Data marketplace participants

Figure 3.4. I_1.2.1: Explore homepage (1)


TRUSTS Business Processes

Upload a dataset

Upload your dataset by filling up the required information.

Select marketplaces

Select data marketplaces you want to transact with.

Create contract

Review requests from potential data consumers and generate contracts.

Control shared-data

Review data usage from data consumers.

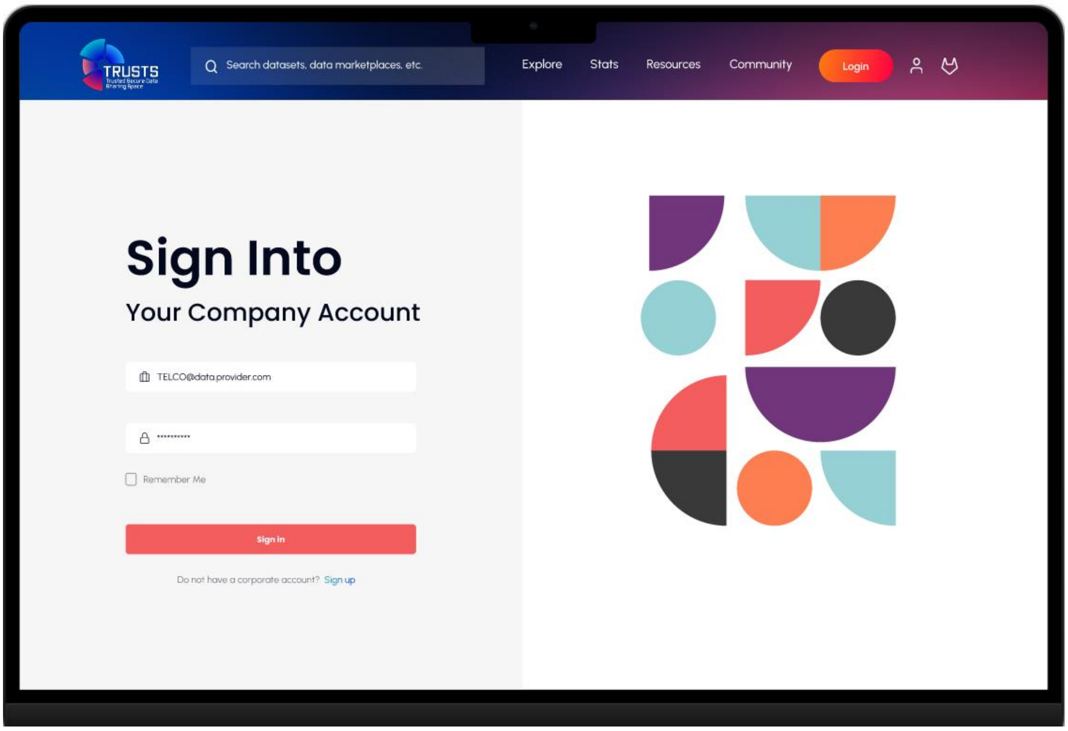
Get the latest TRUSTS updates

Your e-mail

Figure 3.5. I_1.2.1: Explore homepage (2)

3.1.3 Subtask 1.3: Signing in as a data provider

Subtask 1.3 instructs data providers on how to sign in as a data provider. Interface *I_1.3.1* asks data providers to sign in by entering their *company ID* and *password*. The interfaces also include a “Remember Me” and a “Forgot password?” link to help data providers retrieve their login credentials. Moreover, the interface offers a sign-in alternative for data providers who do not possess a corporate account (refer to Figure 3.6).



Sign Into

Your Company Account

TELCO@data.provider.com

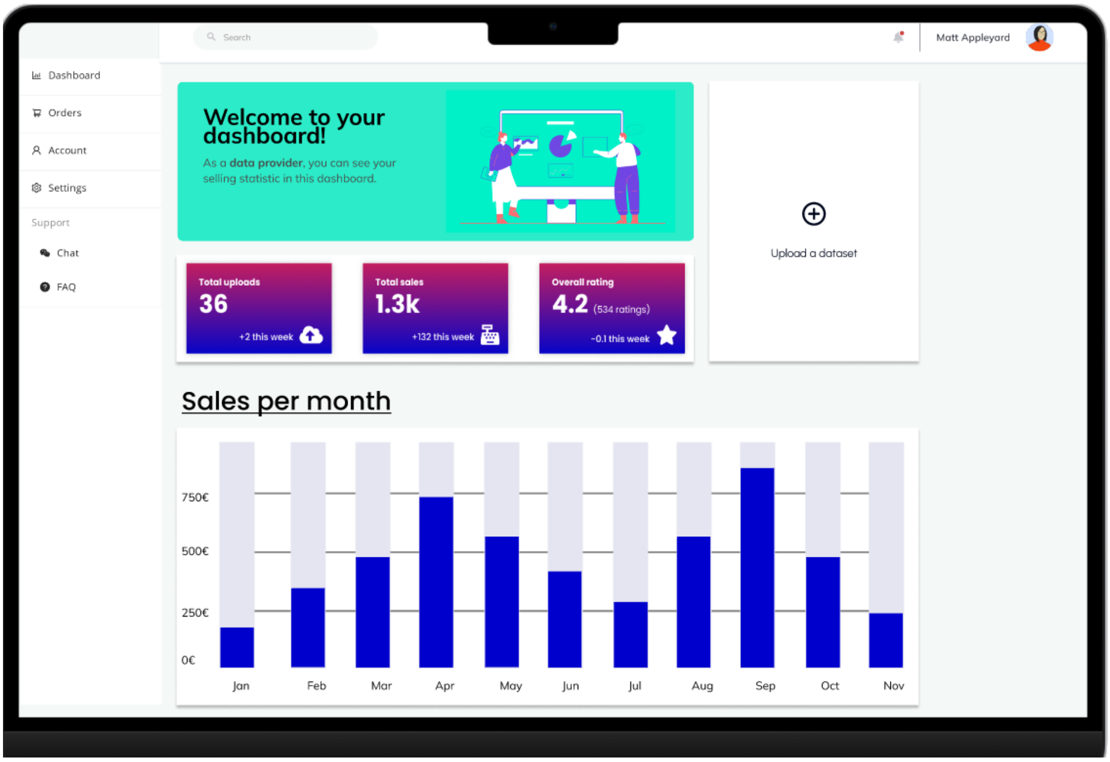
••••••••••

□ Remember Me

Do not have a corporate account? Sign up

Figure 3.6. I_1.3.1: Sign in

Data providers are redirected to their personalized dashboard after successfully signing in (see Figure 3.7). The dashboard displays essential metrics, including upload counts, sales figures, and overall ratings. Furthermore, data providers can upload datasets through the dashboard.



Welcome to your dashboard!

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

Figure 3.7. I_1.3.2: View dashboard

3.2 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 through preparing their shared dataset (refer to Table 3.2). Subtask 2.1 requires data providers to complete the provided template to describe their dataset accurately. 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 by the meta-platform. Finally, 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.

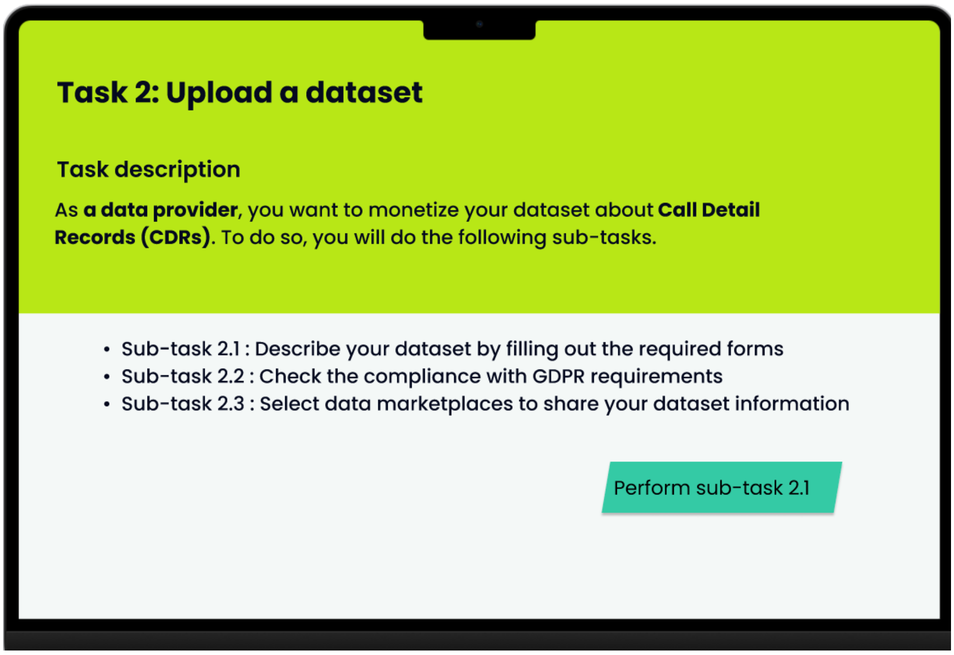
Table 3.2. Task 2 description

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 • DP_DO_M$_2$: Guided data ownership configuration
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.	

ID	Interface	Description	
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.	• DP_DO_M$_3$: Customizable ownership settings
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 the International Data Space Association (IDSA) as 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.	

3.2.1 Introducing Task 2

Data providers first engage with Interface *I_2* to get an overview of Task 2 (Figure 3.8).



Task 2: Upload a dataset

Task description

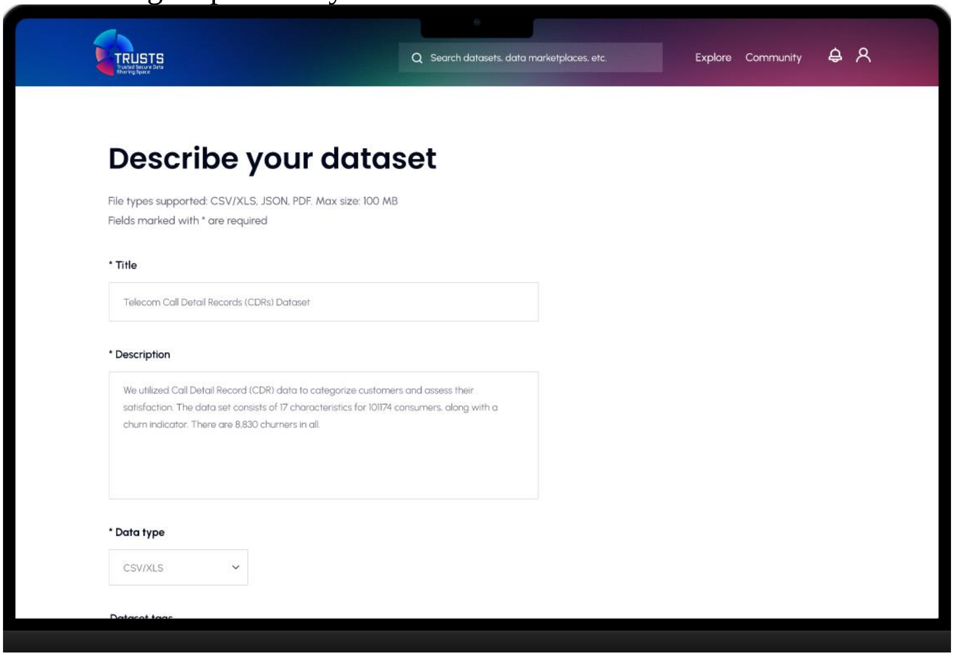
As **a data provider**, you want to monetize your dataset about **Call Detail Records (CDRs)**. To do so, you will do the following sub-tasks.

- Sub-task 2.1 : Describe your dataset by filling out the required forms
- Sub-task 2.2 : Check the compliance with GDPR requirements
- Sub-task 2.3 : Select data marketplaces to share your dataset information

Figure 3.8. I_2: Task 2 description

3.2.2 Subtask 2.1: Describing the dataset by filling out the template

In this subtask, data providers interact with a template designed to collect information about their dataset. Data providers start to interact with Interface *I_2.2.1* (Figure 3.9). The prototype interface specifies the supported file types (CSV/XLS, JSON, PDF) and the maximum file size (100 MB). Fields marked with an asterisk (*) must be filled out. Data providers must provide a descriptive title for their dataset, give a detailed description, and select the appropriate data type. Furthermore, data providers must include dataset tags separated by commas.



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

Describe your dataset

File types supported: CSV/XLS, JSON, PDF. Max size: 100 MB
Fields marked with * are required

* Title

Telecom Call Detail Records (CDRs) Dataset

* 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.

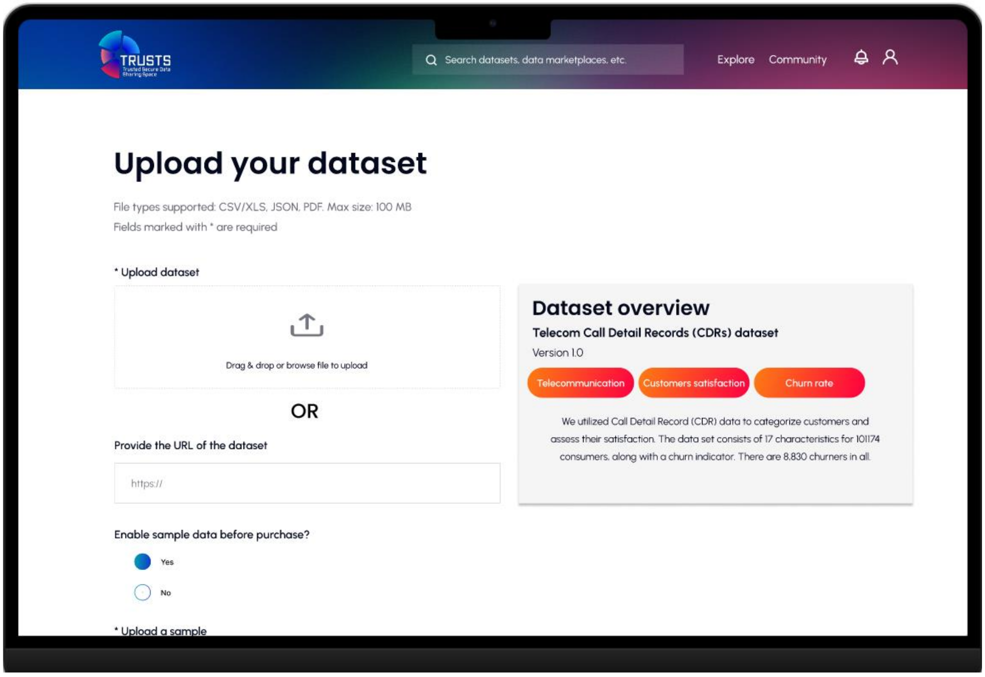
* Data type

CSV/XLS

Dataset tags

Figure 3.9. I_2.2.1: Describe dataset

Afterward, data providers are asked to upload their dataset in Interface *I_2.2.2* by dragging and dropping, browsing a file, or providing its Uniform Resource Locator (URL) (see Figure 3.10). They can also enable and upload sample files. This interface also provides the dataset overview on the proper interface, generated by information from the previous interface *(I_2.2.1).*



Upload your dataset

File types supported: CSV/XLS, JSON, PDF. Max size: 100 MB
Fields marked with * are required

* Upload dataset

Drag & drop or browse file to upload

OR

Provide the URL of the dataset

https://

Dataset overview

Telecom Call Detail Records (CDRs) dataset
Version 1.0

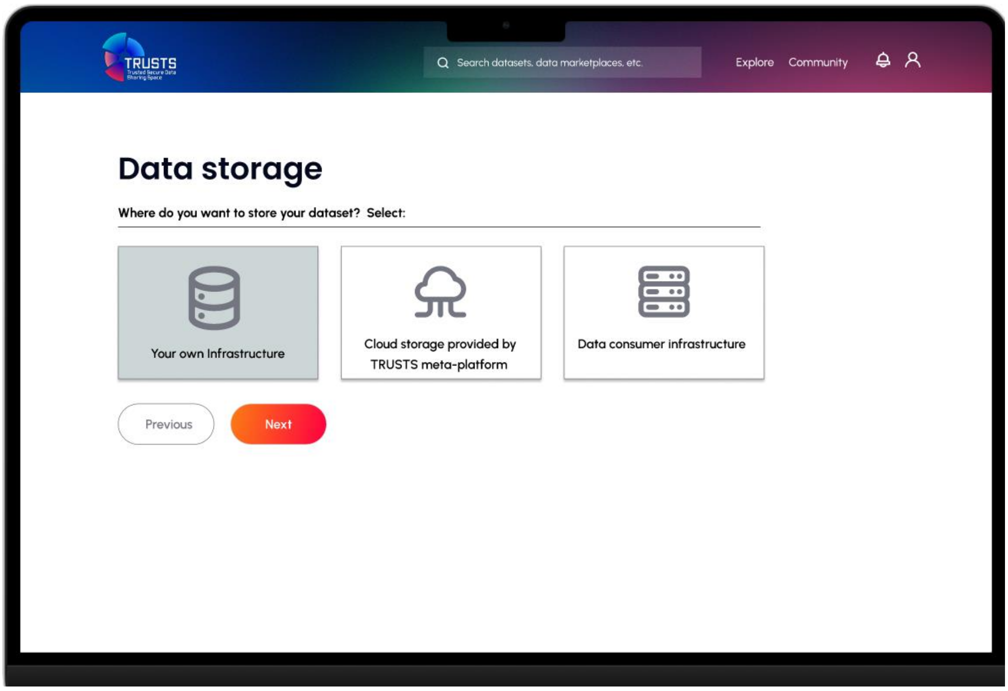
We utilized Call Detail Record (CDR) data to categorize customers and assess their satisfaction. The data set consists of 17 characteristics for 101174 consumers, along with a churn indicator. There are 8,830 churners in all.

Enable sample data before purchase?
● Yes
○ No

* Upload a sample

Figure 3.10. I_2.2.2: Upload dataset

After uploading the dataset, data providers use Interface *I_2.2.3* (Figure 3.11) to select their preferred data storage option. The available choices include “Your own Infrastructure,” “Cloud storage provided by TRUSTS meta-platform,” and “Data consumer infrastructure.” The user opts for “Your own Infrastructure” as their desired data storage location in this demonstration.



Data storage

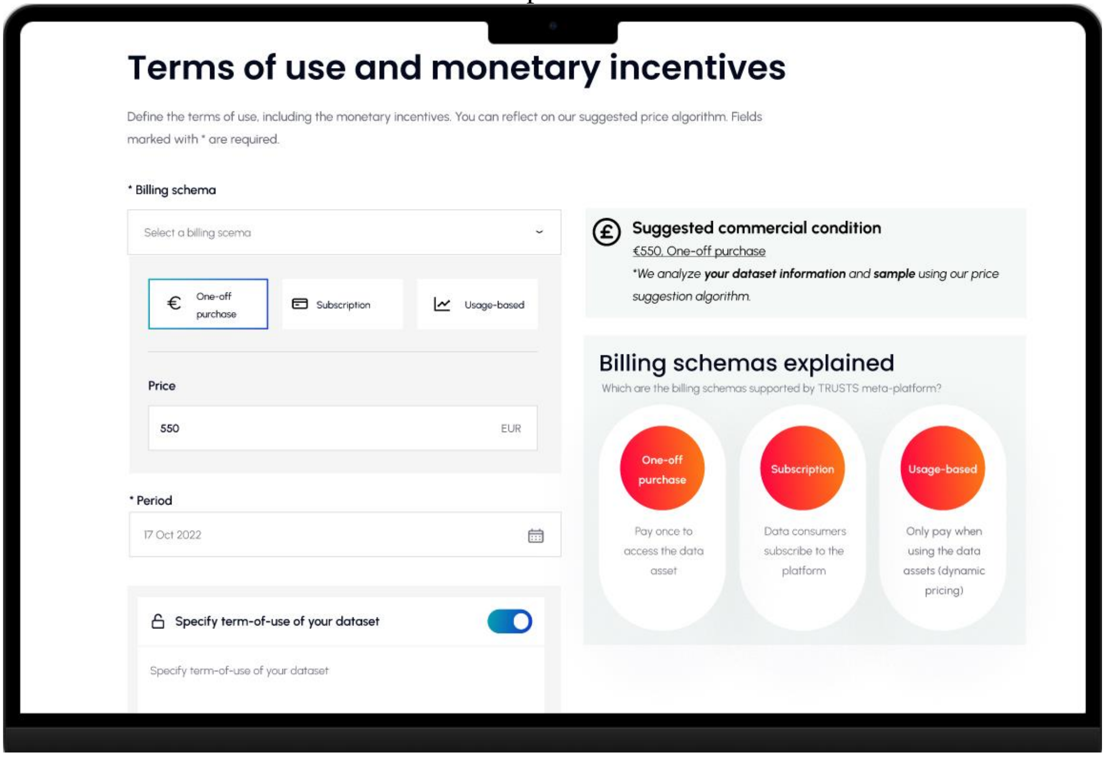
Where do you want to store your dataset? Select:

Your own Infrastructure
Cloud storage provided by TRUSTS meta-platform
Data consumer infrastructure

Figure 3.11. I_2.2.3: Select data storage

Next, data providers interact with *I_2.2.4*, where they are asked to define their dataset's terms of use and monetary incentives (refer to Figure 3.12). The interface is divided into two parts. On the left side, data providers must select a billing schema from the available options: one-off purchase, subscription, or usage-based. They also need to set a price, period, and specify any terms of use associated with their dataset.

On the right side of the interface, there is a suggested commercial condition generated by the meta-platform's price suggestion algorithm, which takes into account the dataset information and sample provided. In this case, the suggested condition is €550 for a one-off purchase. Below the suggestion, there is a brief explanation of the billing schemas supported by the TRUSTS meta-platform, helping data providers understand the differences between the options and make an informed decision.



Terms of use and monetary incentives

Define the terms of use, including the monetary incentives. You can reflect on our suggested price algorithm. Fields marked with * are required.

* Billing schema

Select a billing scema

Price

550 EUR

* Period

17 Oct 2022

Specify term-of-use of your dataset

Specify term-of-use of your dataset

Suggested commercial condition

€550. One-off purchase

We analyze **your dataset information and **sample** using our price suggestion algorithm.*

Billing schemas explained

Which are the billing schemas supported by TRUSTS meta-platform?

One-off purchase
Pay once to access the data asset
Subscription
Data consumers subscribe to the platform
Usage-based
Only pay when using the data assets (dynamic pricing)

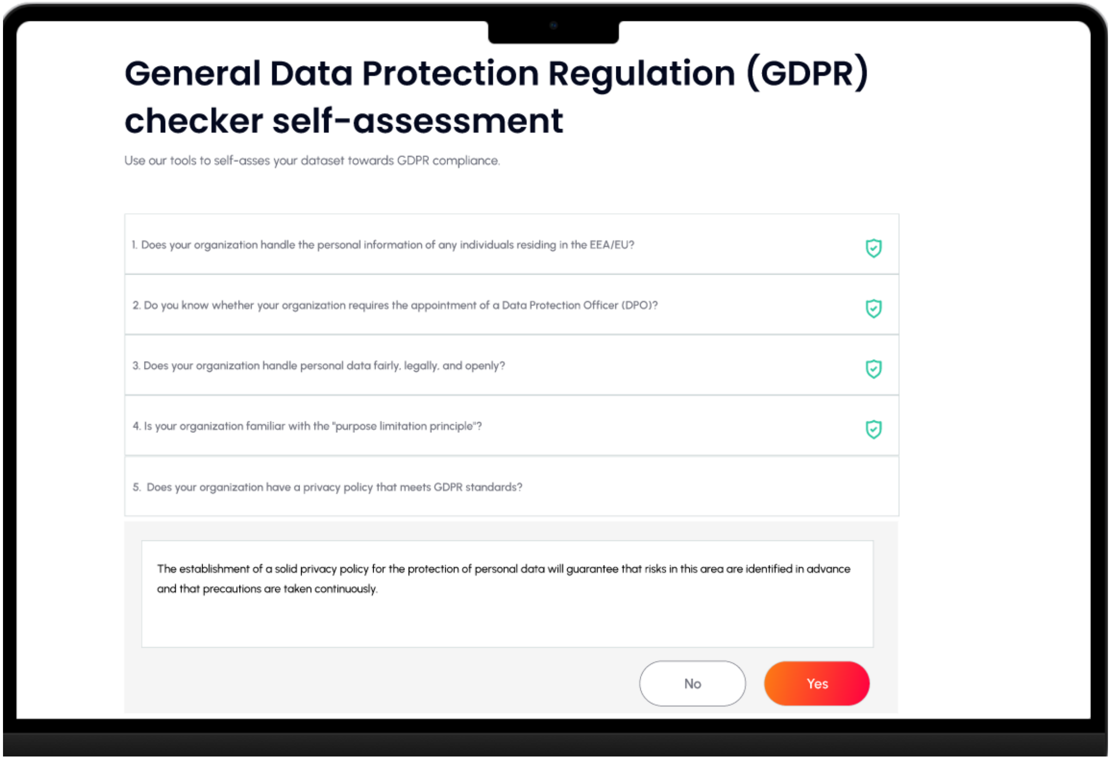
Figure 3.12. I_2.2.4: Define terms of use

The interfaces developed for Subtask 2.1 embeds four design principles of smart contracts: DP_DO_M$_1$ (A terms-of-use template with metadata generation), DP_DO_M$_2$ (Guided data ownership configuration), and DP_DO_M$_3$ (Customizable ownership settings).

The interfaces *I_2.1.1* (Describe dataset), *I_2.1.2* (Upload dataset), *I_2.1.3* (Select data storage), and *I_2.1.4* (Define terms of use) show DP_DO_M$_1$ principle employed in the prototype. For DP_DO_M$_2$, Interface *I_2.2.4* (Define terms of use) demonstrates guided data ownership configuration. By providing suggested commercial conditions and billing schemas, the meta-platform assists data providers in understanding their options and making informed decisions regarding data ownership. Interface *I_2.2.4* displays customizable ownership settings for DP_DO_M$_3$. Data providers can fill out the "Specify terms of use for your dataset" form to define their requirements beyond the provided options.

3.2.3 Subtask 2.2: Checking GDPR compliance

In Subtask 2.2, data providers utilize the TRUSTS meta-platform's self-assessment tool, *I_2.3.1*, to check their dataset's GDPR compliance. The self-assessment tool covers a variety of GDPR compliance questions, including handling of personal information of individuals residing in the European Economic Area (EEA) / European Union (EU), appointing a Data Protection Officer (DPO), the fair, legal, and open handling of personal data, being familiar with the “purpose limitation principle,” and having a privacy policy that complies with GDPR.



General Data Protection Regulation (GDPR) checker self-assessment

Use our tools to self-asses your dataset towards GDPR compliance.

1. Does your organization handle the personal information of any individuals residing in the EEA/EU? ✓

2. Do you know whether your organization requires the appointment of a Data Protection Officer (DPO)? ✓

3. Does your organization handle personal data fairly, legally, and openly? ✓

4. Is your organization familiar with the "purpose limitation principle"? ✓

5. Does your organization have a privacy policy that meets GDPR standards?

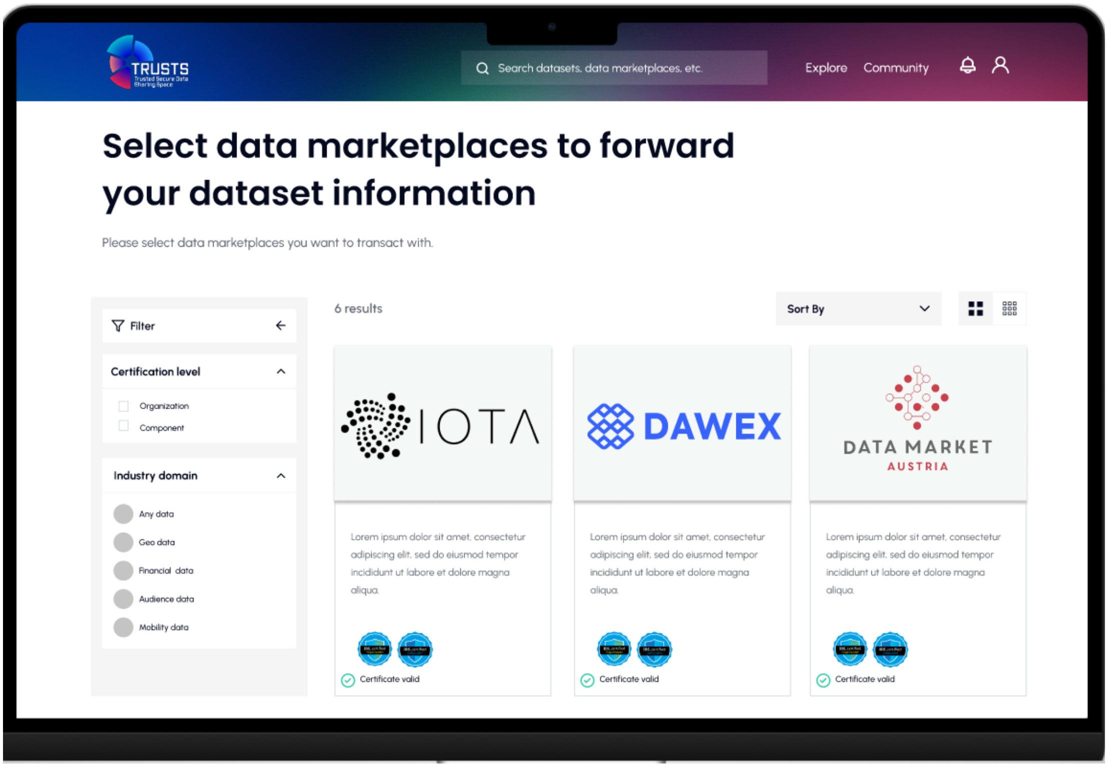
The establishment of a solid privacy policy for the protection of personal data will guarantee that risks in this area are identified in advance and that precautions are taken continuously.

Figure 3.13. I_2.3.1: Check GDPR compliance

3.2.4 Subtask 2.3: Selecting data marketplaces to share meta-data

Subtask 2.3 requires data providers to choose the data marketplaces to distribute their dataset's metadata. As shown in Figure 3.14, Interface *I_2.4.1* lists available 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_S_M$_1$ (Certification seals) and DP_C_M$_1$ (Certification validity audit).

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 domain.



TRUSTS

Search datasets, data marketplaces, etc.

Explore Community

Select data marketplaces to forward your dataset information

Please select data marketplaces you want to transact with.

Filter

Certification level

☐ Organization

☐ Component

Industry domain

● Any data

● Geo data

● Financial data

● Audience data

● Mobility data

6 results

Sort By

IOTA

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

✓ Certificate valid

DAWEX

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

✓ Certificate valid

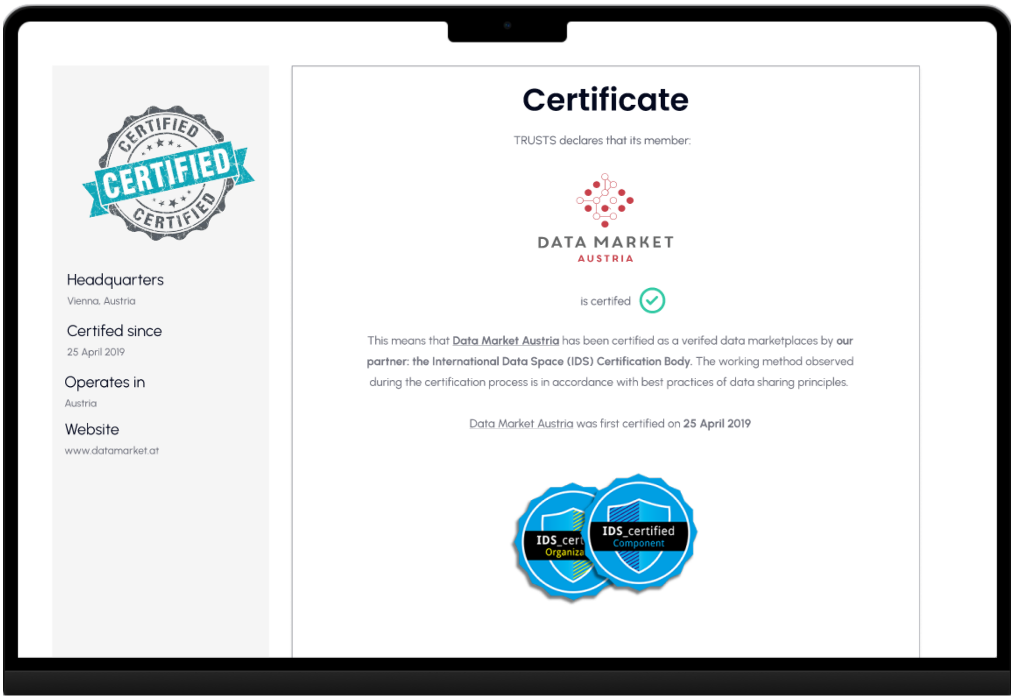
DATA MARKET AUSTRIA

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

✓ Certificate valid

Figure 3.14. I_2.4: Decide data marketplaces

Data providers can view the certification details of a specific data marketplace in *I_2.4.2* (Figure 3.17), 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$_2$ (Transparent 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 various entities 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 of 25 April 2019, 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:

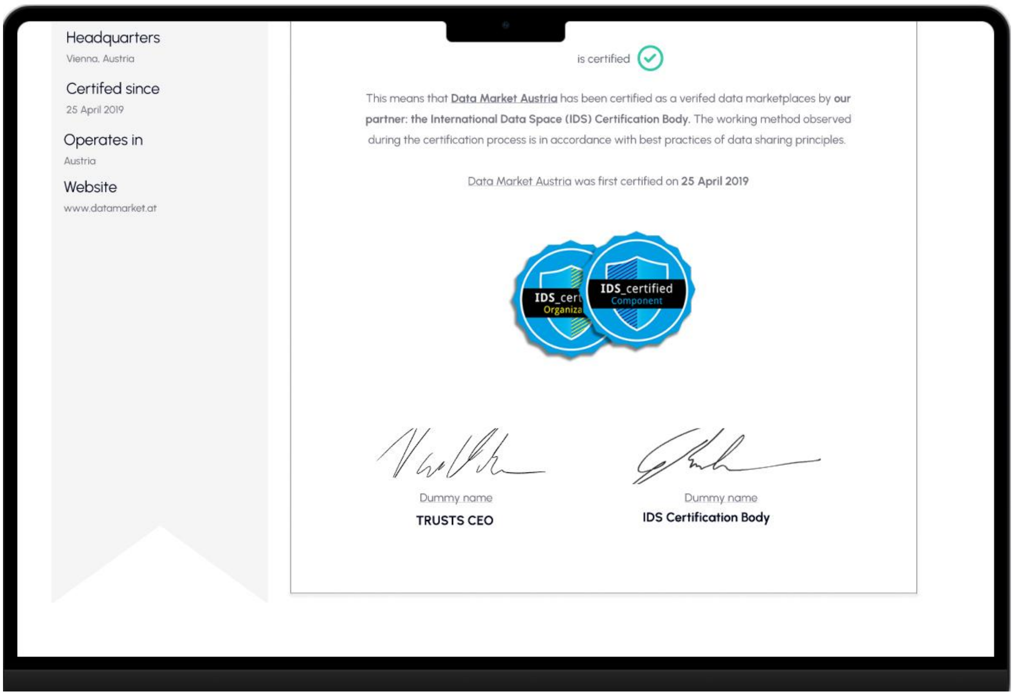
DATA MARKET
AUSTRIA

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 3.15. 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**

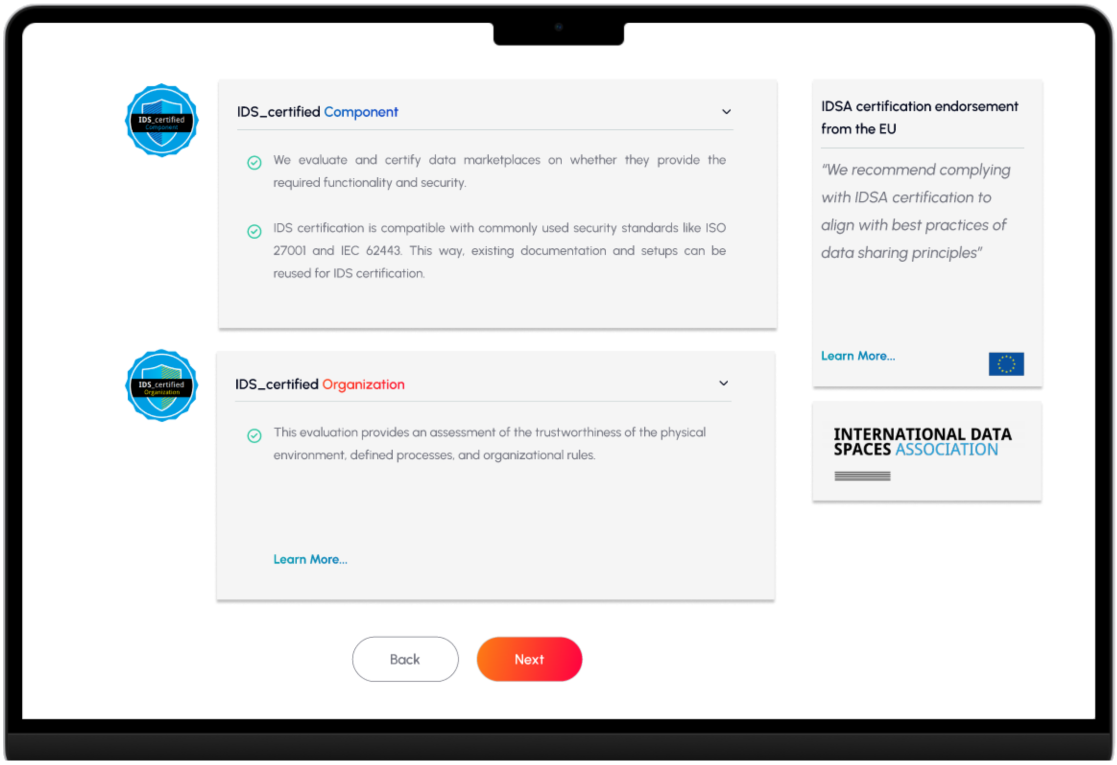
Dummy name
TRUSTS CEO

Dummy name
IDS Certification Body

Figure 3.16. I_2.4.2: View certificate status 2

Data providers continue to engage with *I_2.4.3* (Figure 3.17). 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$_2$, 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$_2$, 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$_3$, emphasizes the importance of complying with IDSA certification to align with data-sharing best practices. The IDSA logo, following design principle DP_C_M$_1$, 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.

Learn More...

IDSA certification endorsement from the EU

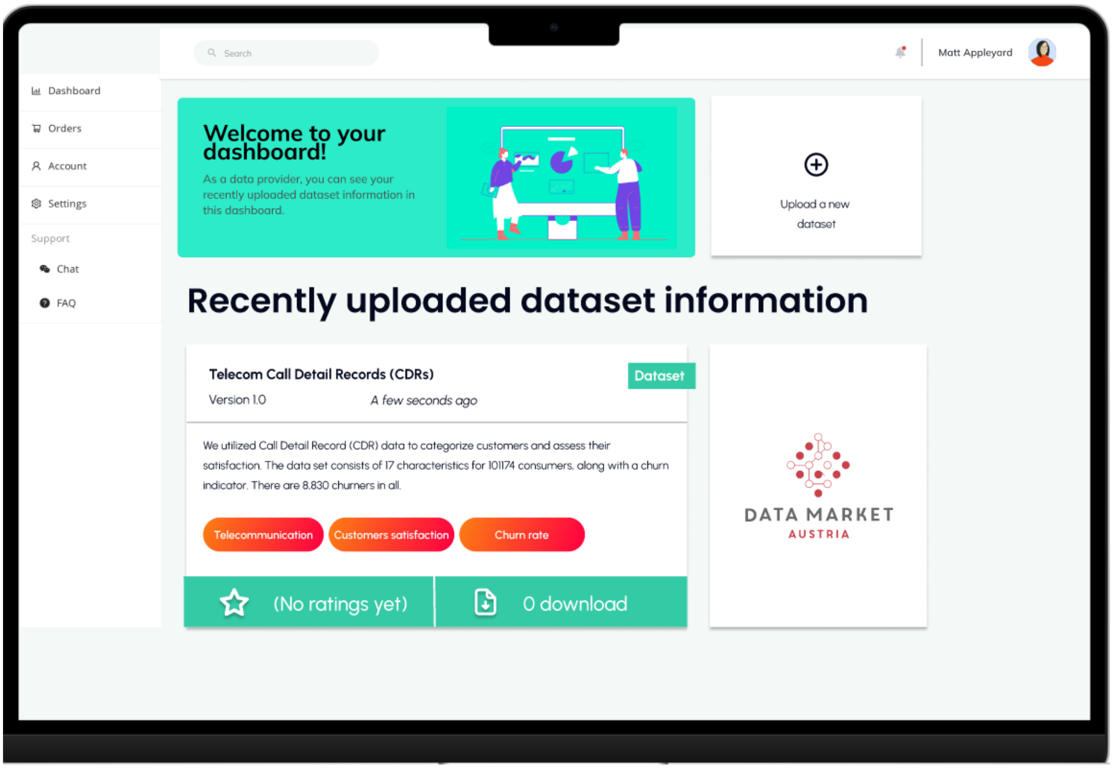
"We recommend complying with IDSA certification to align with best practices of data sharing principles"

Learn More...

IDS_certified Component
IDS_certified Organization
INTERNATIONAL DATA SPACES ASSOCIATION
Back
Next

Figure 3.17. I_2.4.3: View certificate information

In the final interface of this subtask, *I_2.4.5*, data providers can view the updated dashboard displaying the recently uploaded dataset information. The dashboard summarizes the dataset, including the title, version, upload timestamp, a brief description, relevant tags, and additional information such as ratings and download counts. The Data Market Austria logo is also displayed, indicating that the dataset has been successfully shared with this particular data marketplace.



Welcome to your dashboard!

As a data provider, you can see your recently uploaded dataset information in this dashboard.

Recently uploaded dataset information

Telecom Call Detail Records (CDRs)

Version 1.0 *A few seconds ago*

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.

Figure 3.18. I_2.4.5: View updated dashboard

3.3 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 3.3 summarizes the description of Task 3.

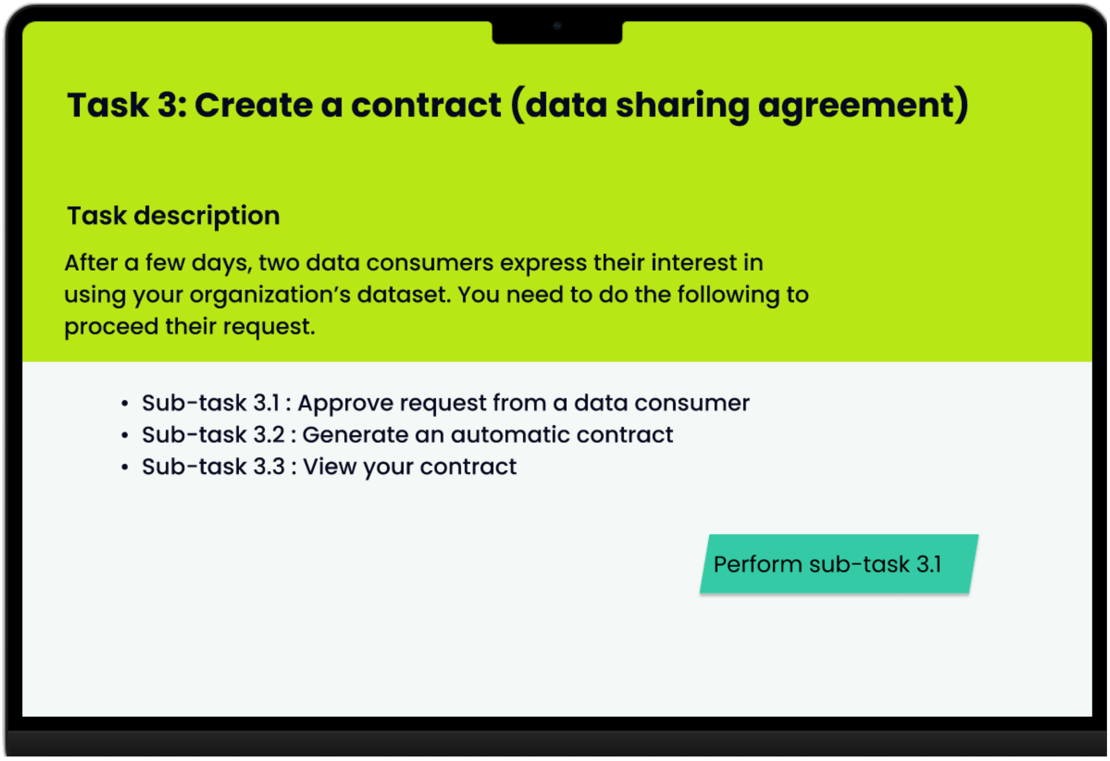
Table 3.3. Task 3 description

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
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	

ID	Interface	Description	
		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.	management and dispute resolution
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

3.3.1 Introducing Task 3

I_3.1.1 introduces Task 3, which involves creating a contract between the data provider and interested data consumers (Figure 3.19). The interface sets the scenario where two data consumers have expressed their interest in using the data provider's dataset. Data providers are guided through approving the requests, creating an automatic data-sharing agreement contract, and finally viewing the finished contract.



Task 3: Create a contract (data sharing agreement)

Task description

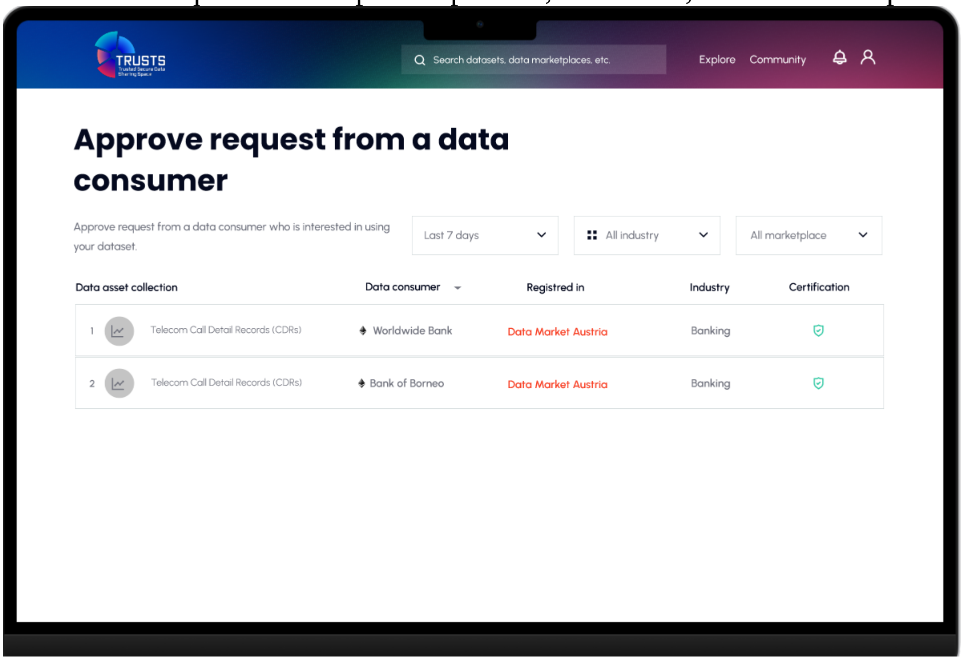
After a few days, two data consumers express their interest in using your organization's dataset. You need to do the following to proceed their request.

- Sub-task 3.1 : Approve request from a data consumer
- Sub-task 3.2 : Generate an automatic contract
- Sub-task 3.3 : View your contract

Figure 3.19. I_3 Task 3 introduction

3.3.2 Subtask 3.1: Approving a request from a data consumer

Interface *I_3.1.1* presents data providers with a table displaying requests from data consumers interested in using their dataset (refer to Figure 3.20). 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_M_1, 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

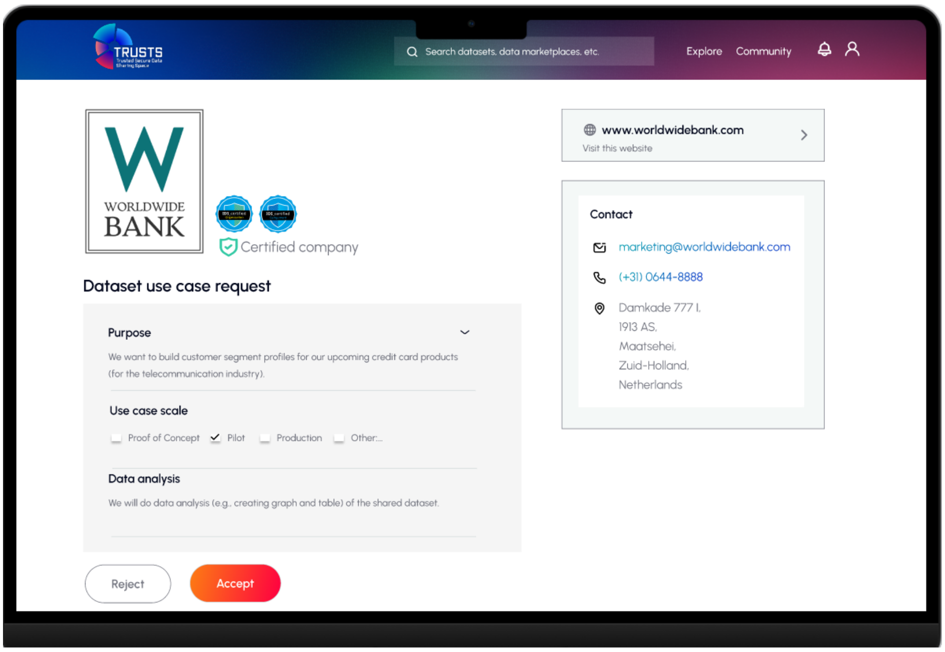
Approve request from a data consumer who is interested in using your dataset.

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 3.20. I_3.1.1 Select: a request

Data providers interact with Interface *I_3.1.2* after choosing a request. 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
IDS_certified
IDS_certified

✓ Certified company

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.

Reject | Accept

www.worldwidebank.com
Visit this website

Contact

marketing@worldwidebank.com

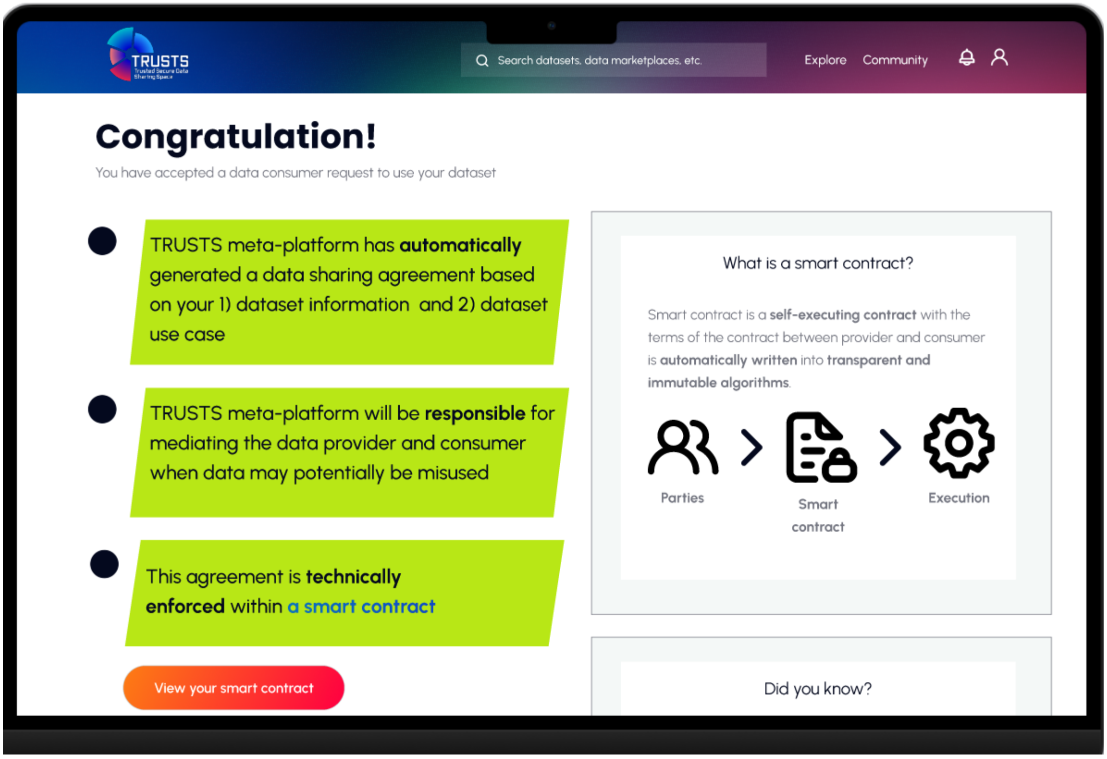
(+31) 0644-8888

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

Figure 3.21. I_3.1.2: Accept a request

3.3.3 Subtask 3.2: Generating an automatic contract

Data providers engage with the *I_3.2.1* interface to receive an explanation about smart contracts when they accept a request. 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_C_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.



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**

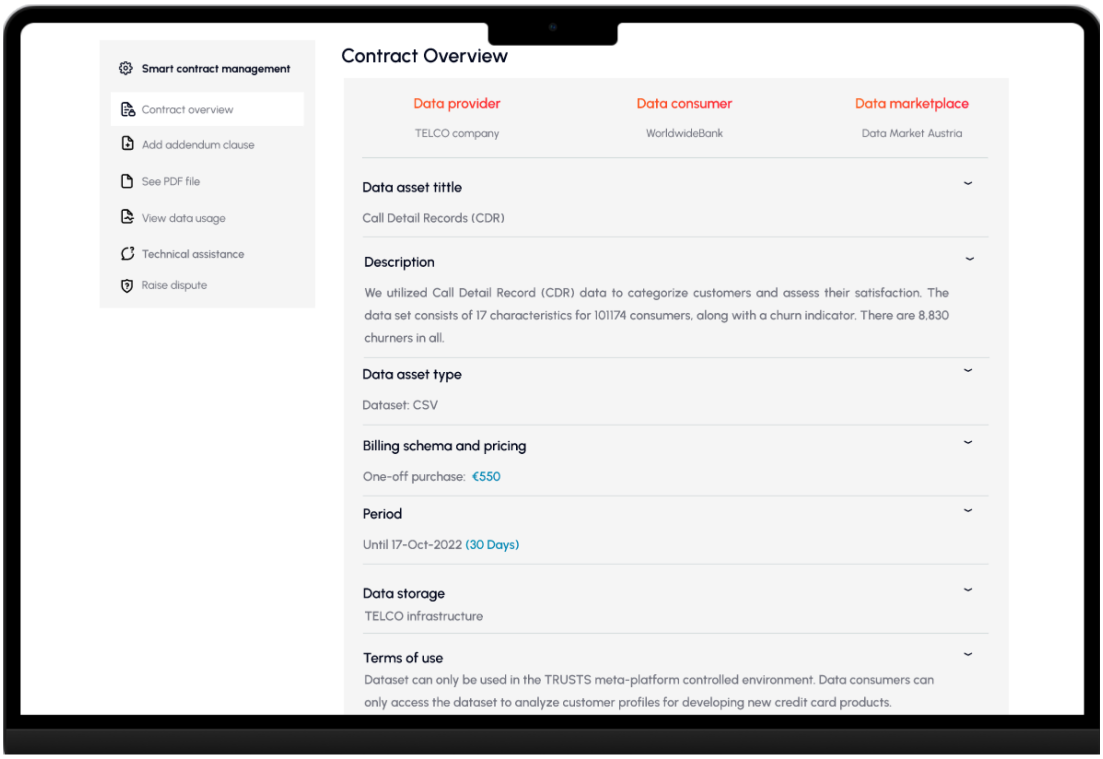
What is a smart contract?

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 3.22. I_3.2.1: View smart contract explanation

Data providers can view a contract summary between the TELCO company (data provider) and WorldwideBank (data consumer) registered in Data Market Austria on Interface *I_3.2.2* (refer to Figure 26). 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.



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

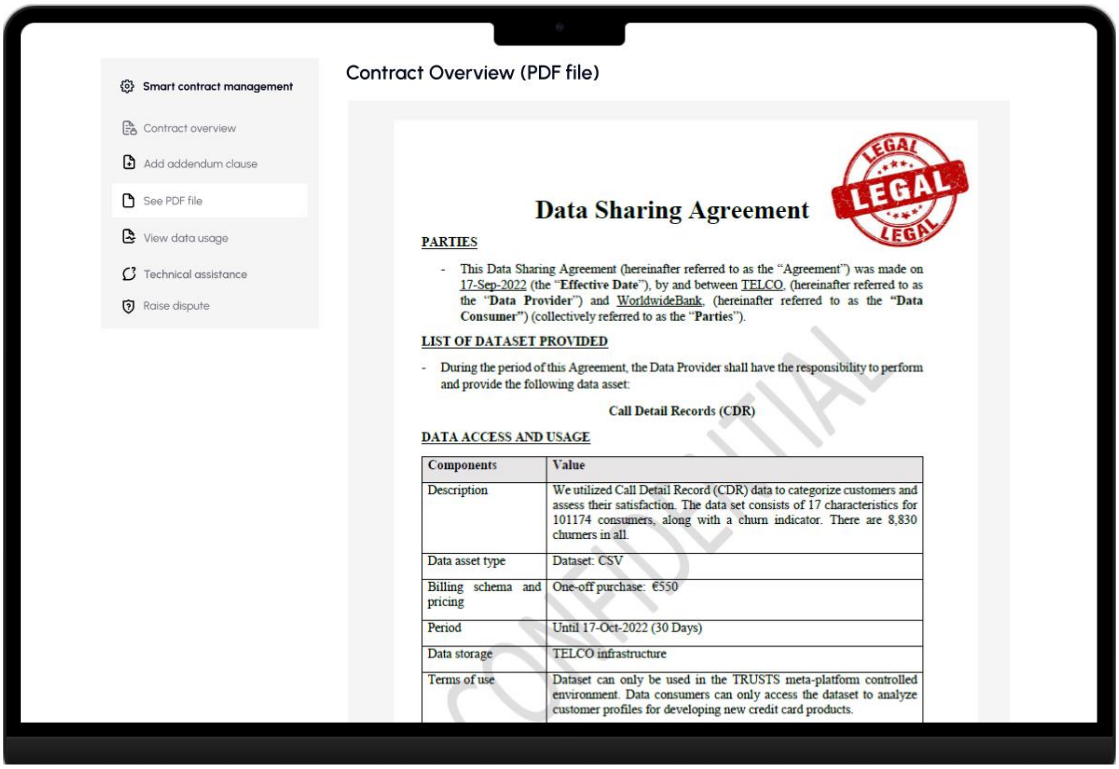
Terms of use

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 3.23. I_3.2.2: View contract

3.3.4 Subtask 3.3: Viewing your contract

Data providers can download and access the contract in PDF format by clicking the PDF file on Interface *I_3.2.2* (refer to Figure 3.24). This format facilitates data providers in reviewing, saving, and sharing the contract with relevant parties. It produces a clear and legally recognized document that delineates the terms and conditions of the data-sharing agreement between the data provider and the data consumer. The PDF format availability of the contract supports the DP_C_M3 (integrated legally-valid contract management and dispute resolution) by automatically generating a legally binding contract. This highlights the meta platform's ability to create a contract that complies with legal requirements and serves as a valid agreement for all parties involved.



Contract Overview (PDF file)

Data Sharing Agreement

PARTIES

- This Data Sharing Agreement (hereinafter referred to as the "Agreement") was made on 17-Sep-2022 (the "**Effective Date**"), by and between TELCO, (hereinafter referred to as the "**Data Provider**") and WorldwideBank, (hereinafter referred to as the "**Data Consumer**") (collectively referred to as the "**Parties**").

LIST OF DATASET PROVIDED

- During the period of this Agreement, the Data Provider shall have the responsibility to perform and provide the following data asset:

Call Detail Records (CDR)

DATA ACCESS AND USAGE

Components	Value
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 3.24. I_3.2.3: See contract PDF file

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

Task 4 aims to guide data providers through controlling how data consumers utilize their datasets. 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 3.4 provides an overview of the description of Task 4.

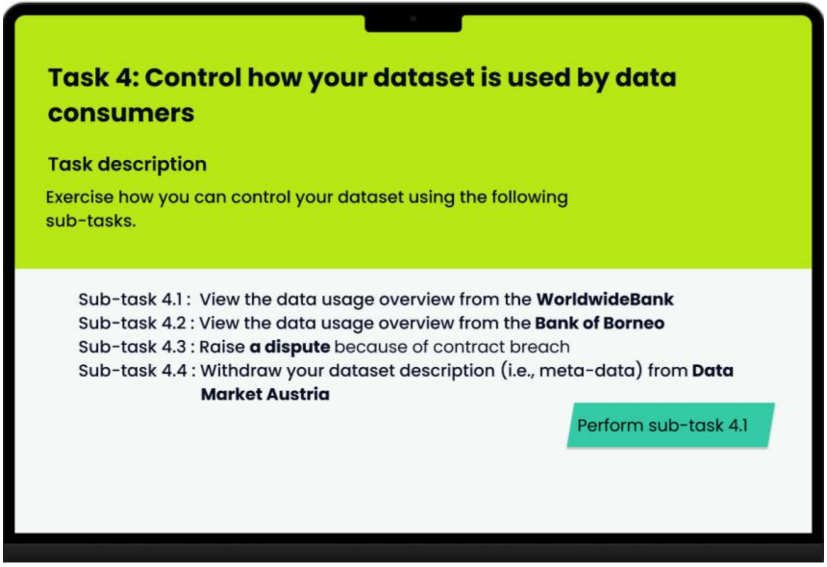
Table 3.4. Task 4 description

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			

ID	Interface	Description	
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
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_M_3: 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.	

3.4.1 Introducing Task 4

In the Task 4 introduction interface (Figure 3.25), data providers are presented with an overview of the actions they can take to control their dataset.



Task 4: Control how your dataset is used by data consumers

Task description

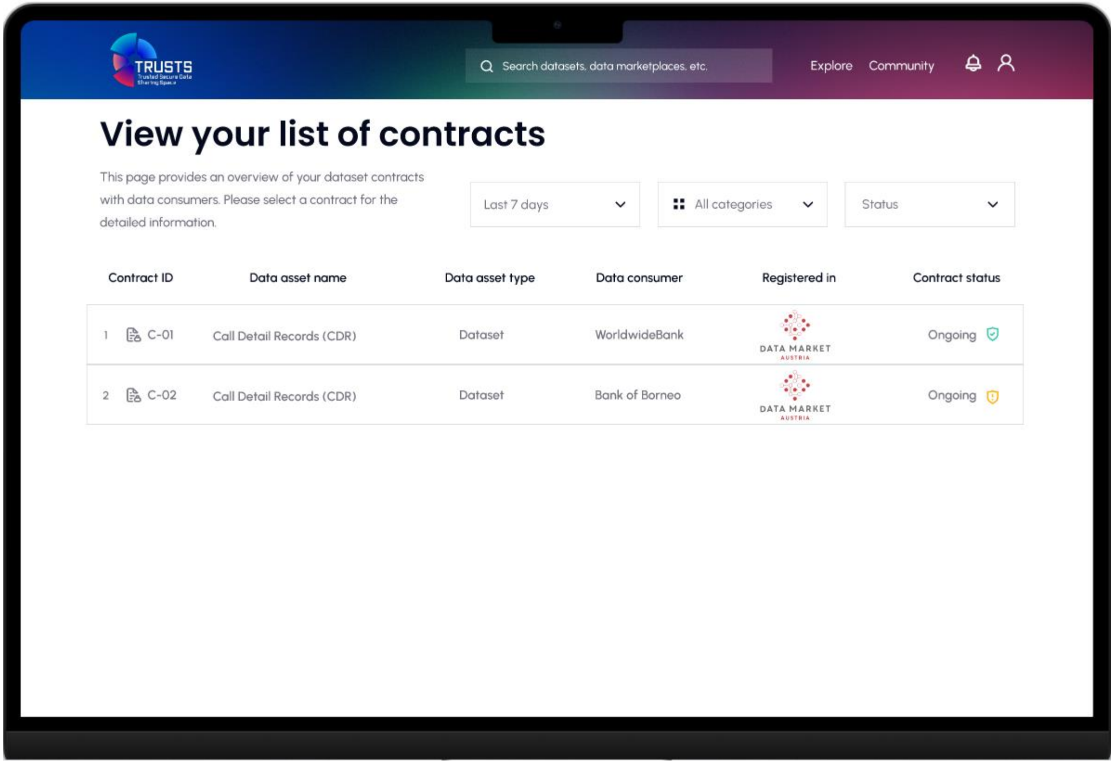
Exercise how you can control your dataset using the following sub-tasks.

Sub-task 4.1 : View the data usage overview from the **WorldwideBank**
Sub-task 4.2 : View the data usage overview from the **Bank of Borneo**
Sub-task 4.3 : Raise **a dispute** because of contract breach
Sub-task 4.4 : Withdraw your dataset description (i.e., meta-data) from **Data Market Austria**

Figure 3.25. I_4: Task 4 introduction

3.4.2 Subtask 4.1: Viewing the data usage overview from the WorldwideBank

Interface *I_4.1.1* displays a list of user contracts with data consumers (Figure 3.26). It also shows crucial information such as contract ID, data product name, data product type, data consumer, the marketplace the contract is registered in, and the contract status. The WorldwideBank contract displays a green status, indicating the absence of issues. On the other hand, the Bank of Borneo contract has a warning status.



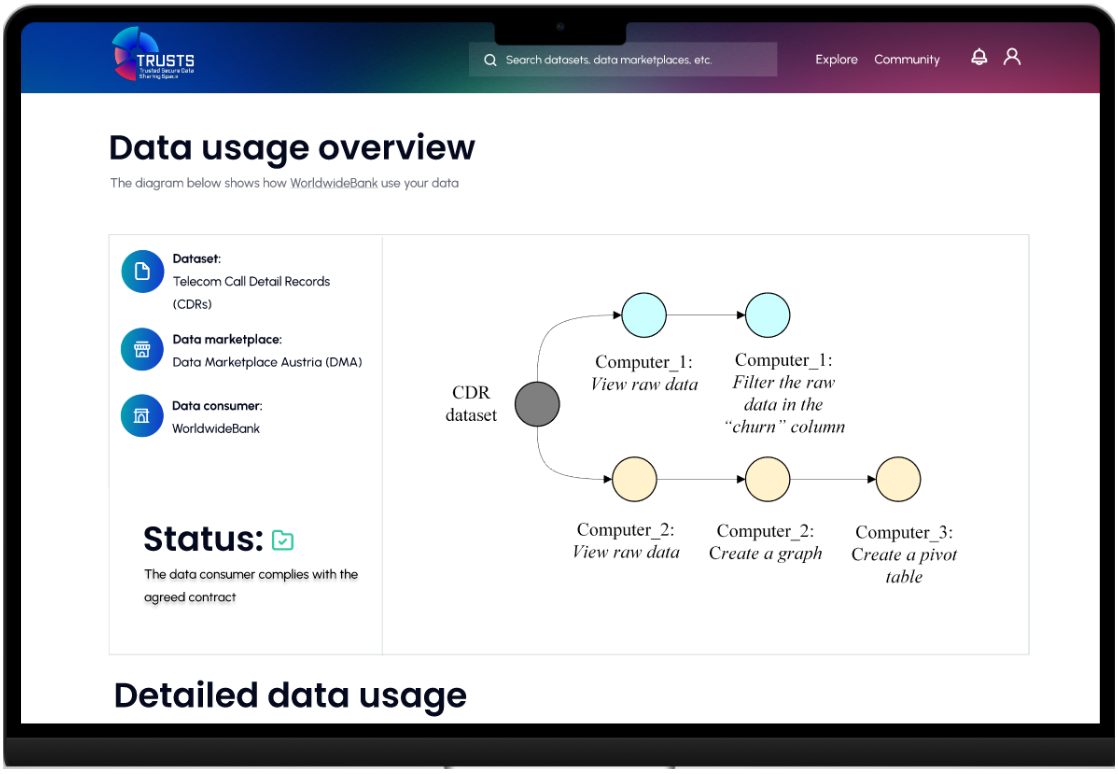
View your list of contracts

This page provides an overview of your dataset contracts with data consumers. Please select a contract for the detailed information.

	Contract ID	Data asset name	Data asset type	Data consumer	Registered in	Contract status
1	C-01	Call Detail Records (CDR)	Dataset	WorldwideBank	DATA MARKET AUSTRIA	Ongoing
2	C-02	Call Detail Records (CDR)	Dataset	Bank of Borneo	DATA MARKET AUSTRIA	Ongoing

Figure 3.26. I_4.1.1: Select contract 1

After clicking a contract ID in the previous interface, data providers are directed to interface *I_4.1.2*, which provides a detailed data usage overview for the WorldwideBank contract (Figure 3.27 and 3.28). The interface shows a provenance graph to display how data is utilized. *I_4.1.2* also presents supplementary details, including the dataset name, data marketplace, and data consumer. Furthermore, the interface shows an "OK" status, indicating that the data consumer complies with the agreed contract. The detailed data usage section provides a chronological list of data usage events with corresponding dates, times, and workspace information. *I_4.1.2* interface demonstrates the implementation of design principle DP_DC_M2 (Data traceability), as data providers can confirm that their data is being used appropriately.


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

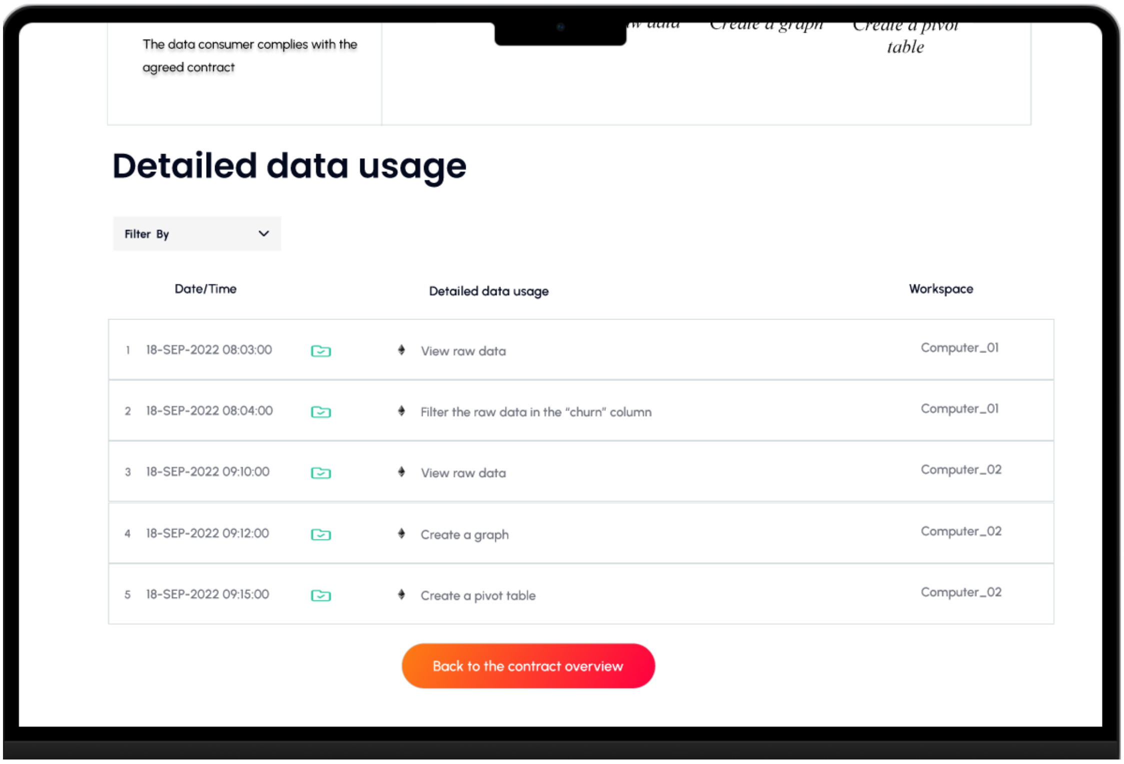
Status: ✓

The data consumer complies with the agreed contract

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 3.27. I_4.1.2: View data usage 1



The data consumer complies with the agreed contract

Detailed data usage

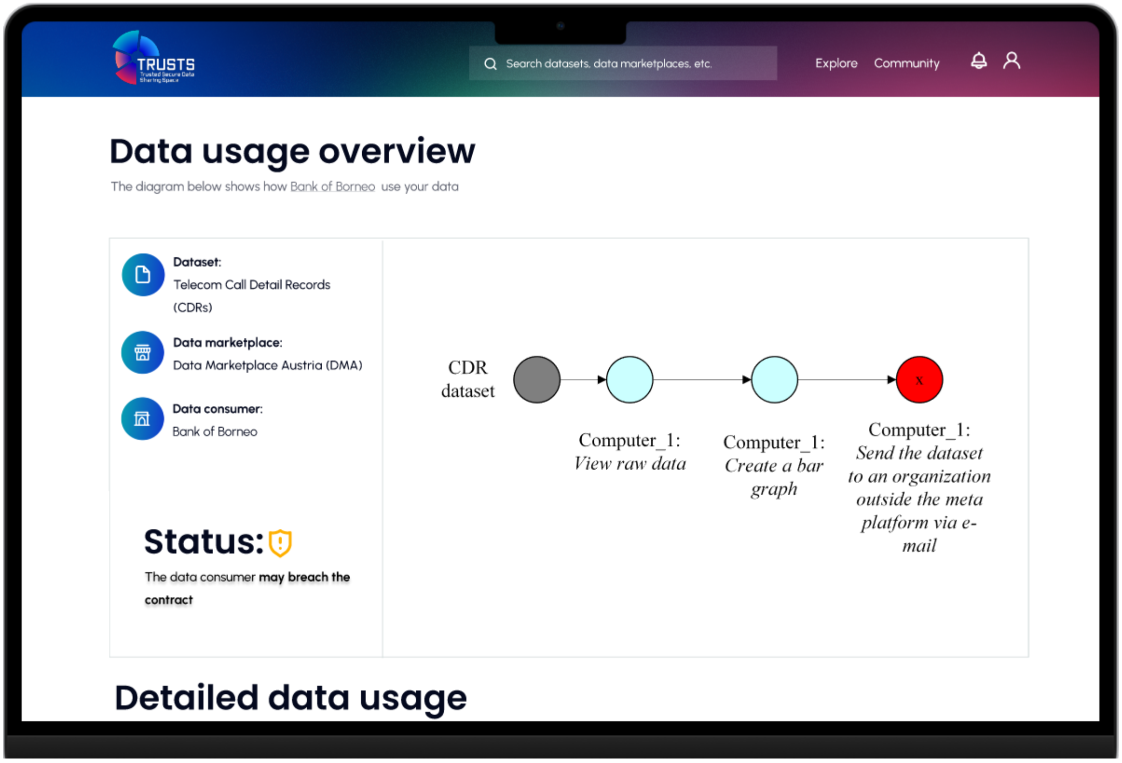
Filter By

	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	View raw data	Computer_02
4	18-SEP-2022 09:12:00	Create a graph	Computer_02
5	18-SEP-2022 09:15:00	Create a pivot table	Computer_02

Figure 3.28. I_4.1.2: View data usage 1 (2)

3.4.3 Subtask 4.2: Viewing the data usage overview from the Bank of Borneo.

Data providers return to the interface *I_4.1.1* to select a contract with the warning sign. After this, the user goes to *I_4.2.2* to check the details (Figure 3.29 and 3.30). *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.


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)

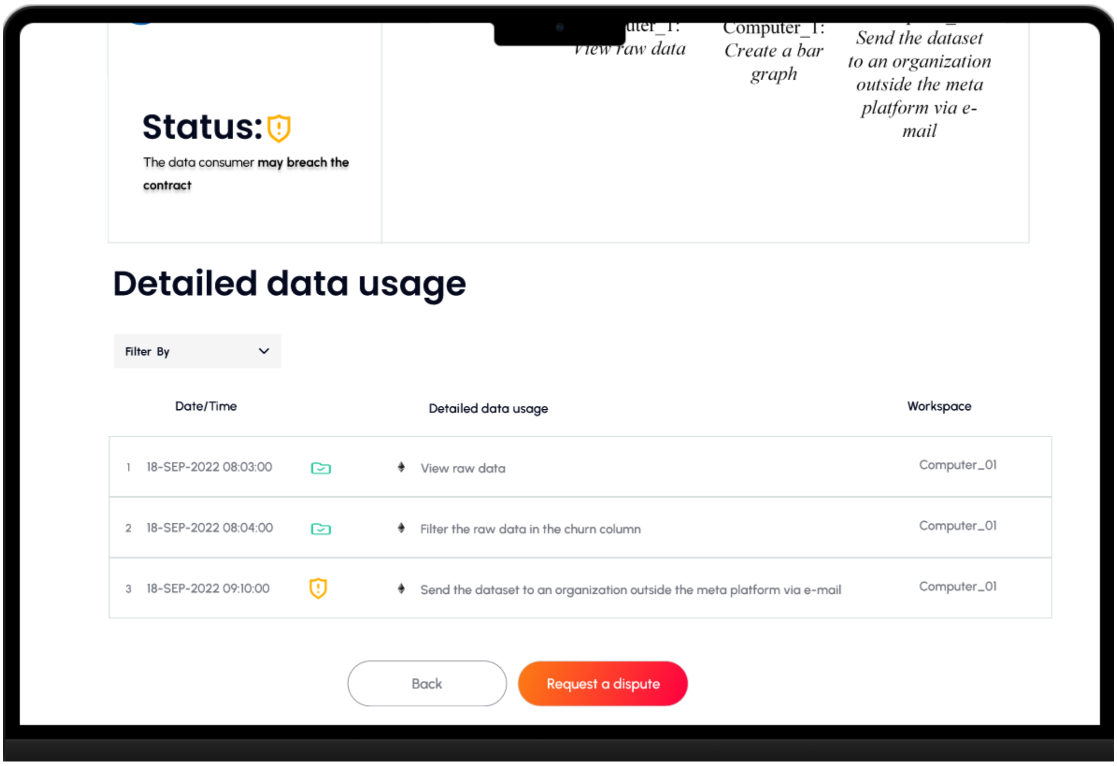
Data consumer: Bank of Borneo

Status: The data consumer **may breach the contract**

CDR dataset
x
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*

Detailed data usage

Figure 3.29. I_4.2.2: View data usage 2


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**

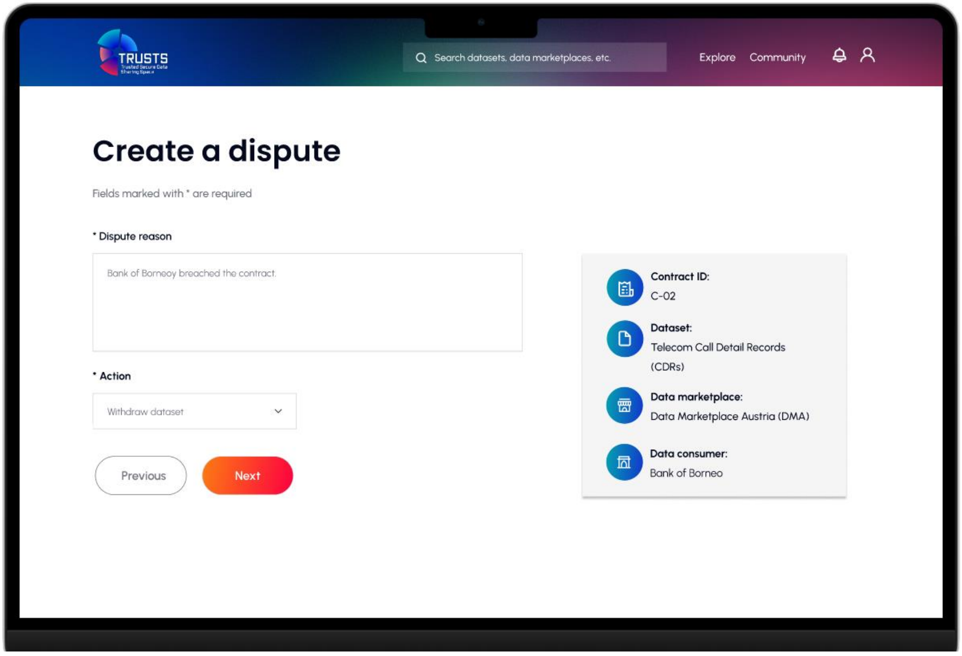
Detailed data usage

	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 3.30. I_4.2.2: View data usage 2

3.4.4 Subtask 4.3: Raising a dispute because of a contract breach

Data providers interact with *I_4.3.1* (Figure 3.31) and *I_4.3.2* (Figure 3.32) to complete Subtask 4.3. Data providers can initiate a dispute in case of a contract breach on Interface *I_4.3.1*. They must provide a detailed reason for the dispute and select an appropriate action to be taken. The right panel displays essential information about the contract, such as contract ID, dataset, data marketplace, and data consumer, which helps data providers ensure they raise a dispute for a correct contract.


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

Create a dispute

Fields marked with * are required

* Dispute reason

Bank of Borneoy breached the contract.

* Action

Withdraw dataset

Contract ID:
C-02

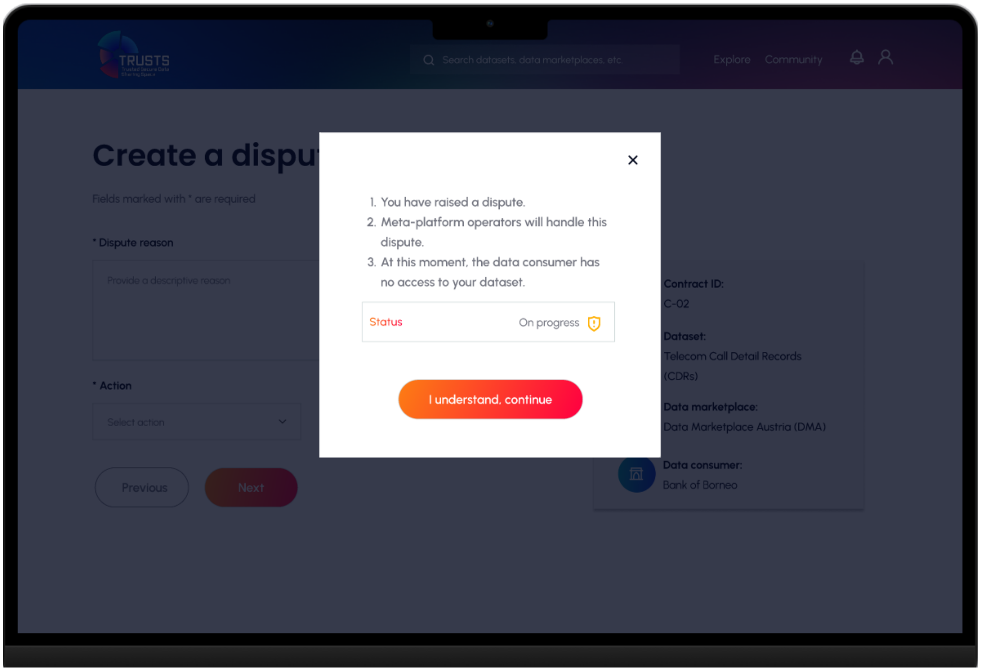
Dataset:
Telecom Call Detail Records (CDRs)

Data marketplace:
Data Marketplace Austria (DMA)

Data consumer:
Bank of Borneo

Figure 3.31. I_4.3.1: Raise a dispute

Interface *I_4.3.2* notifies data providers that the TRUSTS meta-platform operators will handle the dispute and that the dataset is inaccessible to the data consumer. Data providers can proceed by acknowledging the situation, and the status is displayed as "In progress."


TRUSTS
Trusted Secure Data Sharing Space
Search datasets, data marketplaces, etc.
Explore
Community
Create a dispu
Fields marked with * are required
* Dispute reason
Provide a descriptive reason
* Action
Select action
Previous
Next
×
I understand, continue

1. You have raised a dispute.
2. Meta-platform operators will handle this dispute.
3. At this moment, the data consumer has no access to your dataset.

Status On progress

Contract ID:
C-02

Dataset:
Telecom Call Detail Records (CDRs)

Data marketplace:
Data Marketplace Austria (DMA)

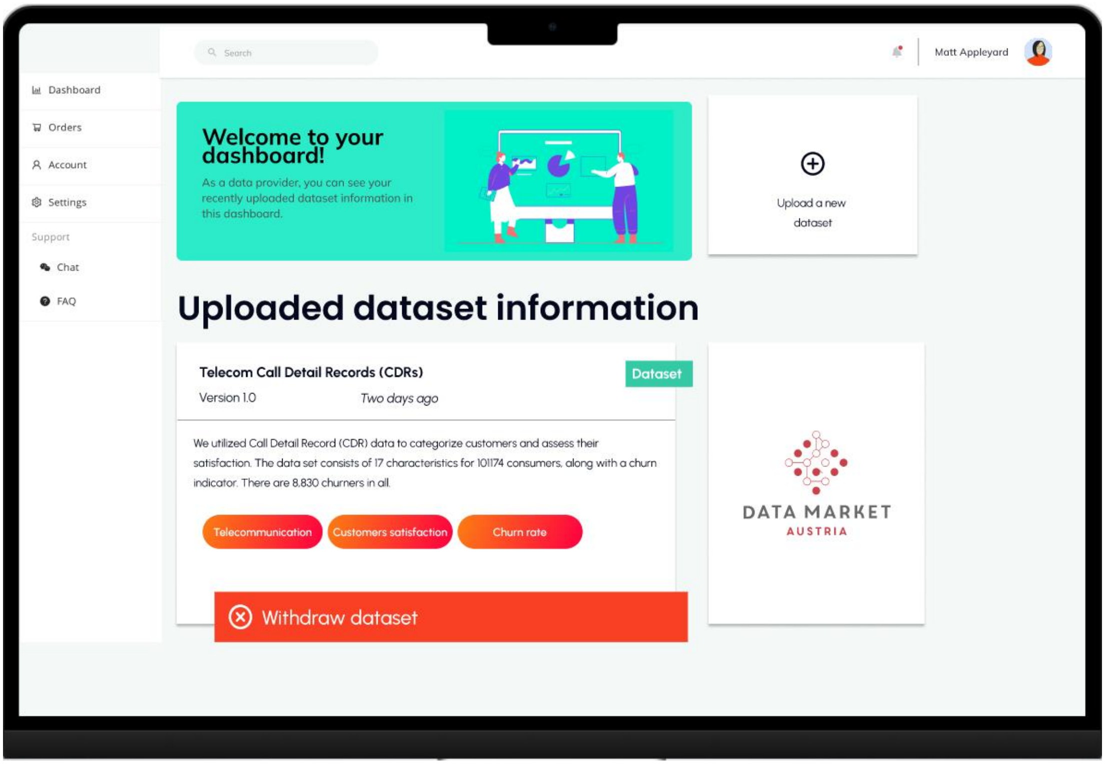
Data consumer:
Bank of Borneo

Figure 3.32. I_4.3.2: Confirming dispute submission

The above interfaces demonstrate the implementation of design principle DP_C_M3 (Integrated legally-valid contract management and dispute resolution), as it allows data providers to report potential breaches of contract and initiate actions to address the issue.

3.4.5 Subtask 4.4: Withdrawing dataset description (i.e., metadata) from Data Market Austria

Data providers withdraw their dataset's metadata from Data Market Austria by interacting with Interface *I_4.4.1* (Figure 3.33). Interface *I_4.4* displays the metadata that has been uploaded, which includes the title, version, and a brief description. This interface embeds the design principle DP_DC_M3, enabling data providers to manage and control their data products through dataset revocation.



Welcome to your dashboard!

As a data provider, you can see your recently uploaded dataset information in this dashboard.

Uploaded dataset information

Telecom Call Detail Records (CDRs) | Dataset

Version 1.0 | *Two days ago*

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.

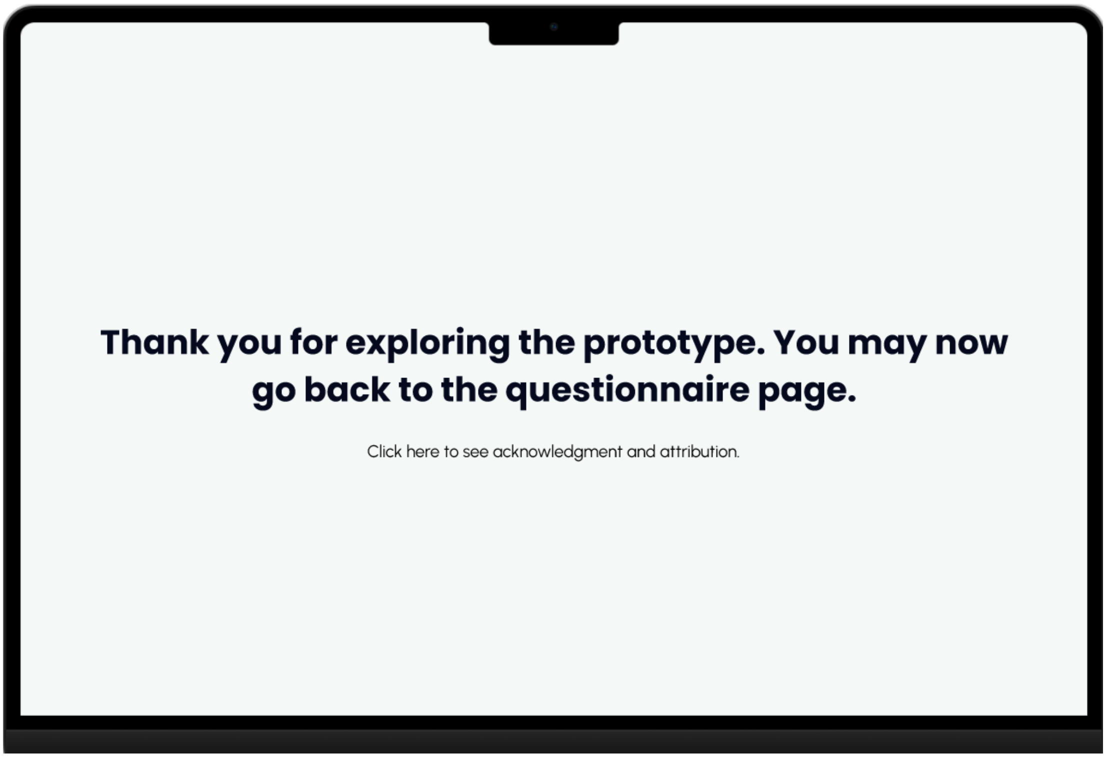
Telecommunication | Customers satisfaction | Churn rate

Withdraw dataset

Figure 3.33. I_4.4.1: Withdraw meta-data

3.4.6 Task epilogue

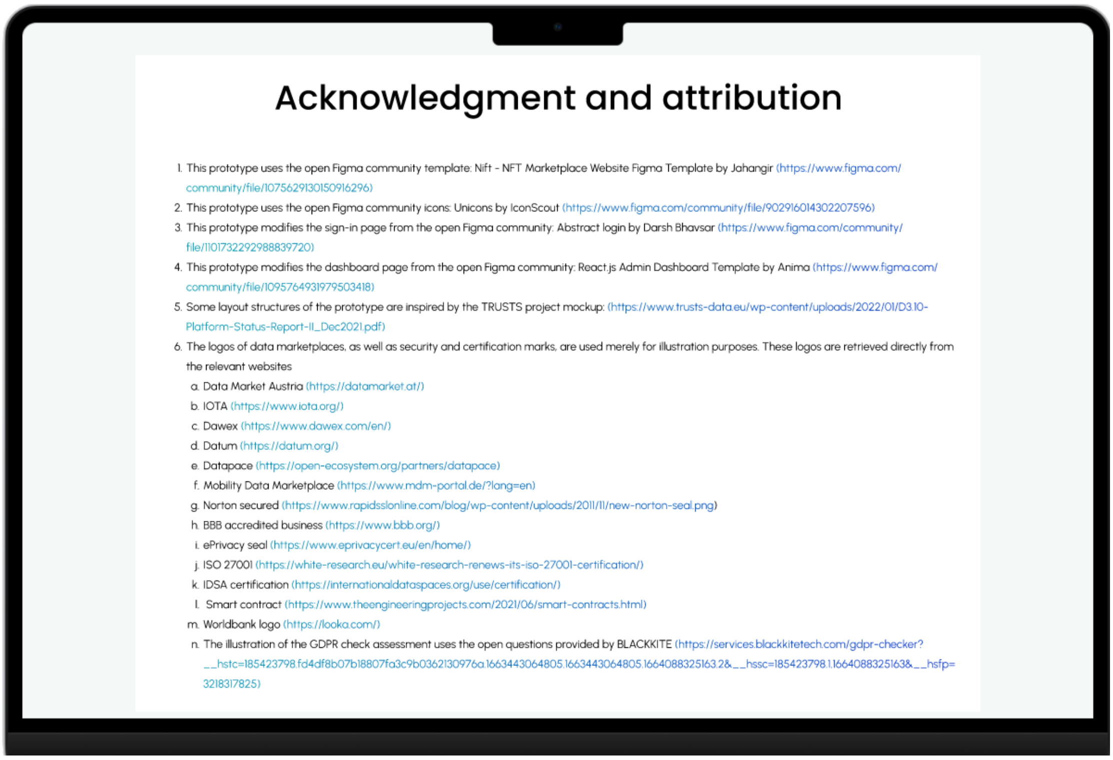
This subtask presents data providers with two interfaces: *I_TE.1* and *I_TE.2*. Figure 3.34 displays the *I_TE.1* interface, which expresses gratitude to data providers for exploring the prototype and offers a hyperlink to redirect them to the questionnaire page. The *I_TE.2* interface acknowledges and attributes the resources, templates, and inspirations used to create the prototype. These acknowledgments and attributions include Figma community templates, icons, logos, and layout structures inspired by various sources (Figure 3.35).



Thank you for exploring the prototype. You may now go back to the questionnaire page.

Click here to see acknowledgment and attribution.

Figure 3.34. I_TE.1: Thank you notes



Acknowledgment and attribution

1. This prototype uses the open Figma community template: Nift - NFT Marketplace Website Figma Template by Jahangir (https://www.figma.com/community/file/1075629130150916296)
2. This prototype uses the open Figma community icons: Unicons by IconScout (https://www.figma.com/community/file/902916014302207596)
3. This prototype modifies the sign-in page from the open Figma community: Abstract login by Darsh Bhavsar (https://www.figma.com/community/file/1101732292988839720)
4. This prototype modifies the dashboard page from the open Figma community: React.js Admin Dashboard Template by Anima (https://www.figma.com/community/file/1095764931979503418)
5. Some layout structures of the prototype are inspired by the TRUSTS project mockup: (https://www.trusts-data.eu/wp-content/uploads/2022/01/D3.10-Platform-Status-Report-II_Dec2021.pdf)
6. The logos of data marketplaces, as well as security and certification marks, are used merely for illustration purposes. These logos are retrieved directly from the relevant websites
   a. Data Market Austria (https://datamarket.at/)
   b. IOTA (https://www.iota.org/)
   c. Dawex (https://www.dawex.com/en/)
   d. Datum (https://datum.org/)
   e. Datapace (https://open-ecosystem.org/partners/datapace)
   f. Mobility Data Marketplace (https://www.mdm-portal.de/?lang=en)
   g. Norton secured (https://www.rapidsslonline.com/blog/wp-content/uploads/2011/11/new-norton-seal.png)
   h. BBB accredited business (https://www.bbb.org/)
   i. ePrivacy seal (https://www.eprivacycert.eu/en/home/)
   j. ISO 27001 (https://white-research.eu/white-research-renews-its-iso-27001-certification/)
   k. IDSA certification (https://internationaldataspaces.org/use/certification/)
   l. Smart contract (https://www.theengineeringprojects.com/2021/06/smart-contracts.html)
   m. Worldbank logo (https://looka.com/)
   n. The illustration of the GDPR check assessment uses the open questions provided by BLACKKITE (https://services.blackkitetech.com/gdpr-checker?__hstc=185423798.fd4df8b07b18807fa3c9b0362130976a.1663443064805.1663443064805.1664088325163.2&__hssc=185423798.1.1664088325163&__hsfp=3218317825)

Figure 3.35. I_TE.2: Acknowledgment and attribution

Online Appendix 4. Developing a data sovereignty measurement model

Online Appendix 4 presents relevant details of the process of developing a data sovereignty measurement model in Chapter 8. In addition, we also aimed to get an initial indication of data sovereignty impacts. We analyze the nomological network of data sovereignty, a framework that represents the relationships between various constructs in a theoretical model. This analysis pre-assessed the importance of data sovereignty as a key factor influencing the data economy antecedents (i.e., trust, perceived risk, and willingness to share business data).

4.1 The initial measurement model of data sovereignty

Table 4.1. The initial measurement model of data sovereignty

Construct	Code	Indicator
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.
	DO_2	-…define how much money I receive for the sensitive data that I would share.
	DO_3	-…decide about the type of sensitive data that I would share.
	DO_4	-…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 usage policies.
	DC_2	-…enables me to track down the history of data usage.
	DC_3	-…enables me to 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).
	DC_4	-…enables me to easily withdraw the description of sensitive data from the meta-platform after sharing it.
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.
	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.
Responsibility	R_1	I believe the meta-platform… -…responsibly selects data marketplace participants that adhere to data exchange standards.
	R_2	-…clearly divides responsibilities between the meta-platform and the data marketplace participants.
	R_3	-…takes responsibility if the sensitive data that I would share is misused or stolen.
Security	S_1	I believe the meta-platform… -… prevents the disclosure of my sensitive data that I would share to unauthorized parties.
	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.
	S_4	-…implements up-to-date security features.
Data Sovereignty	DS_DO	I believe the meta-platform... -…enables me to be the owner of the sensitive data that I would share

	DS_DC	-…enables me to control the sensitive data that I would share.
	DS_C	-…enables me to 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.
Trust in Operator	TO_1	I expect that the meta-platform operator provides services to facilitate sharing sensitive data in my best interest.
	TO_2	I expect that the meta-platform operator provides access to genuine services for sharing sensitive data.
	TO_3	I expect that the meta-platform operator will be trustworthy in handling the description of sensitive data provided by me.
Trust in Data Consumer	TDC_1	I expect that data consumers will fulfill data sharing agreements to use the sensitive data that they obtain through the meta-platform.
	TDC_2	I expect that data consumers will be honest when handling the sensitive data that they obtain through the meta-platform.
	TDC_3	I expect that data consumers will be trustworthy in handling the sensitive data that they obtain through the meta-platform.
Perceived Risk	PR_1*	I feel that sharing sensitive data through the meta-platform is risky.
	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_1	I intend to share sensitive data through this meta-platform
	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

The raw datasets are available online at https://doi.org/10.4121/e4cacfac-31f0-4523-81f4-35383ba958a8.

4.2 G*Power sample calculation

Based on G*Power analysis, with a minimum power of 0.8, a medium effect size, a significance threshold of 0.05, and no more than five arrows pointing to any variable, the requisite minimum sample size is 92.

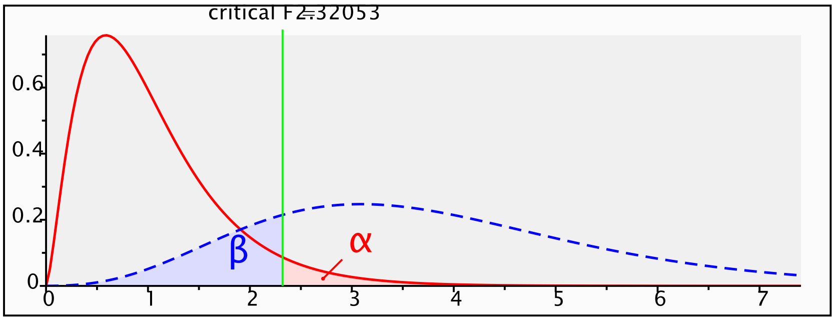


Figure 4.1. G*Power sample calculation (1)

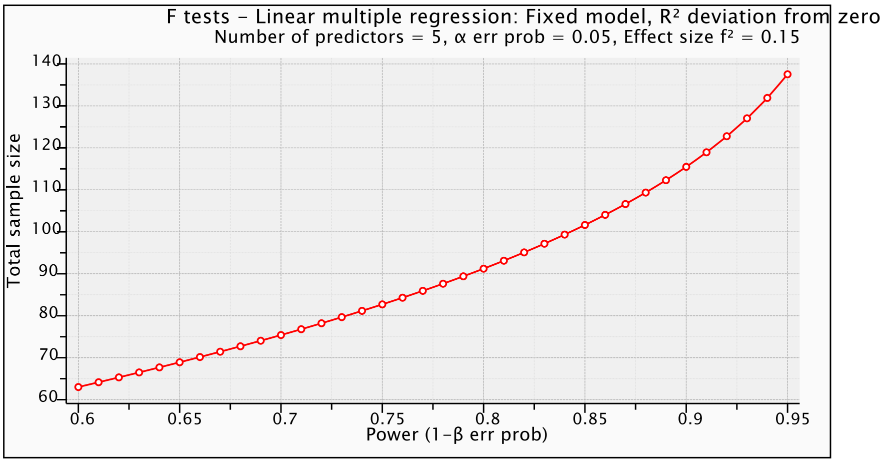


Figure 4.2. G*Power sample calculation (2)

4.3 Validity and reliability analysis

Table 4.2. Validity and reliability analysis

Dimension	Indicators	Convergent validity		Internal consistency reliability			Discriminant validity
		Loadings	AVE	Cronbach's Alpha	Reliability ρ_A	Composite reliability ρ_c	HTMT
		>0.7	>0.5	0.6-0.9	0.6-0.9	0.6-0.9	Lower than 0.9?
Data Ownership	DO_1	0.723	0.544	0.726	0.738	0.826	Yes
	DO_2	0.685					
	DO_3	0.818					
	DO_4	0.717					
Data Control	DC_1	0.719	0.598	0.774	0.783	0.855	Yes
	DC_2	0.863					
	DC_3	0.691					
	DC_4	0.808					
Compliance	C_1	0.876	0.712	0.865	0.868	0.908	Yes
	C_2	0.809					
	C_3	0.871					
	C_4	0.816					
Responsibility	R_1	0.883	0.62	0.692	0.734	0.829	Yes
	R_2	0.772					
	R_3	0.696					
Security	S_1	0.841	0.628	0.696	0.722	0.833	Yes
	S_2	0.864					
	S_3	0.655					
Trust in Operator	TO_1	0.861	0.769	0.85	0.857	0.909	Yes
	TO_2	0.899					
	TO_3	0.87					
Trust in Data Consumer	TDC_1	0.902	0.88	0.932	0.932	0.957	Yes
	TDC_2	0.952					
	TDC_3	0.96					
Perceived Risk	PR_1*	0.879	0.744	0.828	0.835	0.897	Yes
	PR_2*	0.829					
	PR_3*	0.879					

Dimension	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	0.6-0.9	0.6-0.9	0.6-0.9	Lower than 0.9?
Willingness to Share Data	WTSD_1	0.917	0.868	0.924	0.926	0.952	Yes
	WTSD_2	0.941					
	WTSD_3	0.937					

Table 4.3. HTM Matrix

	Compliance	Data Control	Data Ownership	Perceived Risk	Responsibility	Security	Trust in Data Consumer	Trust in Operator
Compliance								
Data Control	0.598							
Data Ownership	0.486	0.759						
Perceived Risk	0.541	0.286	0.388					
Responsibility	0.689	0.611	0.577	0.604				
Security	0.53	0.632	0.476	0.555	0.882			
Trust in Data Consumer	0.303	0.392	0.396	0.479	0.599	0.523		
Trust in Operator	0.458	0.575	0.581	0.492	0.741	0.635	0.808	
Willingness to Share Data	0.278	0.187	0.155	0.482	0.547	0.458	0.27	0.276

Table 4.4. Fornell-Larcker criterion

	Compliance	Data Control	Data Ownership	Perceived Risk	Responsibility	Security	Trust in Data Consumer	Trust in Operator	Willingness to Share Data
Compliance	0.844								
Data Control	0.499	0.773							
Data Ownership	0.417	0.567	0.738						
Perceived Risk	0.46	0.239	0.316	0.862					
Responsibility	0.561	0.46	0.454	0.457	0.787				
Security	0.42	0.476	0.363	0.427	0.618	0.792			

	Compliance	Data Control	Data Ownership	Perceived Risk	Responsibility	Security	Trust in Data Consumer	Trust in Operator	Willingness to Share Data
Trust in Data Consumer	0.269	0.339	0.357	0.419	0.476	0.41	0.938		
Trust in Operator	0.401	0.471	0.48	0.419	0.572	0.488	0.716	0.877	
Willingness to Share Data	0.25	0.162	0.106	0.423	0.435	0.378	0.251	0.246	0.932

The VIF score for data sovereignty dimensions

Dimension	VIF
LV scores - Compliance	1.648
LV scores - Data Control	1.816
LV scores - Data Ownership	1.597
LV scores - Responsibility	2.059
LV scores - Security	1.752

4.4 Initial structural model

We proceeded with the analysis of the nomological net. The nomological net shows no collinearity issues, as all constructs have a VIF larger than 5 (see Table 4.5)

Table 4.5 VIF value for construct

	Data Sovereignty	Perceived Risk	Trust in Data Consumer	Trust in Operator	Willingness to Share Data
Data Sovereignty		1	1	1	1.918
Perceived Risk					1.434
Trust in Data Consumer					2.127
Trust in Operator					2.55
Willingness to Share Data					
Willingness to Share Data					

We then assess the significance and relevance of the relationships within the structural model. The results reveal that data sovereignty positively affects the trust data providers have in the operator of the meta-platform (TO $\beta = 0.631$, $p = < 0.001$) and data consumers using the platform (TDC $\beta = 0.509$, $p < 0.001$). In contrast, data sovereignty reduces the perceived risk associated with data exchange (PR $\beta = 0.593$, $p < 0.001$). Data sovereignty exhibits *complementary mediation*, meaning it influences the outcome variable through both direct and indirect pathways. In this case, data sovereignty has a significant direct effect on the Willingness to Share Data (WTSD $\beta = 0.280$, $p < 0.05$) and an indirect effect via Perceived Risk (indirect effects $\beta = 0.146$, $p < 0.05$).

We also assessed the explanatory power of the model. The R^2 values are 0.294 for Perceived Risk, 0.264 for Trust in Data Consumer, 0.408 for Trust in Operator, and 0.240 for Willingness to Share Data. The R^2 score indicates the proportion of variance in the dependent variables explained by the model's independent variables. According to Hair et al. (2021), R^2 values can be classified as weak (0.25 or less), moderate (between 0.25 and 0.5), or substantial (greater than 0.5). In this study, the R^2 values for Perceived Risk, Trust in Data Consumer, and Trust in Operator fall within the moderate range, while Willingness to Share Data Exhibits weak explanatory power. Nevertheless, it is essential to acknowledge that the primary objective of the nomological network is not to create a comprehensive model of willingness to share data but rather to determine whether data sovereignty contributes to Willingness to Share Data. Indeed, the results confirm that data sovereignty significantly contributes to Willingness to Share Data, highlighting the importance of data sovereignty in influencing business data exchange antecedents. While additional factors may explain the variance in the dependent variables, the current model successfully captures the critical role of data sovereignty in data exchange antecedents.

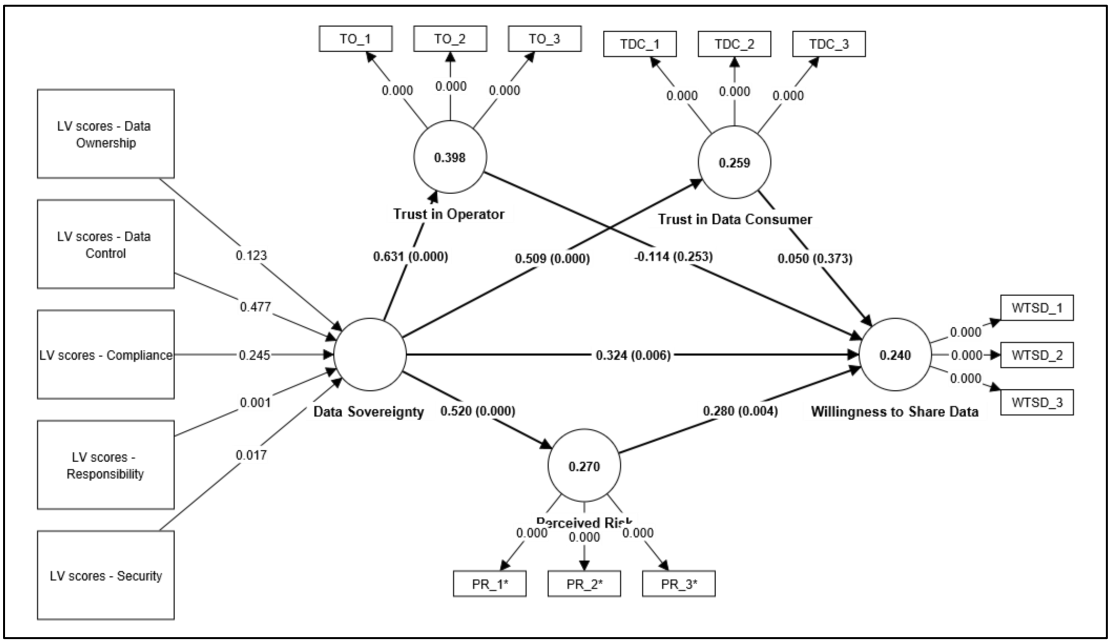


Figure 4.3. The nomological net of data sovereignty

We also examined the f^2 value of data sovereignty for all dependent variables (Table 4.6): Perceived Risk = 0.370, Trust in Data Consumer = 0.350, Trust in Operator = 0.662, and Willingness to Share Data = 0.072. These f^2 values represent the effect sizes of data sovereignty on each dependent variable. Cohen (2013) categorizes effect sizes as small (0.02), medium (0.15), or large (0.35). In this study, the influence of data sovereignty on Perceived Risk can be considered medium, while its impact on Trust in Data Consumer and Operator are large. Though relatively small, the effect of data sovereignty on Willingness to Share Data remains significant, highlighting its contribution to the overall understanding of data exchange antecedents. Despite its modest impact, Data Sovereignty serves as a valuable piece of the puzzle, helping to uncover the complex interplay of factors that drive data providers' willingness to share data.

Table 4.6 f^2 Matrix

	Data Sovereignty	**Perceived Risk**	**Trust in Data Consumer**	**Trust in Operator**	**Willingness to Share Data**
Data Sovereignty		0.37	0.35	0.662	0.072
Perceived Risk					0.072
Trust in Data Consumer					0.002
Trust in Operator					0.007
Willingness to Share Data					

Finally, we evaluated the model's predictive power. The Q^2 values for the indicators of the target construct, Willingness to Share Data, are greater than 0. This result suggests that the model possesses predictive relevance for the target construct, Willingness to

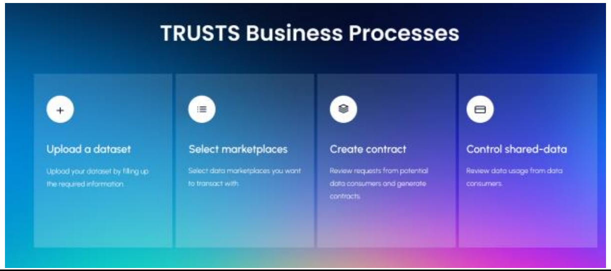
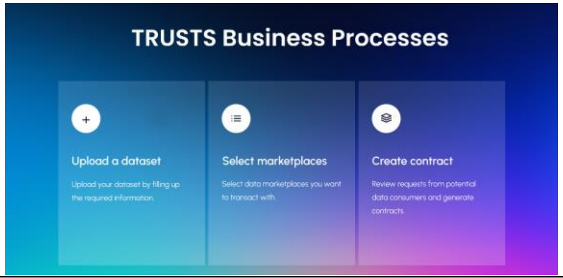
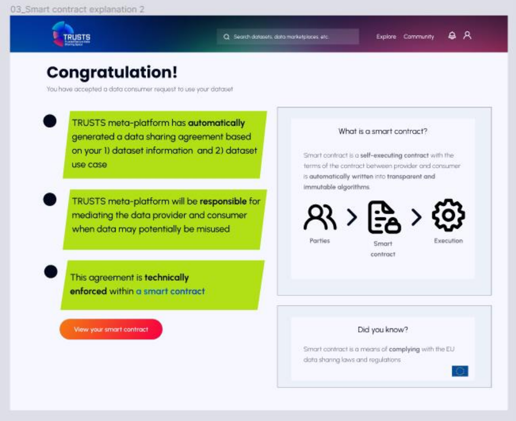
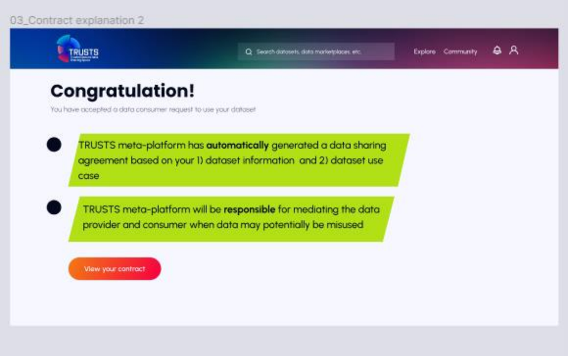
Share Data. A positive Q² value indicates that the model’s predictions for the indicators of Willingness to Share Data are accurate, implying that the model can effectively forecast the dependent variable outcomes based on the established relationships in the dataset.

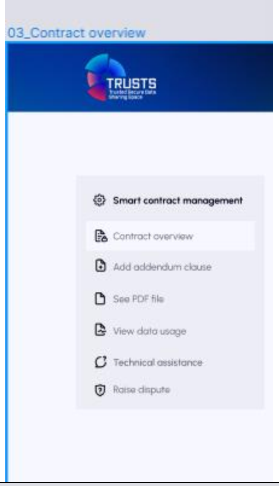
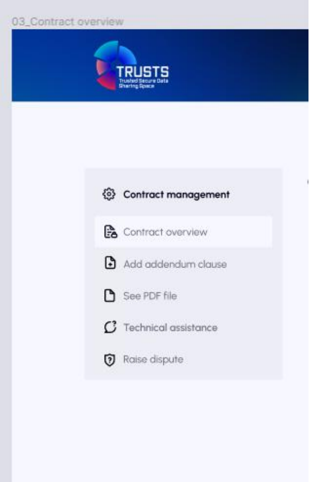
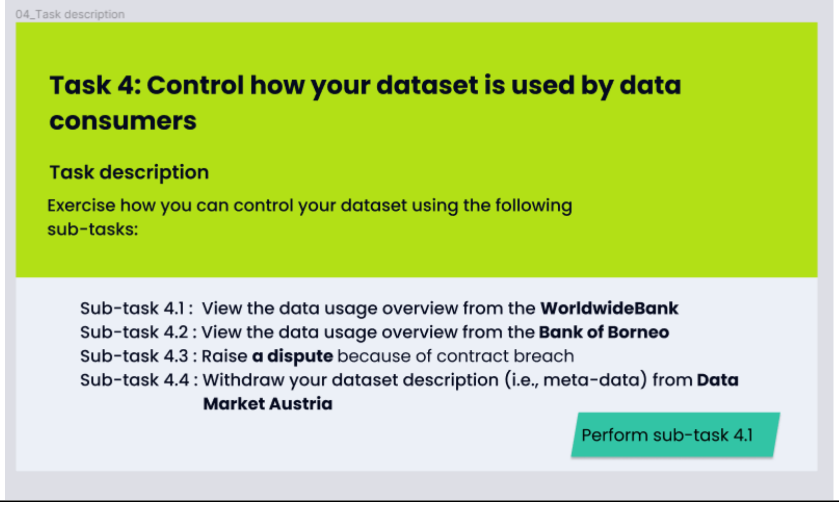
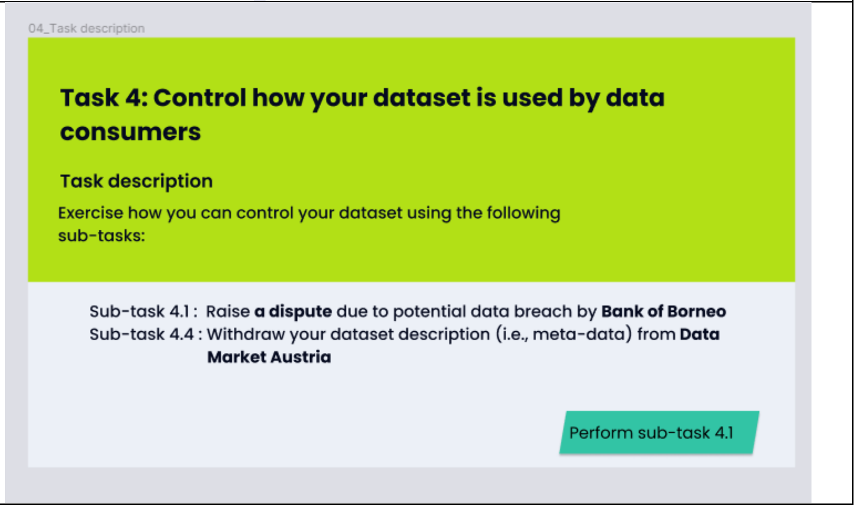
Online Appendix 5. Conducting a controlled experiment

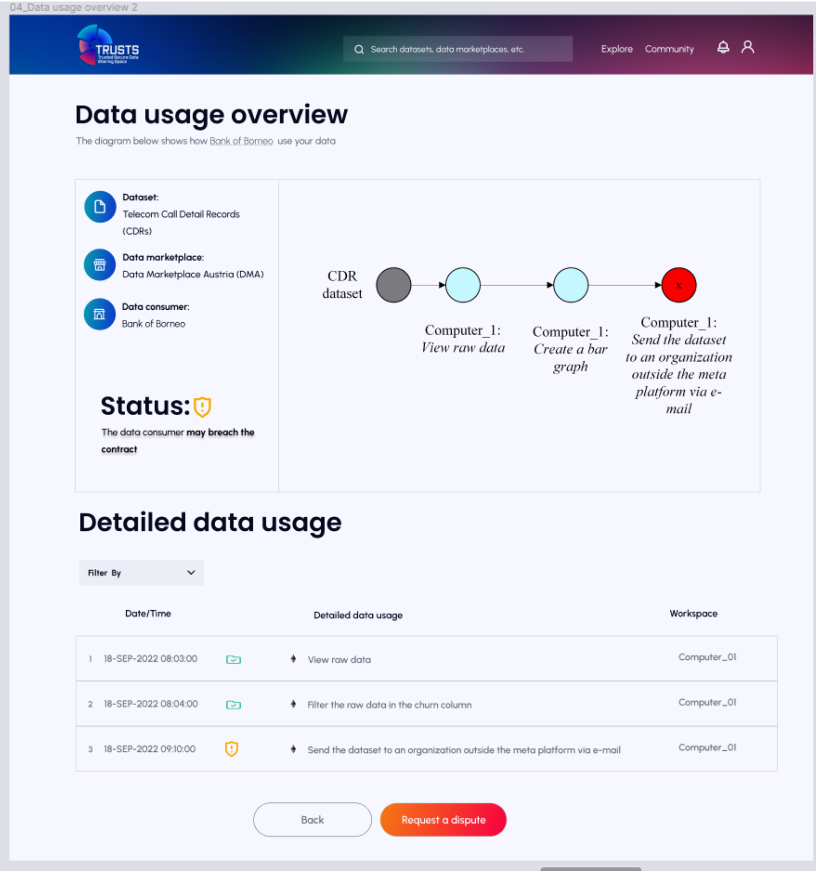
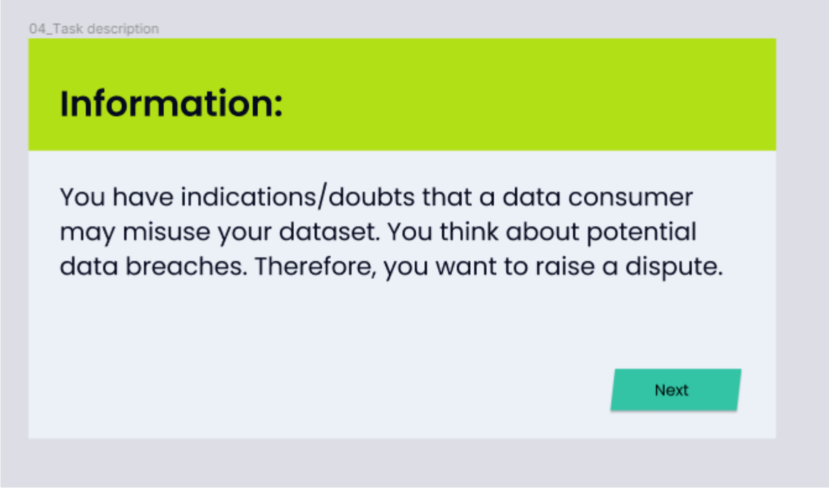
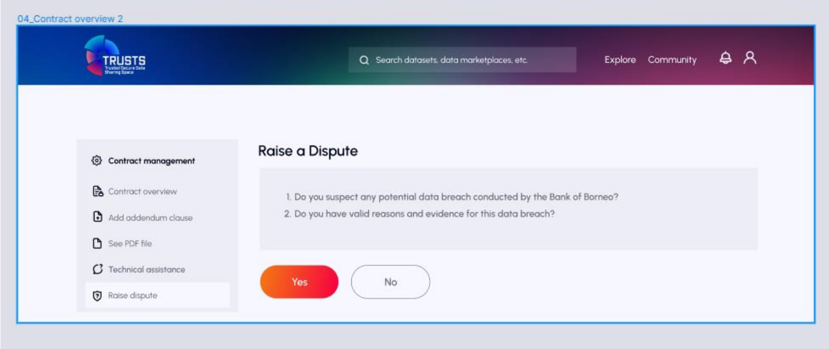
Online Appendix 5 presents relevant details of the process of conducting a controlled experiment in Chapter 8.

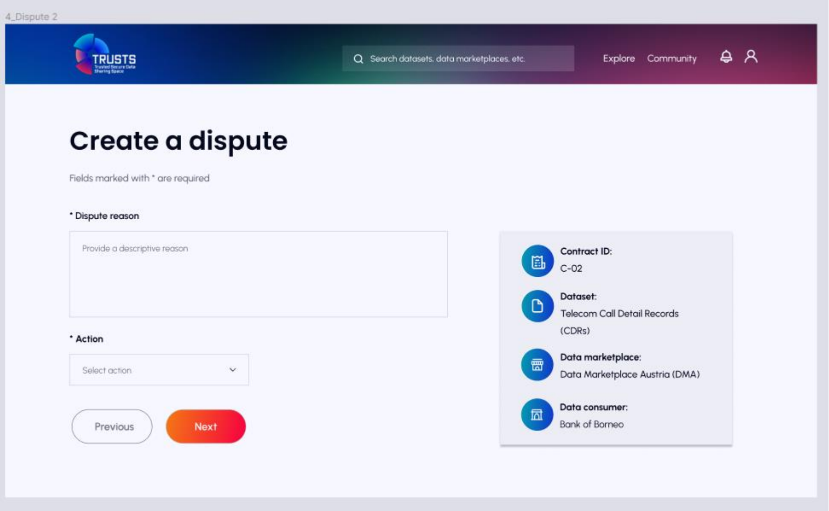
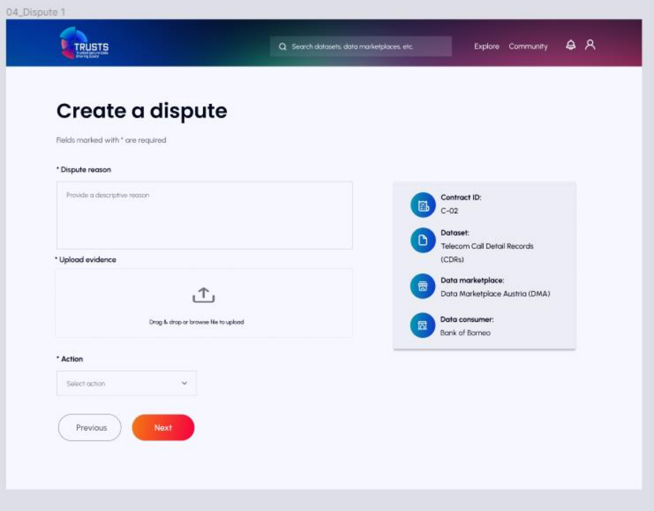
5.1 Prototype manipulation

5.1.1 Smart contracts vs. traditional contracts

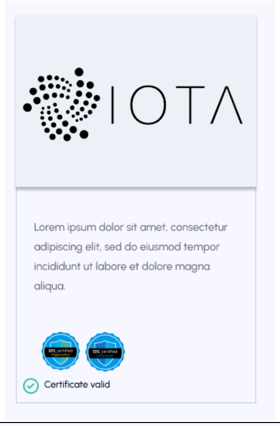
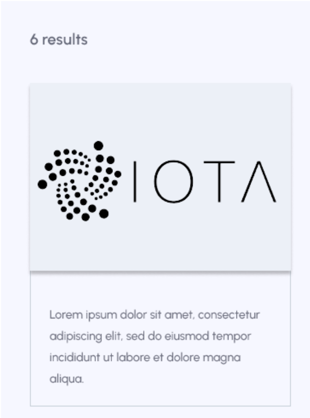
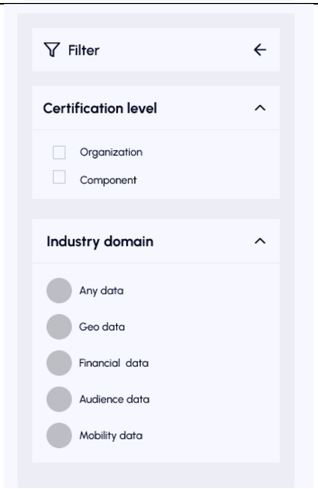
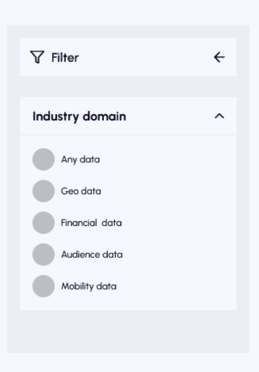
Part of Screen	Smart contracts	Traditional contracts
01_Homepage	 TRUSTS Business Processes Upload a dataset Upload your dataset by filling up the required information. Select marketplaces Select data marketplaces you want to transact with. Create contract Review requests from potential data consumers and generate contracts. Control shared-data Review data usage from data consumers.	Remove “control shared-data” as it is based on smart contract functionalities.  TRUSTS Business Processes Upload a dataset Upload your dataset by filling up the required information. Select marketplaces Select data marketplaces you want to transact with. Create contract Review requests from potential data consumers and generate contracts.
03_Smart contract explanation 2	 03_Smart contract explanation 2 TRUSTS Search datasets, data marketplaces, etc. Explore Community 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 View your 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? Smart contract is a means of **complying** with the EU data sharing laws and regulations	Remove any related smart contract explanations:  03_Contract explanation 2 TRUSTS Search datasets, data marketplaces, etc. Explore Community 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 View your contract

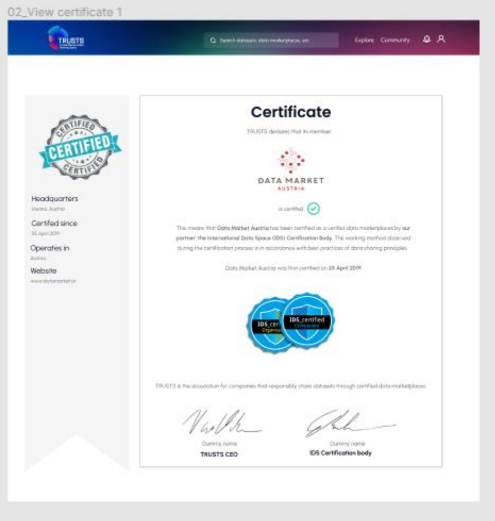
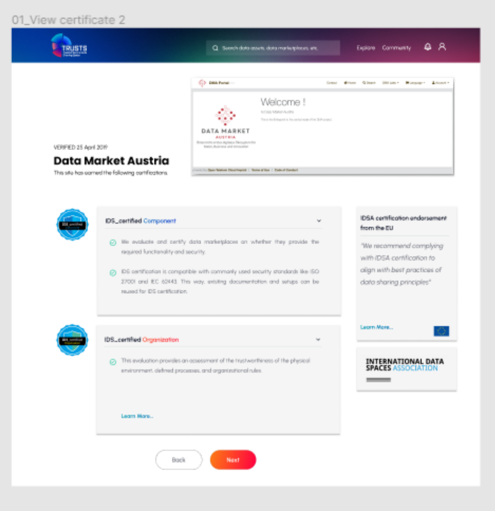
Part of Screen	Smart contracts	Traditional contracts
03_Contract overview	 03_Contract overview **Smart contract management** Contract overview Add addendum clause See PDF file View data usage Technical assistance Raise dispute	Adjust sidebar for contract overview:  03_Contract overview **Contract management** Contract overview Add addendum clause See PDF file Technical assistance Raise dispute
Task 4	 04_Task description **Task 4: Control how your dataset is used by data consumers** **Task description** Exercise how you can control your dataset using the following sub-tasks: Sub-task 4.1 : View the data usage overview from the **WorldwideBank** Sub-task 4.2 : View the data usage overview from the **Bank of Borneo** Sub-task 4.3 : Raise **a dispute** because of contract breach Sub-task 4.4 : Withdraw your dataset description (i.e., meta-data) from **Data Market Austria** Perform sub-task 4.1	 04_Task description **Task 4: Control how your dataset is used by data consumers** **Task description** Exercise how you can control your dataset using the following sub-tasks: Sub-task 4.1 : Raise **a dispute** due to potential data breach by **Bank of Borneo** Sub-task 4.4 : Withdraw your dataset description (i.e., meta-data) from **Data Market Austria** Perform sub-task 4.1

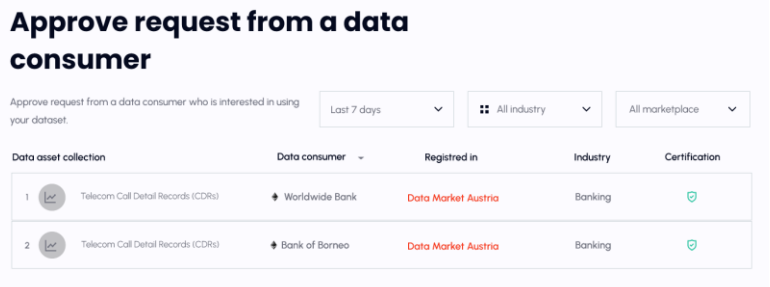
Part of Screen	Smart contracts	Traditional contracts
	With data usage:  04_Data usage overview 2 TRUSTS Search datasets, data marketplaces, etc. Explore Community **Data usage overview** The diagram below shows how Bank of Borneo use your data **Dataset:** Telecom Call Detail Records (CDRs) **Data marketplace:** 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* **Detailed data usage** Filter By 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 Back · Request a dispute	**Without data usage:**  04_Task description **Information:** You have indications/doubts that a data consumer may misuse your dataset. You think about potential data breaches. Therefore, you want to raise a dispute. Next  04_Contract overview 2 TRUSTS Search datasets, data marketplaces, etc. Explore Community **Contract management** Contract overview Add addendum clause See PDF file Technical assistance Raise dispute Raise a Dispute 1. Do you suspect any potential data breach conducted by the Bank of Borneo? 2. Do you have valid reasons and evidence for this data breach? Yes · No

Part of Screen	Smart contracts	Traditional contracts
	 4_Dispute 2 TRUSTS Search datasets, data marketplaces, etc Explore Community Create a dispute Fields marked with * are required * Dispute reason Provide a descriptive reason * Action Select action Previous Next Contract ID: C-02 Dataset: Telecom Call Detail Records (CDRs) Data marketplace: Data Marketplace Austria (DMA) Data consumer: Bank of Borneo	 04_Dispute 1 TRUSTS Search datasets, data marketplaces, etc Explore Community Create a dispute Fields marked with * are required * Dispute reason Provide a descriptive reason * Upload evidence Drag & drop or browse file to upload * Action Select action Previous Next Contract ID: C-02 Dataset: Telecom Call Detail Records (CDRs) Data marketplace: Data Marketplace Austria (DMA) Data consumer: Bank of Borneo

5.1.2 Certification vs. no certification

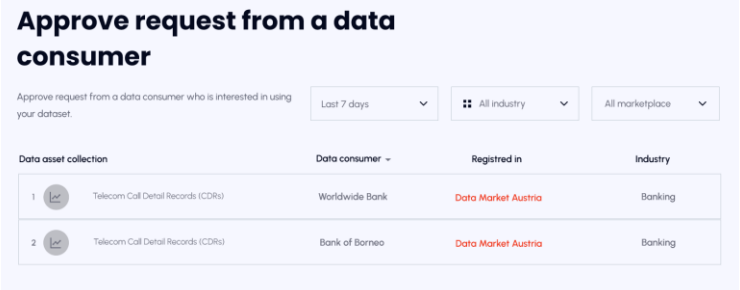
Part of Screen	Certification	No certification
02_Decide data Marketplaces 2	 IOTA Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Certificate valid	Remove the IDSA certification:  6 results IOTA Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
02_Decide data Marketplaces 2	 Filter Certification level □ Organization □ Component Industry domain ● Any data ● Geo data ● Financial data ● Audience data ● Mobility data	Remove this certification filter on 02_Decide data Marketplaces 2  Filter Industry domain ● Any data ● Geo data ● Financial data ● Audience data ● Mobility data

Part of Screen	Certification	No certification
02_View certificate 1	 02_View certificate 1 TRUSTS Search datasets, data marketplaces, etc. Explore Community CERTIFIED 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 certified This means that **Data Market Austria** has been certified as a verified 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** TRUSTS is the association for companies that responsibly share datasets through certified data marketplaces. Dummy name **TRUSTS CEO** Dummy name **IDS Certification body**	Completely remove the 02_View certificate 1 screen
01_View certificate 2	 01_View certificate 2 TRUSTS Search data assets, data marketplaces, etc. Explore Community DMA Portal Welcome ! DATA MARKET AUSTRIA VERIFIED 25 April 2019 **Data Market Austria** This site has earned the following certifications 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. Learn More... IDSA certification endorsement from the EU *"We recommend complying with IDSA certification to align with best practices of data sharing principles"* Learn More... INTERNATIONAL DATA SPACES ASSOCIATION 	Completely remove the 02_View certificate 2 screen

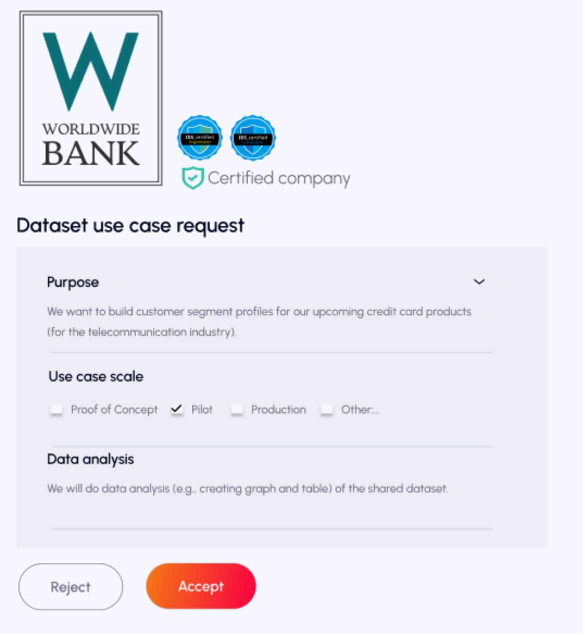
<table>
<tr><th>Part of Screen</th><th>Certification</th><th>No certification</th></tr>
<tr>
<td>03_Accepting data consumer 1</td>
<td>


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 ⌄

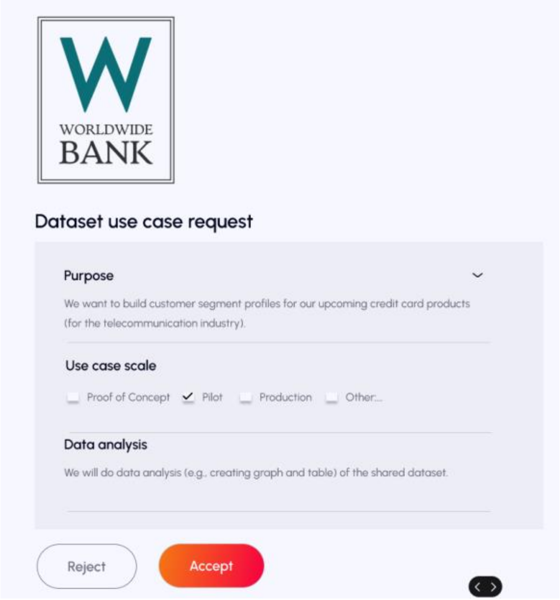
<table>
<tr><th></th><th>Data asset collection</th><th>Data consumer</th><th>Registred in</th><th>Industry</th><th>Certification</th></tr>
<tr><td>1</td><td>Telecom Call Detail Records (CDRs)</td><td>Worldwide Bank</td><td>Data Market Austria</td><td>Banking</td><td>✓</td></tr>
<tr><td>2</td><td>Telecom Call Detail Records (CDRs)</td><td>Bank of Borneo</td><td>Data Market Austria</td><td>Banking</td><td>✓</td></tr>
</table>
</td>
<td>
Remove the certification “checkmark”:



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 ⌄

<table>
<tr><th></th><th>Data asset collection</th><th>Data consumer</th><th>Registred in</th><th>Industry</th></tr>
<tr><td>1</td><td>Telecom Call Detail Records (CDRs)</td><td>Worldwide Bank</td><td>Data Market Austria</td><td>Banking</td></tr>
<tr><td>2</td><td>Telecom Call Detail Records (CDRs)</td><td>Bank of Borneo</td><td>Data Market Austria</td><td>Banking</td></tr>
</table>
</td>
</tr>
<tr>
<td>03_Accepting data consumer 3</td>
<td>


WORLDWIDE BANK
Certified company
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.
Reject · Accept
</td>
<td>
Remove the certification “checkmark”:



WORLDWIDE BANK
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.
Reject · Accept
</td>
</tr>
</table>

5.2 G*Power sample calculation for experiment

According to G*Power calculation, given the minimum power of 0.8, medium effect size, a significance level of 0.05, and the number of groups = 4, the minimum sample size is 128.

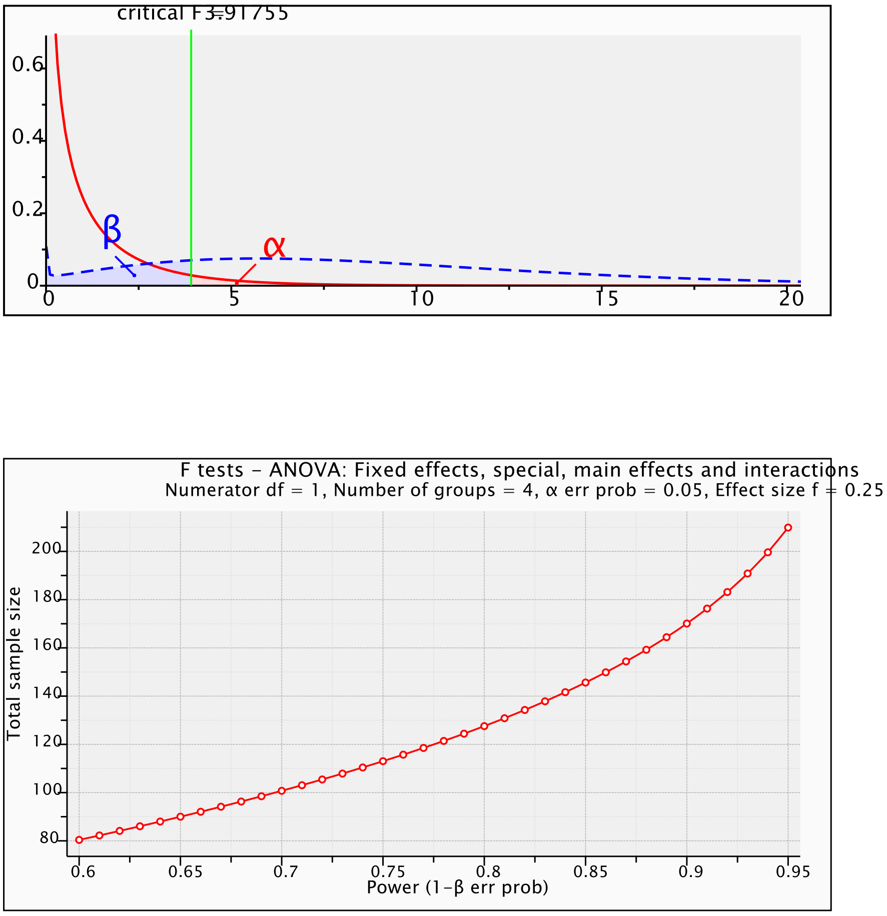


Figure 5.1. G*Power sample calculation for experiment

References

Aydin, A., & Bensghir, T. K. (2019). *Digital Data Sovereignty: Towards a Conceptual Framework*. 2019 1st International Informatics and Software Engineering Conference (UBMYK), Ankara, Turkey.

Banse, C. (2021). *Data Sovereignty in the Cloud - Wishful Thinking or Reality?* Proceedings of the 2021 on Cloud Computing Security Workshop, New York, New York, the United States.

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

Calzada, I. (2021). Data Co-Operatives through Data Sovereignty. *Smart Cities, 4*(3), 1158-1172. https://doi.org/10.3390/smartcities4030062

Chapdelaine, P., & McLeod Rogers, J. (2021). Contested Sovereignties: States, Media Platforms, Peoples, and the Regulation of Media Content and Big Data in the Networked Society. *Laws, 10*(3), 66. https://doi.org/10.3390/laws10030066

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

Corbett, J., & Cochrane, L. (2020). Geospatial Web, Participatory. In A. Kobayashi (Ed.), *International Encyclopedia of Human Geography (Second Edition)* (pp. 131-136). Elsevier. https://doi.org/10.1016/B978-0-08-102295-5.10604-3

Couture, S., & Toupin, S. (2019). What Does the Notion of "Sovereignty" Mean When Referring to the Digital? *New media & society, 21*(10), 2305-2322. https://doi.org/10.1177/1461444819865984

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

Dabrock, P. (2020). *How to Put the Data Subject's Sovereignty into Practice. Ethical Considerations and Governance Perspectives*. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, New York, New York, the United States.

De Filippi, P., & McCarthy, S. (2012). Cloud Computing: Centralization and Data Sovereignty. *European Journal of Law and Technology, 3*(2).

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.

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).

Gupta, A., Lanteigne, C., & Kingsley, S. (2020). SECure: A Social and Environmental Certificate for AI Systems. *arXiv preprint arXiv:2006.06217*.

Hartsch, F., Kemmerer, J., Labelle, E. R., Jaeger, D., & Wagner, T. (2021). Integration of Harvester Production Data in German Wood Supply Chains: Legal, Social and Economic Requirements. *Forests, 12*(4), 1-16. https://doi.org/10.3390/f12040460

Hellmeier, M., & von Scherenberg, F. (2023). *A Delimitation of Data Sovereignty from Digital and Technological Sovereignty*. ECIS 2023 Research Papers, Kristiansand, Norway.

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

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

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

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

Kukutai, T., & Taylor, J. (2016). *Indigenous Data Sovereignty: Toward an Agenda*. ANU press.

Kushwaha, N., Roguski, P., & Watson, B. W. (2020). *Up in the Air: Ensuring Government Data Sovereignty in the Cloud*. 2020 12th International Conference on Cyber Conflict (CyCon), Tallinn, Capital of Estonia.

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.

Lian, Y. (2021). *Data Rights Law 3.0*. Peter Lang Verlag. https://doi.org/10.3726/b18421

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

Mark, R. (2019, 2019/01/01/). Ethics of Public Use of AI and Big Data: The Case of Amsterdam's Crowdedness Project. *The ORBIT Journal*, *2*(2), 1-33. https://doi.org/https://doi.org/10.29297/orbit.v2i1.101

Martens, K., & Zscheischler, J. (2022). The Digital Transformation of the Agricultural Value Chain: Discourses on Opportunities, Challenges and Controversial Perspectives on Governance Approaches. *Sustainability*, *14*(7), 1-15. https://doi.org/10.3390/su14073905

Mawere, M., & Van Stam, G. (2020, 2020). Data Sovereignty: A Perspective From Zimbabwe. WebSci '20 Companion, Southampton, United Kingdom.

Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging Models of Data Governance in the Age of Datafication. *Big Data &amp; Society*, *7*(2), 1-15. https://doi.org/10.1177/2053951720948087

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

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.

Nugraha, Y., Kautsarina, & Sastrosubroto, A. S. (2015). *Towards data sovereignty in cyberspace*. 3rd International Conference on Information and Communication Technology (ICoICT), Bali, Indonesia. https://dx.doi.org/10.1109/icoict.2015.7231469

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

Otto, B., & Burmann, A. (2021, 2021/08/01). Europäische Dateninfrastrukturen. *Informatik Spektrum*, *44*(4), 283-291. https://doi.org/10.1007/s00287-021-01386-4

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

Peterson, Z. N. J., Gondree, M., & Beverly, R. (2011). *A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud*. Proceedings of the 3rd USENIX conference on Hot topics in cloud computing, Portland, Oregon, the United States.

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.

Polatin-Reuben, D., & Wright, J. (2014). *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet*. 4th USENIX Workshop on Free and Open Communications on the Internet, San Diego, California, the United States.

Redeker, M., Volgmann, S., Pethig, F., & Kalhoff, J. (2020). *Towards Data Sovereignty of Asset Administration Shells across Value Added Chains*. 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria.

Ruparelia, N. B. (2016). *Cloud Computing*. The MIT Press.

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.

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

Schleicher, D., Fehling, C., Grohe, S., Leymann, F., Nowak, A., Schneider, P., & Schumm, D. (2011). *Compliance Domains: A Means to Model Data-Restrictions in Cloud Environments*. 2011 IEEE 15th International Enterprise Distributed Object Computing Conference, Helsinki, Finland.

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.

Singi, K., Choudhury, S. G., Kaulgud, V., Bose, R. P. J. C., Podder, S., & Burden, A. P. (2020). *Data Sovereignty Governance Framework*. Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, New York, New York, the United States.

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

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

Vaile, D. (2014). The Cloud and Data Sovereignty After Snowden. *Journal of Telecommunications and the Digital Economy*, *2*(1), 1-58. https://doi.org/10.3316/informit.187308443693292

Zieglmeier, V., & Pretschner, A. (2023). *Trustworthy Transparency by Design*.

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