TRUSTS
Trusted Secure Data Sharing Space

D7.5
Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship II

Authors: A. Huber (G1), N. Simon (IDSA), A. Zuiderwijk (TUD), H. Ofe (TUD), A. Abbas (TUD), G. Avgousti (EBOS), B. Utermark (G1)

Additional Information: This deliverable examines the potential methods for safeguarding intellectual property rights for users of data markets, identifies potential threats, and outlines a plan for improving the protection of these rights.

January 2023

TRUSTS Trusted Secure Data Sharing Space

D7.5 Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship II

Document Summary Information

Grant Agreement No	871481	**Acronym**	TRUSTS
Full Title	TRUSTS Trusted Secure Data Sharing Space		
Start Date	01/01/2020	**Duration**	36 months
Project URL	https://trusts-data.eu/		
Deliverable	**D7.5 Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship II**		
Work Package	WP7 Business Model, Exploitation & Innovation Impact Assurance		
Contractual due date	31/12/2022	**Actual submission date**	31/01/2023
Nature	Report	**Dissemination Level**	Public
Lead Beneficiary	Governance One GmbH		
Responsible Author	Andreas Huber, Bert Utermark (G1)		
Contributions from	G1, TUD, IDSA, DIO, EBOS		

Revision History (including Peer Reviewing & Quality Control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V0.1	2022-11-07	10%	Initial structure / draft	Andreas Huber, Bert Utermark (G1)
V0.2	2022-12-14	75%	Contributions to the text	Andreas Huber (G1), Anneke Zuiderwijk (TUD), Antragama Ewa Abbas (TUD), Hosea Ofe (TUD), Natalia Simon (IDSA), Gianna Avgousti (EBOS)
V0.3	2022-12-20	80%	Draft restructuring and update	Andreas Huber (G1)
V0.4	2023-01-11	85%	Added information, comments from partners	all
V0.5	2023-01-25	96%	Completed first draft for review	Andreas Huber (G1)
V0.6	2023-01-26	98%	Peer review and quality control with TRUST partners from two organizations	Martin Kaltenböck (SWC) Lorenzo Gugliotta (KUL)
V0.7	2023-01-30	99%	Incorporated reviewers' comments/ finalisation of content, additional cross-reviews to other WPs	Andreas Huber (G1)
V1.0	2023-01-31	100%	Formatting and finalizing final version for submission	Andreas Huber (G1)

Disclaimer

Copyright message

Table of Contents

List of Figures

Glossary of terms and abbreviations used

Abbreviation	Description
AI	Artificial Intelligence
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Consortium Agreement
CTF	Cyber Threat Framework
DAO	Decentralised autonomous organization
DataNFT	Data non-fungible token
DLP	Data loss prevention
DMA	The Data Market Austria project is a pioneer of the data services ecosystem in Austria aimed to provide a data innovation environment by improving technology for secure data marketplaces and cloud interoperability.
DS	Data Stewardship
E2E	End to End
EDI	Electronic Data Interchange
EU	European Union
FAIR	Findable, Accessible, Interoperable and Reusable
FTP	File Transfer Protocol
GA	Grant Agreement
GDPR	General Data Protection Regulation
IoT	Internet of Things
IPR	Intellectual Property Rights
IPRED	Directive on the enforcement of intellectual property rights
ML	Machine Learning
NIST	National Institute of Standards and Technology
OMG	Object Management Group
OWL	Web Ontology Language
RDF	Resource Description Framework
SME(s)	Small Medium Enterprises
STIX	Structured Threat Information eXpression
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege
TRUSTS	Trusted Secure Data Sharing Space
TRUSTS OpCo	TRUSTS Operating Company
WP	Work Package
XML	Extensible Markup Language

Executive Summary

This deliverable is part of the Work Package 7 “Business Model, Exploitation & Innovation Impact Assurance” of the ''TRUSTS - Trusted Secure Data Sharing Space” project and gives a detailed description and outlining of the related: Legal requirements to be embedded in the platform's terms of use, defined mechanisms to report suspected Intellectual Property (IP) infringement, proposed onboarding Intellectual Property Rights (IPR) protection information and education requirements for TRUSTS user groups, and proposed Data Stewardship Support Services for different (potential) data provider groups. The purpose of this deliverable was to set up the guidelines on how IPR will be managed by the TRUSTS Operating Company (TRUSTS OpCo).

The deliverable issued two types of mechanisms for IP protection: technical measures and contractual measures that need to be considered on a later stage of establishing the TRUSTS OpCo. Technical measures include securing IP both physically and digitally, data anonymization, and ensemble learning. The International Data Space Association (IDSA) approach is also offering several mechanisms to support the IPR protection, including the IDS metadata broker and the IDS Clearing House. In terms of contractual measures, the deliverable is offering a Code of Conduct for using the TRUSTS Platform and Terms and Conditions for using TRUSTS Services. The document concludes with recommendations towards the conceptualization of TRUSTS aiming at efficient and affordable IPR protection mechanisms.

Task 7.3 in WP7 was successfully concluded. In deliverable D58 (7.10) the intellectual property rights (IPR) aspects of data exchange portals, specifically focusing on the organizational and operational aspects of IPR protection for the TRUSTS operator and the internal IPR of the software used in the TRUSTS platform by the consortium partners were investigated. The economic mechanisms for cost and revenue sharing within TRUSTS consortia were examined, as well as legal tools for the protection of data exchanged via the TRUST platform.

The task also delved into concepts for data governance and data stewardship for users of the TRUSTS platform, which includes establishing control over data ownership, access, and usage decisions to minimize the risks associated with data sharing. Additionally, it highlighted the benefits of open datasets for companies and the different types of open datasets available, such as open government data, open research data, and data openly shared by other companies.

The task also developed a process of threat modelling, which is a method for identifying, analysing, and assessing potential threats to an organization or system. The TRUSTS threat modelling process was defined as an iterative loop, starting from an early phase of the design of an application or data model, continuing throughout its whole life cycle. The importance of supporting data sharing and commercialization while considering the needs and requirements of various stakeholders, including data providers and users, prioritizing security, reliability, scalability, flexibility, and simplicity was emphasized.

Furthermore, T7.3 proposed the establishment of a TRUST-DAO (Decentralized Autonomous Organization) model for managing services, software licenses, and cost sharing within the TRUSTS operating company (OpCo) using dataNFT-based services and license cost sharing system within a TRUSTS-DAO framework. It was explained that implementing dataNFT in a TRUSTS-DAO model can provide a secure and transparent way to protect members' intellectual property rights (IPR) and manage the usage and ownership of software licenses and software components in the TRUSTS platform.

WP	Functional Context	Name of TRUSTS module / set of software components	Description
WP3	Smart contracts (T3.2)	Smart contract executor	Tool providing and executes smart contracts
WP3	Semantic layer (T3.4)	Vocabulary Management System	A UI where users can manage vocabularies that are to be use through the project
WP3	Semantic layer (T3.4)	Metadata Broker	Central metadata repository of the platform. Is compliant to the IDS communication protocol
WP3	Semantic layer (T3.4)	Metadata Storage System	The triplestore (database) where the metadata is actually stored in RDF format.
WP3	Semantic layer (T3.4)	Platform Interface	The base component of the user interface that each node in the platform will have, allows for onboarding searching and consuming assets.
WP3	Semantic layer (T3.4)	IDS Extension for CKAN	An extension that is required to make the CKAN platform interact with IDS components.
WP3	Semantic layer (T3.4)	Vocabulary Extension for CKAN	An extension that is required to have the CKAN platform software to use the vocabularies in asset onboarding
WP3	Semantic layer (T3.4)	TRUSTS Client	
WP3	Brokerage (T3.6)	Recommender system	Providing services to recommend connections between datasets, services and users
WP3	Transfer learning methodology		
WP4	De-anonymisation / anonymisation toolkit (T4.3)		
WP4	Metadata schema for data assets		
WP4	Protocol for metadata exchange		
WP4	Protocol for Private Set Intersection	PSI library PSIttacus	Java library that enables two parties to find identical data in their data sets without sharing the full sets with each other

Table 11 chapter 6.3.4 from D58 (D7.10): Functional context of software components used in TRUSTS

In T7.3, the importance and necessity of creating specialized contracts for TRUSTS OpCo to protect the intellectual property rights (IPR) of users on the TRUSTS platform were discussed. It was found that data, which is not typically protected by patent or copyright laws, can be owned but enforcing legal claims for it can be difficult if it is taken without permission. There is a need for contracts that regulate the use of the TRUSTS platform and provide legal certainty. Two draft contracts were presented: a "Code of Conduct for using the TRUSTS Platform" (CC) and "Terms and Conditions for using TRUSTS Services" (TC). The CC serves as general guidelines for user behaviour on the platform and does not contain any enforceable provisions. The TC, on the other hand, governs the conditions under which transactions between users take place, defining the rights and obligations of data providers and data consumers, as well as the legal position of the TRUSTS OpCo. It is acknowledged that the drafts presented will require revision and enhancement as the TRUSTS OpCo is established.

The draft "Code of Conduct for using the TRUSTS Platform" (CC) serves as a framework for amicable cooperation on the TRUSTS data exchange platform. The code aims to establish and promote efficient and targeted data exchange within the framework of the trading platform, with the goal of improving and optimizing the use of data, and achieving positive outcomes for employment and growth, as well as sustainable social stability and prosperity. The code sets out general principles and rules of conduct for participants, including compliance with legal provisions, particularly the General Data Protection Regulation (GDPR) and transparency regarding the origin and traceability of data collection. Participants are expected to act in accordance with principles of integrity, fairness, and partnership, and to communicate with each other in a respectful manner. The code also recognizes that data is sensitive and emphasizes the importance of preserving informational self-determination and protecting privacy. The code is intended to be a living document and will be supplemented and expanded in the future to include sanctions and penalties if relevant findings are obtained through the operation of TRUSTS.

During the project, a draft of the "Terms and Conditions for using TRUSTS Services" (TC) was developed as a proposal for what the terms and conditions could look like when the TRUSTS OpCo is operational. The draft TC is intended to provide a legal framework for the platform, but it is acknowledged that certain decisions regarding the organization and structure of the platform may need to be changed or adapted at a later stage. The draft TC is formulated in such a way that it can apply to different legal forms of the operating company. The TC defines key terms such as "TRUSTS Platform”, "Data”, “Data Assets” and "Participant". It also explains the process of "Listing," which is a requirement for all participants to go through before they can offer or request data on the platform. The TC also outlines the different functional roles on the platform, including Data Provider, Data Demander, and Operator. It states that the TC governs the rights and obligations of all participants in relation to TRUSTS OpCo.

The protection of IPR in datamarkets is crucial to guarantee the security, transparency and fairness of data exchange platforms for both data providers and consumers. This can be achieved through the deployment of technical measures such as encryption, secure data storage and monitoring mechanisms, as well as by reaching a consensus among stakeholders on the IPR of services and software components. The IDS metadata broker, IDS clearing house and TRUST-DAO model were proposed to manage and protect IPR in data exchange platforms.

In the era of increasing use of data assets, it is crucial for data exchange platforms to provide a secure and profitable environment for data exchange. This final report outlined recommendations for securing intellectual property rights (IPR) in data markets and ensuring the longevity of these platforms: Firstly, the development of standard data exchange protocols is crucial for seamless data integration while preserving IPR protection. Secondly, implementing monitoring and reporting mechanisms, such as the ones developed in the TRUSTS project, will allow data providers to monitor and report any unauthorized access to their data. Thirdly, strengthening technical measures for data protection, like encryption and secure storage, will ensure the protection of IPR in data exchange platforms. Fourthly, the enhancement of security protocols for data exchange, including encryption techniques, will prevent unauthorized access and protect against data theft and manipulation. Fifthly, establishing a data exchange governance framework covering data privacy, protection, and ownership is necessary for secure and profitable data exchange. Sixthly, regulation of data exchange contracts will ensure transparency and fairness for both data providers and consumers. Seventhly,

collaboration between data providers, consumers, and exchange platforms is essential for the success and sustainability of data platforms. This can be achieved through industry forums, working groups, and support initiatives such as the Data Space Support Centre. Eighthly, improving user awareness and education on IPR protection will ensure data providers understand the importance of protecting their data and IPR. Ninthly, integrating IPR protection into data management systems, especially for SMEs, will allow for easy management of IPR and control over data access. Tenthly, investment in research and development for innovative solutions for IPR protection in data exchange platforms will ensure the long-term security and effectiveness of these platforms. Eleventhly, adopting international standards for IPR protection in data markets will ensure a uniform approach and interoperability between data exchange platforms globally. Twelfthly, promoting the harmonization of legal frameworks for IPR protection in data markets across countries and regions will provide a stable environment for secure data exchange and protect the rights of all parties involved.

1 Report Synopsis: Key Findings and Organizational Overview

1.1 Outlining the Structure of this Deliverable

The following section provides an overview of the deliverable's structure. The document lays out a description of the general context and detailed information regarding supporting mechanism for IPR protection.

The structure of this deliverable is the following:

Section	Caption	Short explanation
Section 1	Uncovering the key findings and organization of this report	Introduction to this report with a definition of IPR and an overview of each chapter.
Section 2	TRUSTS Support on Data Governance and Data Stewardship for Users	Offers a summary of the current state and the regulations and policies for IPR protection
Section 3	TRUSTS Support on Data Governance and Data Stewardship for Users	Provides the most promising approaches of Data Governance and Data Stewardships in connection with data sharing spaces while discusses their advantages with respect to TRUSTS and discusses how to achieve data security in the context of data sharing
Section 4	Comprehensive threat protection: The TRUST Threat Model	Conceptualization of a TRUSTS threat model for protecting Intellectual Property Rights (IPR). It explains the development of the model and its various components, which are designed to identify and assess potential threats to IPR.
Section 5	TRUSTS Monitoring & Surveillance Mechanisms for IPR Protection	Suggests concepts and actual development of monitoring and surveillance mechanism for managing IPR of the TRUSTS platform
Section 6	Managing Intellectual Property Rights (IPR) within a TRUSTS Operating Company (OpCo): Organizational and Operational Considerations	Conceptualization of protecting IPR within the context of a TRUSTS Operating Company (OpCo). It explores the organizational and operational considerations that are involved in effectively protecting and utilizing IPR within the OpCo environment. The report covers topics such as the identification and protection of IPR assets, the development of internal policies and procedures for managing IPR, and the alignment of IPR strategies with the overall goals and objectives of the OpCo.
Section 7	TRUSTS Platform Contractual Measures for IPR protection	Introduces some concepts regarding contractual measures for IPR protection and a draft Code of Conduct and a draft “Terms & Conditions” for the future TRUSTS platform Op Co.
Section 8	Conclusions and Recommendations	Concludes the report and provides recommendations for further development of IPR protection in data markets.

1.2 Mapping Projects' Outputs

The purpose of this section is to map TRUSTS GA commitments, both within the formal deliverable and task description, against the project's respective outputs and work performed.

TRUSTST Task:		Respective Document Chapter(s)	Justification
T7.4 *IPR and Data Stewardship*	In this task we target challenges around Intellectual Property Rights (IPR) and Data Stewardship (DS). The goal is to protect original data owners/providers and re-sellers of enriched data whilst supporting innovation and value extraction. Obviously, minimum legal requirements must be reflected in the technical design of the TRUSTS platform as well as in the general terms and governing contracts. This must be complemented with effective mechanisms to report and address suspected IPR infringement. But beyond, TRUSTS must define its overall approach as to how active its role should be in the domain of IPR protection, and – within legal confinements – where to strike the balance between opposing interests of different TRUSTS user groups vis-à-vis a sustainably viable business model. Particularly for SMEs, regulations and (dispositive) rights regarding the use and re-use of their IP is not self-evident. The same holds true for requirements towards SMEs acting as buyer of data for aggregation, enrichment, and onward sales. The task must define how TRUST will go about related segmentation of user groups (if any), and different onboarding as well as continuous information/education requirements and services. In turn, this links to enabling Data Stewardship on the side of (prospective) data providers. Existing attempts of data markets have often suffered from the lack of available data and data quality because many organizations – in particular SMEs and semi-governmental agencies do not have a sufficient internal data governance, and do not "know what they know" or how to commercialize this data in a meaningful, yet protected way that also enables them to retain control over their data integrity. This task will research the support services requirements for different (potential) data provider groups to optimize eased attraction and onboarding of (SME) data providers onto the platform, to enable value creation and extraction within TRUSTS.	Chapters 2, 3 Chapter 4 Chapter 7 Chapter 5 Chapter 2 Chapter 3 Chapter 6	Introducing chapters to the topic Overview to existing and necessary technical mechanism for protecting IPR Draft Code of Conduct and Terms & Conditions for further use and adaption Perspectives and needs of data market users (seeker and provider) vs. perspective from the operator of the data market
TRUSTS IPR and Data Stewardship Deliverable			

Table 1: Adherence to TRUSTS GA Deliverable & Tasks Descriptions

1.3 Interdependencies of Task 7.3 with other Tasks in the Project

Task T7.3 has interdependencies with several other work packages. First and foremost is the development of a sustainable business model. WP T7.1 is dedicated to this task. Depending on the results of WP T7.1, this had an impact on the work of WP T7.5, which dealed with the business planning and commercialization issues. WP T7.3 acknowledged the results of the other WP tasks.

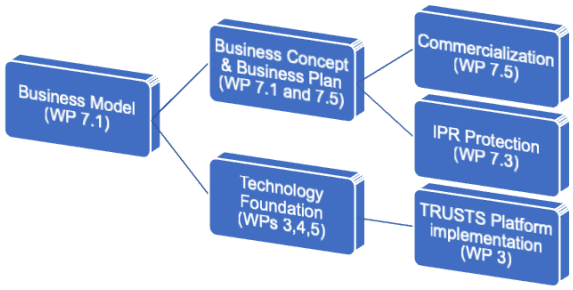

Figure 1: Interdependencies of Task 7.3 with other tasks in the project

1.4 Extracting the Core Information: A Summary of the Most Relevant Results and Proposals in this Deliverable

1.4.1 Summary of Chapter 2 - Concept of Mechanisms for Protecting IPR

The chapter discusses the approach of TRUSTS to protecting intellectual property rights (IPR) in data assets. The text explains that IPR management is an important part of any business strategy and that traditional forms of IPR protection, such as copyright and patents, do not apply to data. The text then lists several options for protecting IPR in a data platform like TRUSTS, including protection through contracts, contract-based access mechanisms to data, technical security systems for transmission, storage, and access, monitoring of user behaviour, encryption and watermarking of data, and protection by the nature of the data. The text also includes a table that shows the expected protective effect and complexity of implementation for each option.

The chapter further discusses the current state of issue and solutions for intellectual property rights (IPR) protection in the context of the TRUSTS project. The text explains that IP management is an important part of the lifecycle of research and innovation projects and that the technological revolution, and the emergence of new technologies and business models have created new opportunities and challenges for protecting intangible assets. The benefits of protecting IP are highlighted, such as protecting inventions, ensuring the quality and origin of products, generating revenue through licensing contracts and increasing the market value of a business. Only some kind of data are protected by its origin (for example protected by copyright or patents). The other kinds of data are hardly protectable with existing laws. It is also mentioned that according to the project's general assembly, the legal framework governing the use and re-use of IP are not self-evident, particularly for small and medium-sized enterprises. It is explained that partners in the project are recommended to inform each other about their individual protection activities plans, especially for potentially joint IP, and that the primary function of an IP right is to give its holder a competitive advantage in commercial activities by preventing unauthorized exploitation.

1.4.2 Summary of Chapter 3 - TRUSTS Support on Data Governance and Data Stewardship for Users

The text discusses the importance of data governance and data stewardship for users of the TRUSTS platform. It explains that data governance is defined as the activities of exercising control over data ownership, access, and usage decisions to minimize the risks associated with data sharing. Data governance is important to TRUSTS because it helps organisations monitor data sharing and usage conditions, and it needs to balance

sharing and exclusivity to prevent data misuse or privacy harm. Data stewardship is an essential aspect of data governance and encompasses the tactical management and oversight of a company's data assets. Data stewardship facilitates collaboration between business and IT, drives the correction of data issues, and improves the overall data management process. Some factors and sub-factors of data governance are especially important for data sharing, such as decision rights allocation for involved actors, definition criteria identification for data ownership and access, contribution estimation, data use case, conformance, monitoring, and data provenance.

The chapter is about TRUSTS Data Stewardship support services for data providers. It discusses the benefits of open datasets for companies and the different types of open datasets available for companies to use, such as open government data, open research data, and data openly shared by other companies. Open datasets can increase a company's competitive advantage, contribute to economic growth, and help entrepreneurs make more informed decisions about their business models. Various business models are based on open government data and the value proposition of each business model archetype. Additionally, researchers may be hesitant to share their data openly due to concerns about commercial or competitive misuse of their data, but the expectation to generate wealth through the downstream commercialization of research outputs may motivate researchers to openly share their data.

TRUSTS created a platform for data sharing and commercialization that considers the needs and requirements of various stakeholders, including data providers and users. The platform prioritized security, reliability, scalability, flexibility, and simplicity. It supports electronic, confidential processes and open data, as well as direct services to end-customers. Participants in an electronic survey conducted by TRUSTS highlighted a need for the platform to support subscription options, connection with popular marketplaces, easy retrieval of datasets, keyword-based searching and browsing through structured categories, ratings and comments from other users, anonymization of datasets, and networking between partners. Additionally, participants identified standardization gaps and ways to boost the data marketplace, such as providing more guidelines for data anonymization and making the process of buying and selling data more efficient.

1.4.3 Summary of Chapter 4 - Navigating the intersection of IPR and cybersecurity in data exchange platforms: Threat Modelling for TRUSTS

In summary, threat modelling is a process for identifying, analysing, and assessing potential threats to an organization or system, which involves several different phases and steps. This process involves developing and applying a possible representation of adversarial threats. For the TRUSTS platform, the process starts with identifying security objectives and assessing the possible impact on the applications, followed by decomposing the applications, identifying threats, documenting the threats, and rating the threats to prioritize and address the most significant ones. The TRUSTS threat modelling process needs to be an iterative loop, starting from an early phase of the design of an application or data model, continuing throughout its whole life cycle. Preliminary stages and preparation of the threat analysis include establishing a systematic information security process, defining the scope of the security concept, conducting a structural analysis, and defining basic requirements for the risk analysis. The investigation objects during the analysis (structure analysis) include all relevant components of the threat such as business processes, critical information, applications, affected rooms and networks. Different types of threats for data exchange portals include physical threats such as fire, water, and natural catastrophes, as well as cyber threats such as cyber-attacks, malware, and social engineering. It is important to have strong security measures in place to mitigate these risks and regularly monitor and audit to detect potential vulnerabilities.

Key Findings of Chapter 4.1 - Data Exchange Portal

Data exchange portals like the TRUSTS platform are unique in the way they facilitate the exchange of data between various organizations, individuals, or systems. The data exchanged through TRUSTS platform can be easily replicated and used simultaneously, making it essential to have proper security measures in place to protect the data. Data management is also crucial, as the ability to support a variety of data formats, including text, spreadsheets, and database formats is important. Additionally, TRUSTS as data exchange portal can be connected or integrated with other systems to enable easy data exchange between different systems. The

nature of data is such that it only holds value or relevance when it is used in its specific context or combined with other data. This makes traceability of data lineage challenging, as it is nearly impossible to trace the exact path of the data once it has been extracted from a data set or database and combined with other data. Additionally, reluctance to share data is a common issue, where individuals or institutions are unwilling to share or provide low-quality data. The true value of data is only revealed when it is shared. To ensure proper handling of data, it must be accompanied by information about its origin, particularly to demonstrate credibility, quality, and security. The TRUSTS platform has functions to store this metadata, such as data lineage, data provenance, and meta data information. This helps to address some of the challenges in handling data and ensures that data is used in the correct context.

Key Findings of Chapter 4.2 - Process of threat analysis

The potential influencing factors on a threat model include the technology and architecture of the TRUSTS platform, the types of data being exchanged, the users of the portal, and the regulatory environment. The technology and architecture of the data exchange portal can affect the potential threats, as certain technologies or design choices may make the portal more vulnerable to certain types of attacks. For example, a portal that uses outdated software or lacks proper security measures may be more susceptible to hacking or data breaches. The types of data being exchanged on TRUSTS can also affect the potential threats. For example, sensitive personal data or financial information may attract more malicious actors than less sensitive data would. The users of TRUSTS, including the data providers and consumers, can also influence the potential threats. For example, if TRUSTS is primarily used by government agencies, the potential threats may be different than if it is primarily used by businesses. Different sectors will have a different threat potential: some data is only valuable because of its freshness – since other data is valuable due to its insights or as results from further transformation of data. So, within different sectors and according to the specific type and necessity of protection, the threat level might differ very much. Finally, the regulatory environment, including data protection laws and industry standards, can also affect the potential threats. For example, compliance with data protection law and other relevant regulations may require additional security measures to be in place.

Key Findings of Chapter 4.3 - Preliminary stages and preparation of the threat analysis

To conduct a thorough threat analysis for a data exchange portal, several preliminary steps must be taken. These include establishing a systematic information security process, defining the scope of the security concept through a structural analysis, and determining the basic requirements for the risk analysis. Determining the basic requirements for risk analysis includes establishing a policy for handling risks and assigning responsibilities to different organizational units. The investigation objects during the analysis include all relevant components of the threat, such as business processes, critical information, and applications. The structural analysis is divided into sub-tasks such as capturing associated information, creating a network plan, and listing IT relevant objects. Similar objects are grouped together to reduce complexity and the need for protection is determined based on the potential damage to relevant sub-objects. The threat analysis should be an iterative process, as the underlying technology and the platform itself evolves.

Key Findings of Chapter 4.4 - Different types of threats for data exchange portals

In summary, the potential risks associated with data exchange portals can be grouped into general threat types, including natural disasters, power and communication failures, and cyber-attacks. Cyber-attacks are considered the greatest threat to data exchange portals as hackers or other criminals try to access the portal, illegally access data and information, or disrupt the operation itself. To mitigate this threat, strong security measures such as two-factor authentication should be implemented and regularly monitored for potential vulnerabilities. Cyber-attacks can also be divided into several stages, including reconnaissance, scanning, access, and escalation.

Key Findings of Chapter 4.5 - Possible impact analysis and deployment of counter measures

In addition to identifying the potential risks associated with data exchange portals, it is also necessary to evaluate them and to record the threats combined with their likelihood & impact of a threat. A procedure

and general standard need to be specified, which details which threats need to be addressed first and which ones might have less criticial potential. One way to evaluate the risk of a threat is by measuring the probability of occurrence and the possible damage using a scale of 1 - 10. Then, by combining the results of probability and possible damage, the risks can be categorized as high, medium, or low. Another way to evaluate the risks is by using a method called DREAD. This method analyzes five dimensions of the threat: Damage potential, reproducibility, exploitability, affected users, Discoverability, and assigns a score to each dimension. Once the possible risks of a threat have been identified, it is then necessary to establish acceptance criteria or the actual options for dealing with them. These options include avoiding, reducing, transferring, or accepting the risk. To make these decisions, organizations should define risk acceptance criteria and handle the risks accordingly.

1.4.4 Summary of Chapter 5 - TRUSTS Monitoring & Surveillance Mechanisms for IPR Protection

Key Findings of Chapter 5.2 - Technical Measures to protect IPR in data sharing

In this section, the focus is on how to achieve data security in the context of data sharing specifically in relation to Intellectual property (IP) protection. The first step is to identify and map the IP assets within a project. This includes listing and analyzing all expected IP values in a systematic way to have a sort of project IP portfolio. To achieve this, an IPR Repository is created to represent the living IPR database during the project's implementation. This will identify project intangibles, retrace their ownership, and help partners to recognize their IP assets and ascertain the existence of third parties' rights. Technical measures such as Artificial intelligence (AI) are also discussed to protect IPR in data sharing. An operational legal framework for the development of European AI and public policies that correspond with the issues at stake, particularly with reference to the training of people in Europe and financial support for applied and fundamental research are also important to include. Lastly, the importance of encouraging the sharing of data generated in the EU to stimulate innovation and creativity in this area is emphasized.

Key Findings of Chapters 5.3 & 5.4 - The IDS metadata broker as matching mechanism and gatekeeper between data provider and data consumer and IDS Metadata Broker and IDS Connector as instance of access and usage control

The IDS metadata broker is a mechanism that enables IP mapping and the representation of the IPR database during the project's implementation. It is defined as an intermediary that manages a metadata repository that provides information about the data sources available in a data space. It can be considered as an optional component of a data space built according to the IDS Reference Architecture Model and is a specialized IDS Connector. The IDS metadata broker consists of a service for data source registration, publication, maintenance, and query, based on an index. It may also provide additional services that must be described by the IDS Information Model. The metadata broker is not involved in the process of data exchange. It is meant to provide an interface for the data provider to send their metadata, which is needed to be stored in a repository. The metadata should then be able to be queried by data consumers in a structured manner. The IDS metadata broker and IDS Connector are instances of access and usage control and are used in the Mobility Data Space to enable new mobility offerings and ensure data sovereignty.

Key Findings of Chapter 5.5 - The IDS Clearing House as monitoring instance of transactions and indicator of fair use

The IDS Clearing House is an optional component of the IDS Reference Architecture that provides a set of clearing and settlement functions for data sharing. It serves as an intermediary between a data provider and a data consumer, ensuring that both parties stick to the contractual obligations, including data usage policies and payment conditions. The Clearing House has functionalities that touch the data exchange and sharing process before, during, and after the process. The Clearing House can track and monitor the use of data to ensure that IPR are being protected and can function as an instrument for conflict resolution if a violation is reported. It is a specialized IDS Connector that communicates with other IDS Connectors and should have a distributed implementation, business service orientation, and interoperability with other intermediary roles.

1.4.5 Summary of Chapter 6 - Managing Intellectual Property Rights (IPR) within a TRUSTS Operating Company (OpCo): Organizational and Operational Considerations

Key Findings of Chapter 6.2 - Navigating the Challenges of Managing Intellectual Property Rights (IPR) for Services and Software Components for Future TRUST Platform Implementation

In summary, the chapter discusses the IPR aspects of cost and revenue sharing within the TRUSTS project, which focuses on developing a concept and prototype for sharing data through a data market. It looks at the organizational and operational aspects of IPR protection and the internal aspects of IPR management, specifically focusing on the intellectual property of the software used in the TRUSTS platform by the TRUSTS consortium partners. It explores different aspects of IPR protection such as organizational aspects of IPR protection for the TRUSTS operating company (OpCo) , economic mechanisms for cost and revenue sharing within TRUSTS consortia, and legal tools for the protection of data exchanged via the TRUSTS platform. The chapter concludes that the establishment of an operating company is a complex undertaking from an organizational, economic, legal, functional, and technical perspective.

This text discusses the challenges of managing intellectual property rights (IPR) for services and software components in the implementation of the TRUSTS platform. It mentions different options for protecting IPR in a data platform like TRUSTS, such as protection through contracts, access mechanisms, technical security systems, monitoring of user behavior, encryption, and watermarking. It also highlights the importance of a further elaborated concept to support these options and the importance of cross-system mapping of data assets, actualization of metadata from decentralized data storage and data networks, and interaction of automatic digital contracts and data assets for the future TRUSTS platform. The text also discusses the challenges of dealing with the timeliness of metadata, marking options, and the need for a system for dealing with the inaccessibility of certain data assets.

Key Findings of Chapter 6.3 - Conceptualizing Intellectual Property Rights (IPR) Management for Services and Software Components for Future TRUST Platform Implementation

In summary, this section discusses various mechanisms for protecting intellectual property rights (IPR) in the context of data sharing within the TRUSTS project. One mechanism proposed is the use of an IDS metadata broker and IDS connector as a matching mechanism and gatekeeper between data providers and consumers, which allows for the efficient management of IP and the identification of exploitable results. Another mechanism proposed is the use of an IDS Clearing House as a monitoring instance of transactions and indicator of fair use, which ensures that both parties stick to the contractual obligations and can be used for conflict resolution if a violation is reported. Additionally, the section proposes a consensus on the intellectual property rights of services and software components among TRUSTS consortium partners and implementing a TRUSTS-DAO (Decentralized Autonomous Organization) model for managing services, software licenses, and cost sharing in the TRUSTS operating company (OpCo). This approach suggests using dataNFT-based services and license cost sharing system within a TRUSTS-DAO framework, which allows for transparency, decentralization, security, flexibility, and lower transaction costs. Lastly, the section suggests implementing dataNFT in a TRUSTS-DAO model for secure and transparent protection of members' IPR and managing the usage and ownership of software licenses and software components in the TRUSTS platform. DataNFTs can be used for tracking and verifying ownership of licenses, sharing software costs among partners, and managing revenue distribution among partners based on their contributions to the company.

1.4.6 Summary of Chapter 7 - TRUSTS Platform Contractual Measures for IPR protection

Key Findings of Chapter 7.2 - Draft "Code of Conduct for using the TRUSTS Platform" (CC)

In T7.3, the importance and necessity of creating specialized contracts for TRUSTS OpCo to protect the intellectual property rights (IPR) of users on the TRUSTS platform were discussed. It was found that data, which is not typically protected by patent or copyright laws, can be owned but enforcing legal claims for it can be difficult if it is taken without permission. There is a need for contracts that regulate the use of the TRUSTS platform and provide legal certainty. Two draft contracts were presented: a "Code of Conduct for using the

TRUSTS Platform" (CC) and "Terms and Conditions for using TRUSTS Services" (TC). The CC serves as general guidelines for user behaviour on the platform and does not contain any enforceable provisions. The TC, on the other hand, governs the conditions under which transactions between users take place, defining the rights and obligations of data providers and data consumers, as well as the legal position of the TRUSTS OpCo. It is acknowledged that the drafts presented will require revision and enhancement as the TRUSTS OpCo is established.

The draft "Code of Conduct for using the TRUSTS Platform" (CC) serves as a framework for amicable cooperation on the TRUSTS data exchange platform. The code aims to establish and promote efficient and targeted data exchange within the framework of the trading platform, with the goal of improving and optimizing the use of data, and achieving positive outcomes for employment and growth, as well as sustainable social stability and prosperity. The code sets out general principles and rules of conduct for participants, including compliance with legal provisions, particularly the General Data Protection Regulation (GDPR) and transparency regarding the origin and traceability of data collection. Participants are expected to act in accordance with principles of integrity, fairness, and partnership, and to communicate with each other in a respectful manner. The code also recognizes that data is sensitive and emphasizes the importance of preserving informational self-determination and protecting privacy. The code is intended to be a living document and will be supplemented and expanded in the future to include sanctions and penalties if relevant findings are obtained through the operation of TRUSTS.

Key Findings of Chapter 7.3 - Draft "Terms and Conditions for using TRUSTS Services" (TC)

During the project, a draft of the "Terms and Conditions for using TRUSTS Services" (TC) was developed as a proposal for what the terms and conditions could look like when the TRUSTS OpCo is operational. The draft TC is intended to provide a legal framework for the platform, but it is acknowledged that certain decisions regarding the organization and structure of the platform may need to be changed or adapted at a later stage. The draft TC is formulated in such a way that it can apply to different legal forms of the operating company. The TC defines key terms such as "TRUSTS Platform", "Data", "Data Assets" and "Participant". It also explains the process of "Listing," which is a requirement for all participants to go through before they can offer or request data on the platform. The TC also outlines the different functional roles on the platform, including Data Provider, Data Demander, and Operator. It states that the TC governs the rights and obligations of all participants in relation to TRUSTS OpCo.

1.4.7 Summary of Chapter 8 - Conclusions and Recommendations

The TRUSTS project successfully conceptualized supporting mechanisms for IPR protection of the future TRUSTS operating company (OpCo). It was covering the technical, legal, and administrative aspects of the challenges of the future TRUSTS OpCo. The main objective was to ensure a secure and legally compliant exchange of data sets and services. To achieve this goal, the project proposes a set of measures to deter and prevent IPR violations, such as performing due diligence on providers, analysing customer/end-users' reviews on TRUSTS product to identify issues, and implementing a reputation scheme for the users. Additionally, the project proposed the use of predefined contracts to facilitate business and the compliance with international, European, and national data protection laws and regulations relevant to data sharing. The TRUSTS platform will provide an easy and friendly user experience, leveraging productivity and decreasing operational costs. The proposed mechanism will ensure the validity of the data sets and services onboarding process and will act as a key enabler for the buyers to annotate and provide feedback about the quality of the data sets and services that they have bought.

2 Concept of Mechanisms for Protecting IPR

2.1 TRUSTS Overall Approach to IPR Protection

Is IP Protection of Data Assets Possible?

Intellectual property rights management plays a crucial role in any business strategy. Understanding how to effectively manage IP can help to promote a business or product and maximize its potential impact. IP can take many forms, such as a specific manufacturing process, plans for a product launch, trade secrets like a chemical formula, or a list of countries in which patents are registered. The concept of protecting IPR has been discussed for over 200 years, but it is only through modern legal systems that effective mechanisms for protecting "intellectual property rights" have been established.

Most intellectual property rights pertain to objects, works of authorship, or trademarks, which are either tangible or the result of a particular form of intellectual creation. For example, a novel or architectural design is protected by copyright due to the creative process and effort put in by the author. This form of IPR protection is well-established, and publishers worldwide rely on it as the foundation of their business. Other forms of protection include the registration of trademarks or word marks for specific jurisdictions with a limited term, or industrial design protection. Patents are another major field of IPR protection, and they are also well-established through national and international agreements.

However, authors' copyrights are automatically in place, and active steps must be taken to protect technical data assets like sensor or machine data. Conversely, industrial data assets are not protected by default, as they are not the result of an artistic or creative process like an author's work, nor can they be protected like a trademark or patented. In principle, traditional IPR protection mechanisms cannot protect them. (Raw) data and data exchange is not yet covered by any traditional IP protection mechanism.

In essence, appropriate options for protecting intellectual property in a data platform like TRUSTS are using a data-protection mechanism that ensures that data is safe and secure:

1. Protection through (user) contracts
2. Protection through contract-based access mechanisms to data
3. Protection through technical security systems for transmission, storage, and access
4. Protection through monitoring of user behaviour and corresponding alarm mechanisms
5. Protection through encryption and / or watermarking of data, and
6. Protection by the nature of the data (e.g., loss of value in the case of obsolete data)

Intellectual property rights are legal mechanisms that protect the rights of creators and owners of creative works. These rights are intended to encourage innovation and creativity by providing exclusive rights to creators and owners to control the use and distribution of their works. However, traditional IP law is ill-suited to protecting the data assets exchanged on the TRUSTS platform, in particularly sensor and / or industrial data assets. One of the main reasons for this is that data assets are often not a tangible asset that can be protected by traditional IP law. (Industrial) data assets are often generated by machines or sensors and have no protection by copyright or patent law. And they are often shared through complex networks of actors (like Gaia-X Data spaces), making it difficult to apply traditional IP law to protect the rights of data creators and owners.

Considering these challenges, the TRUSTS framework has been developed to provide a set of IPR-related tools and governance strategies that are better suited to protecting the data assets exchanged at the TRUSTS platform. These tools and strategies are intended to address the unique challenges of data asset sharing and use by providing a set of mechanisms that can be used to protect the rights of data asset creators and owners while also promoting the sharing and use of data assets among multiple parties. The IPR protection pillars in section 2.2 of the TRUSTS framework are designed to provide a comprehensive approach to protecting the rights of data asset creators and owners. These pillars include legal and regulatory frameworks, technical solutions, and governance strategies that can be used to protect the rights of data asset creators and owners while also promoting the sharing and use of data assets among multiple parties.

The TRUSTS framework is not meant to protect just the data assets shared via the platform, but it's also intended to cover certain assets that are indeed covered by IPRs. The IPR protection pillars in section 2.2 of the TRUSTS framework provide a comprehensive approach to protect the rights of data assets of creators and owners, which is suitable for the challenges of data assets sharing and use.

The following table shows the expected protective effect (+ low, +++ very high) and the assumed complexity of implementation (- easy, -- some effort, --- complex):

Table 2: Possibilities of IPR protection and expected protective effects

#	Protection by	Explanation	Protective Effect	Complexity of implem.
1	(Usage) contracts	Protecting IPR by entering user contracts with the users of the TRUSTS platform (Terms and Conditions and Code of Conduct – see chapters below). IPR issues are integrated into these at the contractual level and sanctioned (contractual penalty in the event of abuse).	++	-
2	Contract-based access mechanisms to data	Linking access to data sets by means of automated contracts (smart contracts) between the parties involved with definition of the type and manner of permitted use - and linking the release of data to the fulfilment of the contract. TRUSTS manages and monitors compliance with the contract and only allows data transfer if all factors of the contract are met.	+++	---
3	Technical security systems for transmission and storage	WP3 and WP4 deal with technical measures to secure transmission, storage and access.	+++	---
4	Protection through monitoring of usage behaviour and corresponding alarm mechanisms	The IDSA components Data-Broker and Data-Clearinghouse are monitoring the data connections / data flow and therefore the user behaviour and can trigger appropriate alarms.	+++	--
5	Protection through encryption and / or watermarking of data	Another protection option is to encrypt the data itself and/or insert watermarks in addition to encrypting the data transmission.	++	---
6	Protection through the nature of the data (e.g., loss of value in the case of outdated data)	If the value of the data is directly related to the data being fresh and up to date, the best protection of IPR is to deny access to the data in case of fraudulent intent to use it. Monitoring and smart contracts are good tools for this.	+++	-

2.2 The four IPR Protection Pillars

The evolving needs and considerations for IPR protection and economic security require a multifaceted enforcement approach. The main pillars that can mitigate IPR infringement are (Rosenbaum, Reilly, & Widmer, 2017):

1. Data and analytics
2. Supply chain integrity
3. Coordination and integration
4. Transparency and awareness.

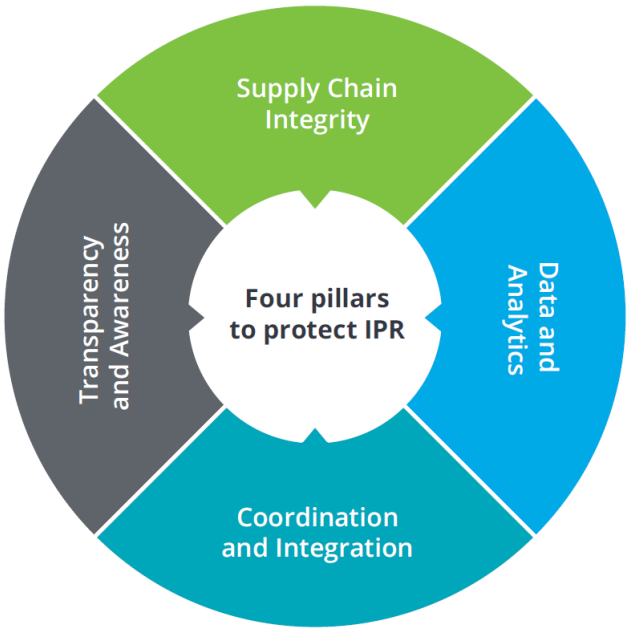

Figure 2: IPR protection pillars (Rosenbaum et al., 2017)

2.2.1 Focus of Protection: Data and Analytics

The use of data and analytics tools to identify IPR breaches can benefit both public and private enterprises (Rosenbaum et al., 2017). One example of an analytic tool is Enterprise Knowledge Graph (EKG). In principle, Ivanov (2018) describes EKG as "a representation of an organization's knowledge domain and artifacts that is understood by both humans and machines." It consists of references to an organization's data to describe "people, place, and things" and their relationships. For instance, Google will return not only traditional search results when people search for "Leonardo da Vinci," but also provides an info-box with information about an individual's relationship with other well-known figures (e.g., Vincent van Gogh, Raffaello Sanzio). "EKGs consists of a semantic network of concepts, properties, instances and relationships representing and referencing foundational and domain knowledge within or across different enterprises" (IAIS, n.d.). EKG employs a representation of formalisms such as Resource Description Framework (RDF, RDF-Schema) or Web Ontology Language (OWL) to holistically describe corporate information across many domains (see IAIS, n.d.).

EKG can identify potentially suspicious behaviour in a network of an organization (Rosenbaum et al., 2017). Nevertheless, Section 2.1.1 states that "the usual IPR protection mechanisms cannot protect data. Therefore, new approaches to data and analytics tools, especially for data protection in the data sharing context, are essential. One crucial element to consider related to data protection is the enablement of *data sovereignty.* Hummel, Braun, Tretter, and Dabrock (2021) conduct a review and summarize that data sovereignty heavily relates to the concept of *control over data.* Taking the perspective of data providers, Abbas (2021) summarizes that control over data refers to the autonomy to decide on rights to access and usage of the shared data. Data providers should also have the ability to track down data usage (i.e., to see if it conforms with pre-

determined data sharing agreements or not). Data providers need to know who reuses their data (and for what reason) to avoid competitors benefiting from the shared data in unanticipated ways.

A potential solution to enable data sovereignty in the data sharing context is by implementing the International Data Space (IDS) components. In the D2.1 report entitled *"Definition and analysis of the EU and worldwide data market trends and industrial needs for growth,"* the detailed elaboration related to these IDS components can be found. In summary, the core component of IDS, referred to as IDS connector, enables data sovereignty by acting as a security gateway where the "data provider always maintains control over the data and sets the conditions for its use." TRUSTS makes use of the IDS connector to ensure data sovereignty and to contribute to data protection endeavours. TRUSTS also explicitly mentions that control over data is one of its potential unique selling propositions (refer to the D7.1 report *"Sustainable Business Model for TRUSTS Data Marketplace I"*).

2.2.2 Focus of Protection: Supply Chain Integrity

Supply chain integrity can help organizations reduce IPR-related risks (Rosenbaum et al., 2017). Supply chain integrity can be achieved by fulfilling three strategic requirements. These are:

1. Trading partner authentication,
2. Complete supply chain visibility, and
3. Integrity tracking & risk identification.

The first requirement is related to the mechanism to ensure that only trusted and verified actors can involve in data sharing activities. TRUSTS has considered this requirement by (in the latter stage) defining required onboarding mechanisms (including certification processes). The second requirement is related to the third one. The idea is to know and track the activities in the supply chain processes. For instance, by implementing the blockchain, actors need to (automatically) input their supply chain task into a distributed ledger environment where all permissioned partners can access the relevant data. This allows for a "single version of the truth", as well as tracking and validating the authenticity and legality of performed tasks (Rosenbaum et al., 2017). Concerning TRUSTS, the use of *smart contracts* will contribute to fulfilling the second and third requirements. TRUSTS will ensure the supply chain visibility and provenance in data exchange processes.

2.2.3 Focus of Protection: Coordination and Integration

Coordination and integration between actors involved in data sharing activities are required to enforce IPR protection (Rosenbaum et al., 2017). One way to orchestrate actors in an ecosystem is by considering the implementation of *data governance*. Khatri and Brown (2010) define data governance as steering in terms of who gets to make the decisions and who is held accountable for making decisions about data and information. The data governance framework of Khatri and Brown (2010) includes five related decision domains, namely data principles, data quality, metadata, access to data, and the data life cycle.

Specifically, in the context of data sharing, Abbas (2021) summarizes that data governance comprises "the activities of exercising control (i.e., defining what, who, and how) over data ownership, access, and data usage decisions to minimize the risks associated with data sharing" (p. 697). Some data governance instruments that are beneficial to data sharing are "regulatory instruments, licenses, formal contract-based agreements, technical measures for data integration and usage policies, data sharing agreements" (Lis & Otto, 2020). Data governance should consider the digital platform characteristics, for example, internal and external contingencies, to decide data governance design (Lee, Zhu, & Jeffery, 2018).

More detailed elaboration related to data governance and its relevance for TRUSTS can be found in section 3.3 - TRUSTS platform support on Data Governance and Data Stewardship for users. The focus will be on the elaboration of data stewardship, especially for onboarding mechanisms for data providers.

2.2.4 Focus of Protection: Transparency and Awareness

The awareness of involved actors related to the IPR endeavours in data sharing activities can be increased by exchanging knowledge, best practices, and education of end-users. These processes can help to safeguard IPR (Rosenbaum et al., 2017). This focus on protection will also benefit from data governance practices, as briefly discussed in the previous section. For instance, Wiseman, Sanderson, Zhang, and Jakku (2019) conduct an empirical investigation in agricultural data sharing. They reveal that transparent data governance helps to build trust in data sharing. Data governance practices (i.e., via data anonymization) strengthen privacy protection (Potiguara Carvalho, Potiguara Carvalho, Dias Canedo, & Potiguara Carvalho, 2020). Appointing a data steward from a trusted partner seems to be a critical factor in reducing the uncertainty in data sharing (Nokkala, Salmela, & Toivonen, 2019). Therefore, data governance via data stewardship and onboarding mechanisms may help to increase transparency and awareness.

2.3 Current State: Issues & Solutions for IPR Protection

Intellectual property rights (IPRs) refer to legal protections for creative or innovative works, such as patents, trademarks, and copyrights. These protections are typically granted to individuals or organizations that create or develop new products, services, or technologies. In the context of TRUSTS, IPR-related tools and governance strategies may be used to protect certain assets that are covered by IPRs, such as technology developed during the project, or research deliverables that are copyrightable.

However, it is important to note that IPRs may not be the most suitable means of protecting data shared via the TRUSTS platform. This is because data, particularly sensitive or confidential data, may require a different type of protection, such as data security measures, rather than legal protections. The complexities of sharing and managing data assets from industrial sources and / or data assets within an open data ecosystem can make it difficult to apply traditional IPR. Instead, TRUSTS may need to develop a framework for protecting data assets that considers the unique characteristics and challenges of data assets sharing in a consortium environment. This framework may include governance strategies, such as data governance policies and procedures, as well as technical measures, such as encryption and firewalls, to protect data from unauthorized access, use, or disclosure. IPR may be relevant for certain assets within TRUSTS, but it is not the primary focus of the project. TRUSTS aims to develop a comprehensive framework that addresses the unique challenges of data sharing in a consortium environment, which includes data governance, data quality, and data security.

Like any other asset, IP needs to be managed and used strategically to ensure smooth cooperation and maximise the impact of project results. Hence, IP management plays an essential part in the entire lifecycle of research and innovation projects funded under the European Commission's Horizon 20201, as TRUSTS.

A printed book can be accessed by one or perhaps two people at once, people who must, of course, be in the same place as the book. But make that same text available in electronic form, and there is almost no technological limit to the number of people who can access it simultaneously, from literally anywhere on the planet where there is an Internet connection. At first glance, this is wonderful news for the consumer and for society. The electronic holdings of libraries (and friends) around the world can become available from a home computer, 24 hours a day, year-round, and never "checked out". These same advances in technology create new opportunities and markets for publishers.

The technological revolution, the data economy and society, the turn to artificial intelligence (AI), the growing importance of new technologies such as blockchain, 3D printing and the Internet of Things (IoT) as well as the development of new business models such as the platform economy, and the data and circular economy, offers a unique window of opportunity to modernise the approach to protecting intangible assets. But represent also a threat due to the higher likelihood and potential for unauthorised access and distribution – due

[1]https://intellectual-property-helpdesk.ec.europa.eu/horizon-ip-scan_en

to its broad accessibility and general connectedness. In recent decades, there has been significant progress in creating a single market for IP, yielding many benefits for the EU economy[2].

IPR play an important role in promoting innovation and protecting investment, in the digital and green economy. Without the protection of ideas, businesses and individuals would not reap the full benefits of their inventions or creations and would focus less on research and development. The 2004 Directive on the enforcement of IPR (IPRED) has proven a relevant tool in fighting IPR abuse[3].

Protecting IP has several benefits[4]:

1. to protect an invention, such as a new product. The owner becomes the only person with the right to use or reproduce it. Others cannot copy or reproduce what this invention is ensuring without the owner's permission.
2. the quality of the product is guaranteed, and its origin is clear. This can be an advantage for businesses because customers may prefer to buy a product that has passed more restrictive checks.
3. not only through direct use of IP, but also indirectly through licensing contracts IP protection can generate higher revenues. This occurs when the owner grants a licence to another company to use the IP protected subject matter for a certain period.
4. Owning a patent or a trademark can increase the business market value and make it easier to find investors or other funding opportunities (Links back to the EU regulatory initiatives in the data realm).

[2] Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience

[3] https://ec.europa.eu/commission/presscorner/detail/en/IP_17_4942

[4] Intellectual property rights

3 TRUSTS Support on Data Governance and Data Stewardship for Users

3.1 Introduction: Data Governance and Data Stewardship for TRUSTS Users

Data governance and data stewardship are essential elements to contribute to data sharing via data marketplace commercialization. Nevertheless, this type of non-technical study is often overlooked in the existing literature (Abbas, Agahari, Van de Ven, Zuiderwijk, & de Reuver, 2021). Therefore, this report aims to elaborate on these elements and to contribute not only to practical relevance but also to existing literature.

Earlier, data governance in the data sharing context is specifically defined as "the activities of exercising control (i.e., defining what, who, and how) over data ownership, access, and data usage decisions to minimize the risks associated with data sharing." Data governance in data sharing mainly focuses on data ownership, access, and usage. Data governance has become very important because of the requirements to monitor data sharing, and data use conditions (Jaiman & Urovi, 2020). It needs to balance sharing and exclusivity because unclear data ownership and data usage cause data misused or privacy harm and eventually lead to market failure (Lee, Zhu, & Jeffery, 2019; Martens, De Streel, Graef, Tombal, & Duch-Brown, 2020). Wiseman, Sanderson, Zhang, and Jakku (2019) conduct an empirical investigation in agricultural data sharing. They reveal that transparent data governance helps to build trust in data sharing. Data governance practices (i.e., via data anonymization) strengthen privacy protection (Potiguara Carvalho, Potiguara Carvalho, Dias Canedo, & Potiguara Carvalho, 2020). Appointing a data steward from a trusted partner seems to be a critical factor in reducing the uncertainty in data sharing (Nokkala, Salmela, & Toivonen, 2019).

Based on De Prieëlle, De Reuver, and Rezaei (2020), Lee, Zhu, and Jeffery (2017), (Van Den Broek & Van Veenstra, 2015), data governance factors for data sharing can be summarised as follows (refer to Table 3).

Domain	Factor	Sub-factors
Data governance mode	Decision rights allocation for involved actors	- Identify the data governance mode (i.e., market, bazaar, hierarchy, or network) - Identify decision right elements - Identify involved actors
Governance of data ownership and access	Definition criteria identification for data ownership and access	- Consider relevant rules (e.g., policies, laws, standards) - Identify criteria for defining data ownership and access - Develop decision models for data ownership and access
	Data ownership and access allocation	- Define ownership of all data types in the platform (e.g., user, process, and system data) - Define access right
	Contribution estimation	- Consider actors' contribution - Identify contribution model dimensions - Combine contribution model with data ownership and access model
	Data use case	- Define data categories of platform data (e.g., user, process, and system data) - Define data use cases and link relevant actors

Domain	Factor	Sub-factors
		- Ensure data use cases is executed with consistency and integrity
Governance of data usage	Conformance	- Know conformance requirements related to data due processes - Define audit process to ensure the conformance for data due processes - Share audit results to stakeholder
	Monitoring	- Identify and inform all data usage activities - Enable all actors to monitor and report the use of data in platforms - Ensure visibility of data supply chain
	Data provenance	- Track all data history via metadata management - Enable data owner verification throughout the data lifecycle

Table 3: Data Governance Factors

The discussion is now focused on data stewardship as an essential aspect of data governance. Data stewardship encompasses the tactical management and oversight of the company's data assets[5]. It is generally a business function facilitating the collaboration between business and IT, driving the correction of data issues, and improving the overall data management process. Their interest is in content, context, quality, and business rules surrounding the data. Data stewardship is the management and oversight of an organization's data assets to help provide business users with high-quality data that is easily accessible in a consistent manner[6]. Benefits of data stewardship:

- improved data quality.
- better data documentation.
- clear, concise data policies and processes.
- more efficient and effective analytics programs.
- more frequent use of data to make decisions.
- improved compliance with data-related regulations.
- fewer errors in processes and decisions that are driven by data; and
- reduced risks around data-related security and privacy requirements.

To have effective data stewardship, it is necessary to have the three P's[7]:

1. policies,
2. processes, and
3. procedures.

Policies establish a set of goals and state 'this is what we need to do' at the enterprise level.

Processes which can be represented by a process flow diagram) state what is required to comply with the policies. A process specifies a high-level set of tasks, the flow of the tasks, and who is responsible for completing each task.

Procedures describe in detail how exactly to perform the tasks.

[5] Mark Allen, Dalton Cervo, in Multi-Domain Master Data Management, 2015

[6] Mary K. Pratt: https://searchdatamanagement.techtarget.com/definition/data-stewardship

[7] David Plotkin, Data Stewardship: An Actionable Guide to Effective Data Management and Data Governance

Data Stewardship as Measure to Protect IPR

In general terms, data stewardship focuses on "the accuracy, integrity, and preservation of information holdings" (Dawes, 1996, p. 393). In this TRUSTS deliverable, we define data stewardship in the context of business data. To quote from Wilkinson et al. (2016, no page): "Beyond proper collection, annotation, and archival, data stewardship includes the notion of 'long-term care' of valuable digital assets, with the goal that they should be discovered and re-used for downstream investigations, either alone, or in combination with newly generated data." Simply said, data stewardship concerns the careful and responsible management of data.

Aligned with the scope of the TRUSTS project, data stewardship does not merely concern technical aspects of data management, but also the non-technical side of it. This perspective is also adopted in various other domains. For example, in the e-government domain, Dawes (1996) states that data and information stewardship include assuring accuracy, validity, security, management, and preservation of information records. She writes that stewardship does not fix a single point of responsibility. Instead, all the different actors (e.g., companies as data providers and as data users, owners of data marketplaces, intermediaries, public agencies) involved are responsible for handling information with care and integrity, regardless of its original purpose or source. In addition, Dawes (1996) writes that stewardship demands that government information be acquired, used, and managed as a resource that has organizational, jurisdictional, or societal value across purposes and over time (Dawes, 1996). It thus promotes two essential requirements for information-based transparency: it protects information from damage, loss, or misuse; and it makes information "fit for use." Some scholars refer to data stewardship with terms such as 'data management and the FAIR data principles. In the following sub sections, we explain these different perspectives and, finally, we discuss the data stewardship perspective adopted within the TRUSTS project.

3.2 Data Management and the FAIR Data Principles

When talking about data stewardship, the literature also often refers to data management and the FAIR principles. The FAIR data principles stand for Findable, Accessible, Interoperable and Reusable data (Force11, 2016; Wilkinson et al., 2016). Wilkinson et al. (2016) state that the FAIR data principles can be used to clarify what comprises good data stewardship and management. Table 1 below contains an overview of the FAIR data principles as defined by the GO FAIR initiative (GO FAIR, no date). The principles pertain to three entity types: data (or any digital object), metadata (information about that digital object), and infrastructure.

FAIR element	Principles related to each element of FAIR
Findable	**F1**. (Meta)data are assigned a globally unique and persistent identifier **F2**. Data are described with rich metadata (defined by R1 below) **F3**. Metadata clearly and explicitly include the identifier of the data they describe **F4**. (Meta)data are registered or indexed in a searchable resource
Accessible	**A1**. (Meta)data are retrievable by their identifier using a standardised communications protocol **A1.1** The protocol is open, free, and universally implementable **A1.2** The protocol allows for an authentication and authorisation procedure, where necessary **A2**. Metadata are accessible, even when the data are no longer available

FAIR element	Principles related to each element of FAIR
Interoperable	**I1**. (Meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation. **I2**. (Meta)data use vocabularies that follow FAIR principles **I3**. (Meta)data include qualified references to other (meta)data
Reusable	**R1**. (Meta)data are richly described with a plurality of accurate and relevant attributes **R1.1**. (Meta)data are released with a clear and accessible data usage license **R1.2**. (Meta)data are associated with detailed provenance **R1.3**. (Meta)data meet domain-relevant community standards

Table 4: An overview of the FAIR data principles.

Anjaria (2020) developed four guidelines for applying the FAIR principles to data sharing platforms, resulting in so-called FAIR data stewardship platforms and models. Anjaria (2020) states that data Findability should be enhanced by assigning persistent HTTP URLs and DOIs of publications to datasets. For Accessibility, suitable dataset formats should be used to describe the metadata, including Extensible Markup Language (XML) and Resource Description Framework (RDF). To improve Interoperability, rich ontology, metadata, standards, and stringent standard interchanging guidelines and formats should be applied to the data. Finally, data Reusability should be ensured by enabling the download of datasets accompanied by rich metadata through the world wide web (Anjaria, 2020).

3.3 TRUSTS Data Stewardship Support Services for Data Providers

3.3.1 Introduction: Open and Commercial Datasets for Data Sharing

Companies nowadays have access to a large range and diversity of **open datasets**, including open government data, open research data, and data openly shared by other companies. Such open datasets are structured, machine-readable, actively published on the internet for public reuse, and ideally also Findable, Accessible, Interoperable and Reusable (FAIR) (Force11, 2016; Wilkinson et al., 2016) by any user, commercial and non-commercial.

Companies can use open datasets to their benefit (Gurin, 2014; Zuiderwijk, Janssen, van de Kaa, & Poulis, 2016). For example, the use of open data may increase companies' competitive advantage (Zuiderwijk, Janssen, Poulis, & Vandekaa, 2015), it may contribute to economic growth through the development of new products and services (Kitsios & Kamariotou, 2019; Magalhaes, Roseira, & Manley, 2014), and it might help entrepreneurs making more informed decisions about their business models (Kitsios & Kamariotou, 2019; Zeleti, Ojo, & Curry, 2016).

A first type of open data that may be beneficial to companies concerns *open government data*. Various business models based on open government data have been described in the literature (e.g., see Kaasenbrood, Zuiderwijk, Janssen, de Jong, & Bharosa, 2015; Magalhaes et al., 2014; Zeleti et al., 2016 for overviews). For example, building on open data business models developed by practitioners, Zeleti et al. (2016) identify five business models for the commercial use of open government data: *Freemium*, *Premium*, *Cost Saving*, *Indirect Benefit* and *Parts of Tools*. For each of these models, they describe the different value disciplines that drive the model, including *Usefulness*, *Process Improvement*, *Performance* and *Customer Loyalty. Magalhaes et al.*

(2014) provide a taxonomy consisting of three business model archetypes: enablers, facilitators, and integrators. Moreover, they present the value proposition of each business model archetype in relation to value creation in the open government data ecosystem.

A second type of open data useful for companies includes open research data. Research data include administrative data associated with research, as well as the data generated by research. As technology advances, more people can easily create, store, and transmit growing volumes of data and digital collections. It is imperative to have a structure in place to manage and protect data assets, ensuring reliable and timely access to accurate data, within a framework that provides built-in privacy and security safeguards and data-management and sharing capabilities that meet federal mandates. Previous research found that the commercialization of research findings can be a reason for researchers to not share their research data openly (Fecher, Friesike, & Hebing, 2015). Researchers may fear the commercial or competitive misuse of their data (Fecher et al., 2015), or losing opportunities for commercialization they had wished to exploit themselves (Kim & Adler, 2015). On the other hand, a lack of concerns about the commercial potential of data may increase researchers' willingness to openly share their data (Zuiderwijk & Spiers, 2019), and the expectation to generate wealth through the downstream commercialization of research outputs can motivate researchers to openly share their data (Arzberger et al., 2004). While the drivers and inhibitors for researchers to share their data towards companies have been investigated in the past, less is known about companies' drivers and inhibitors towards reusing open research data.

A third type of open data possibly useful for companies concerns data openly shared by other companies. Several companies have already started to share their data openly. For example, in 2012 and 2013, Nike launched various initiatives to stimulate entrepreneurs to create companies based on the exploitation of Nike's digital products (Clarke, 2013). Other examples include companies such as Google and Twitter, which make some of their data publicly available through Application Programming Interfaces (APIs). This data can be useful for other companies to improve or extend their services and products. The data may also be used as a justification to customers on certain decisions taken. For instance, the open business data may provide information concerning factory working conditions and allow for ethical scrutinization and inspection.

It is important to note that these different types of open data require different types of stewardship and governance. For example, while governments may be driven to share their data for transparency and accountability purposes, companies have a commercial interest and need to generate profit.

Another data category that can be shared is **commercial datasets.** Nevertheless, the existing literature has hardly discussed the types of commercial datasets that are shared in data marketplaces. A study that identifies the types of commercial datasets (but in the broader context of data sharing) is an examination conducted by Dahlberg and Nokkala (2019). Dahlberg and Nokkala (2019) identify the types of commercial datasets shared via digital platforms in the supply chain. The categories include "*planning material data; invoices and payments; project schedules; instructions guarantee; and bilateral information."* (p. 633). The research also identifies the types of data that contain *"competitive advantage; price data; internal sensitive data; and business sensitive drawings"* (p. 635) are categorized as non-shareable. More research is needed to define, for example, how to distinguish whether datasets contain information about competitive advantage or not.

3.3.2 Envisioned TRUSTS Support Services for Onboarding of Data Providers

TRUSTS will provide supporting services for onboarding data providers, particularly SMEs and in particular SMEs and semi-governmental agencies that do not have sufficient internal capabilities. These data providers generally do not "know what they know" or commercialise this data in a meaningful yet protected way that also has them retain control over their data integrity.

Translating from the previous elaboration to practice, the following data stewardship supports can be considered for future TRUSTS support services:

#	Topic	Aspects
1	Dissemination activities	Dissemination data sharing use cases and success stories, including how it benefits data providers
2	Internal decision rights allocation	Developing an internal organisation body that has the right to decided commercial data sharing activities
3	Technical preparation	Supporting required technical requirements for data sharing processes, for example, the installation of IDS components like IDS connector.
4	Dataset identification	Identifying datasets that can potentially be shared via data marketplaces.
		Assessing the compliance of to-be-shared datasets towards existing rules (e.g., policies, laws, and standards), including relevant techniques related to, e.g., data anonymisation
		Approximating the pricing of datasets
5	Dataset preparation and enhancement (see Section 3.3.5)	Preparing dataset by performing data cleansing
		Enhancing raw dataset by performing analytics
6	Contract development	Developing contracts by defining clear data ownership and access. In some cases, the contracts can also explicitly mention specific data use cases (i.e., use shared datasets for only specific purposes).
		Translating physical contracts into smart contracts
7	Metadata management	Creating metadata for datasets by considering the FAIR data principles
8	Dataset monitoring	Monitoring dataset by analysing access and usage of shared datasets
		Track all data history via metadata management
		Reporting and addressing suspected IPR infringement

Table 5: Data Stewardship Support

More generic data stewardship elements that are relevant for TRUSTS are:

- Responsibility and accountability: data marketplaces need to have a clear policy on which actors are responsible for what activities and actions.
- Data quality issues (e.g., accuracy, completeness, timeliness)
- Data preservation: it needs to be clear to the different actors involved in data marketplaces how the data is preserved, for how long, with which guarantees, and what risks are involved.
- Standardization: for both data providers and data users there should be a clear policy on what standards are used in the data marketplace and what procedures and templates data providers should follow to provide their data in a format that is aligned with these standards.
- Interoperability: the data marketplace should indicate a strong preference for data formats that enhance interoperability and support interoperable data and standards to the fullest.
- Data misinterpretation: data marketplaces need to report what principles they implement to reduce the risk of data misuse and damage (e.g., also reputation damage).

3.4 Requirements for Data Preparation and Data Integration

Data is an important asset, just like cash and other physical assets. Enabling successful DS is the key to an effective data governance program and ultimately to the effective use of institutional data assets.

As the name suggests, the data preparation process transforms raw data from multiple sources into a standardized format. This 'preparation' makes the data ready for use by business intelligence tools and is thus a prerequisite to analysis[8]. The true power of data lies in how it is captured, processed, and turned into true actionable insights. Data Preparation is a scientific process that extracts, cleanses, validates, transforms, and enriches data prior to analysis. Data preparation enables to discover, detain, distil, document, and deliver data, it empowers the entire enterprise to make the most of all its valuable data assets.

Data preparation also involves finding relevant data to include in analytics applications to ensure they deliver the information that analysts or business users are seeking. To support machine-learning (ML) algorithms that can recommend or even automate actions to augment and accelerate data preparation.

Typical distinct steps of data preparation are illustrated in Figure 3 below including[9]:

- **Data collection:** The first step to data preparation is identifying which data is important and gathering it all in one place. Relevant data is gathered from operational systems, data warehouses and other data sources.
- **Data discovery and profiling:** The next step is to explore the collected data, to better understand what it contains and what needs to be done to prepare it for the intended uses. Data profiling helps identify patterns, inconsistencies, anomalies, missing data, and other attributes and issues in data sets.
- **Data cleansing and validation** imply standardizing the gathered data. Data from different sources will have different formats focused on presenting specific information. The identified data errors are corrected to create complete and accurate data sets that are ready to be processed and analysed. Then to validate its consistency, completeness, and accuracy.
- **Data transformation and enrichment** pertains to altering the master data to fit the needs of analytics or intelligence tools. Enhances the data sets as needed to produce the desired business insights.

[8]SHARJEEL ASHRAFAPRIL 30, 2020 https://dataintegrationinfo.com/data-preparation-process/

[9] Data preparation definition, By Ed Burns, Executive EditorMary K. Pratt, last updated in July 2020

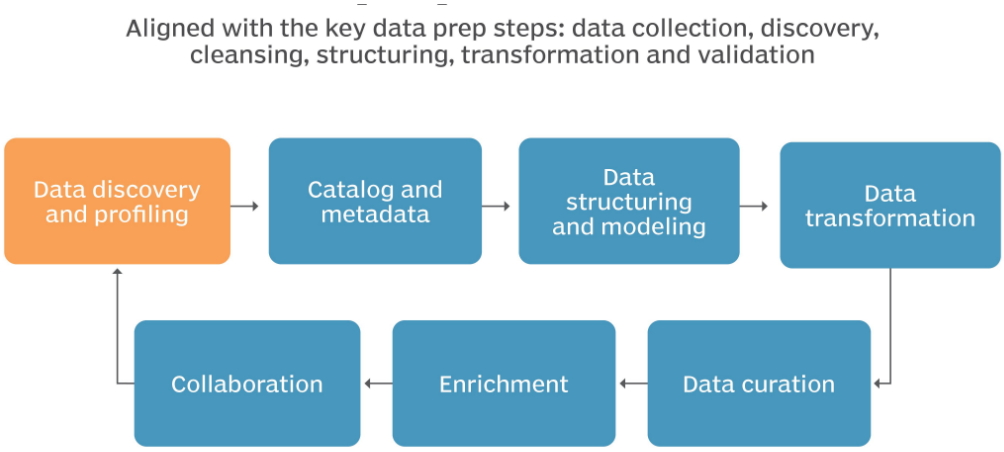

Figure 3: Data preparation capabilities and data preparation steps

Fostering data sharing requires a secure environment where TRUSTS can keep investing in data generation and collection, while sharing them in a secure way, confident that sensitive data will not be acquired, used, or disclosed unlawfully.

Data is at the core of AI and ML projects so is for TRUSTS. Even more so than application code, data is crucial in training, testing, validating, and supporting the ML algorithms at the heart of AI systems.

TRUSTS will respect the legal and ethical constraints imposed by the European values to which all partners will adhere and will abide by the data protection regulations as well as embrace their corporate social responsibility.

The TRUSTS project aims to provide a level playing field for setting up data value chains in industry. In such value chains different organisations need to cooperate in the various stages of the product life cycle using different data sources and data platforms. The TRUSTS European Data Market addresses the need to be able to quickly set-up digital support for such data value chains in an increasingly dynamic manufacturing ecosystem, while at the same time addressing key challenges, e.g., semantic interoperability, security in cross-domain setups, findability of data sources, entity linking, ensuring data quality and commercial confidentiality.

3.5 Requirements for Platform Connectivity

Online platforms play a prominent role in creating digital value that underpins current and future economic growth in the EU[10]. Online platforms have a massive impact on individual users and businesses, and are recasting the relationships between customers, advertisers, workers, and employers.

A platform that can connect to networked devices and provide a hosted infrastructure to cost-effectively and securely manage and route data. According to the Software Product Manager, Brad Cole[11] the Top 5 IoT Platform requirements you should consider are security, reliability, scalability, flexibility, and finally simplicity. Primarily, **security** is key. In addition to knowing the platform is secure at a technical level, you also want to know the team operating the platform follows industry-standard security controls. platform is **reliable**. The device connection mechanism must be rock-solid since there usually are not any humans at the other end to re-try if something goes wrong. The system must operate as if the devices were on another planet, and no one can get to them. The platform itself needs to be robust and offer the opportunity to add more devices. In other words, it needs to be scalable and have a device layer that handles connectivity to large numbers of devices and easily interacts with them.

[10] https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU(2021)656336_EN.pdf
[11] Top 5 Platform Requirements, Brad Cole, Sep 28, 2018

The expansion of registered devices should not require extensive infrastructure planning or lead-times. It should be simple and efficient. The subject of the user interface should be simple and intuitive. Even at massive scale, administrators should be able to change device configuration settings, transfer files, upgrade firmware, and automate processes so it all happens on a schedule, or as network issues arise.

TRUSTS creates value by facilitating exchanges/transactions and through fostering innovation. It provides a structure that can take advantage of digital technologies, low search costs to generate efficient matches between globally connected users, increase the efficiency of data exchange through lower search costs and low reproduction and verification costs.

In TRUSTS, an electronic survey was disseminated to all TRUSTS partners, who were asked to further disseminate it to an as-wide-as-possible audience to receive feedback analysis from different several stakeholders for a commercial financial and operators' industry vertical data marketplace platform.

An in-depth quantitative and qualitative analysis of the feedback to the questionnaire was achieved and is further elaborated within the first version of the "Industry specific requirements analysis, definition of the vertical E2E data marketplace functionality and use cases definition" report "D2.2"[12] of TRUSTS.

Regarding the desired process for providing services, participants highlighted the following requirements:

- The process should be electronic.
- The process should be confidential, according to GDPR policies.
- Open data should be supported.
- Providing services directly to end-customers should be supported.
- The platform should support subscription, featuring annual license subscription as well.
- A connection of the platform with highly visiting applications marketplaces, such as Google Play and Apple Store, should be provided26.
- Retrieving datasets should be easy.
- Keyword based searching of datasets should be supported.
- Alternatively, to keyword searching for a dataset, browsing through structured content categories should be supported.
- Each dataset should include description and tags.
- Ratings and comments from other users who have already used the dataset should also be provided.
- Information about the anonymization of the dataset is important.
- Viewing a small sample of the dataset before buying it would also be useful.
- A discrete distinction between free and paid datasets should be provided.
- Networking between partners should be supported.

Following, participants were asked to identify in their opinion the standardization gaps and the way forward to boost the data marketplace endeavour, and to describe the required standardization for federated data marketplaces. The gaps and problems identified were as follows:

- There are currently too many marketplaces and no overview.
- A standard meta-model for data exchange is missing, containing for instance standard vocabulary (e.g., Asset Administration Schell).
- Usage Control and legal framework (e.g., contracts) for data exchange is missing.

The requirements that were identified in this respect included:

- Strong authentication mechanisms to create trust.
- Intelligent matchmaking mechanisms, facilitating users to identify the data or services needed.
- Advanced searching options, including filters for the cost of a dataset or application / service.

[12] D2.2 Industry specific requirements analysis, definition of the vertical E2E data marketplace functionality and use cases definition I

4 Navigating the Intersection of IPR and Cybersecurity in Data Exchange Platforms: IPR Threat Modelling for TRUSTS

4.1 Threat Modelling for Data Exchange Portals

Threat modelling in data portals is a crucial aspect of ensuring the security and integrity of digital information. This chapter describes the procedure for developing a TRUSTS threat model. On a platform like TRUSTS there are data assets offered and exchanged. Data assets are generally outside the scope of legal IP protection – unless they are covered by specific laws like copyright or patents – and therefore protecting the offering, exchanging and transmission of data assets is crucial. The technical aspects are covered in the technical working packages 3 and 4 and partly in this report in this chapter 4 and in chapter 5. The TRUSTS IPR Threat Model is a framework used to systematically survey threats. Because IPR and technical threats cannot be treated separately, both threats, IPR-related and technical, are always listed here.

As the use of data portals continues to grow, it becomes increasingly important for organizations to understand the potential risks and take measures to mitigate them. A threat modelling process is a systematic approach to identifying and evaluating the potential threats to a system or process. The following chapter describes an approach of a TRUSTS Threat Modelling. This process begins with identifying the goals and objectives of the system or process, and then identifying potential threat sources. Once potential threats have been identified, they are evaluated based on their likelihood and potential impact. This allows organizations to prioritize their efforts and focus on the most significant risks.

One of the key aspects of threat modelling in data portals is identifying potential vulnerabilities in the system. These vulnerabilities can include weaknesses in the software or hardware, as well as vulnerabilities in the processes and procedures used to manage and access the data. For example, a data portal that allows users to upload and download files without proper authentication or encryption could be vulnerable to unauthorized access or data breaches. To protect information against these vulnerabilities, it is necessary to implement various security measures such as encryption, multi-factor authentication, and access controls. Encryption can help protect data in transit and at rest, while multi-factor authentication can help prevent unauthorized access to the portal. Access controls can be used to restrict access to certain data or features based on user roles or other criteria. Another important aspect of threat modelling in data portals is identifying and mitigating the potential impact of a security incident. This can include creating incident response plans, testing them regularly and having an incident management team. This can help ensure that the organization is prepared to respond quickly and effectively in the event of a security incident.

The TRUSTS approach does include all the above-mentioned aspects of IPR protection by design and processes. The objective of this chapter is to identify and assess potential threats.

4.1.1 Introduction and Description

The basic idea behind a portal like TRUSTS is that it serves as an "entry point" to a plethora of different information. Portals typically bundle various information channels, search and filter functions, and personalization to provide users with an environment where all relevant information can be easily accessed and collected. This environment is tailored to the preferences and tasks of each individual user. Within the main window, there are usually smaller, virtual windows - also known as "portlets" - that separate the different types of information and applications. These portlets can be configured, minimized, or closed altogether. These features, when examined critically, are not new and have been present in graphical and window-oriented operating systems for years. Due to the platform-independence of the underlying web infrastructure, portals offer users the ability to access their desired information from any location, if they have access to their familiar working environment. From a technical standpoint, a portal is not an isolated system, but rather a collection of existing applications or information services that have been bundled together to achieve the aforementioned goals. As such, its structure is not monolithic, but rather consists of different functional blocks, some of which may be implemented by different systems. (Rütschlin, 2001).

The TRUSTS platform is a system that facilitates the exchange of data between various organizations, individuals, or systems. It typically enables users to securely upload, download, and share data in a controlled manner. TRUSTS can be utilized for a range of purposes, such as exchanging information between government agencies, sharing data with research partners, or enabling data-sharing between businesses. Additionally, it should ensure easy access to information through a simple search function and present all information using a consistent user interface. All information and applications should be accessible through a unified window, or a homogenized user interface (Rütschlin, 2001).

Data exchange portals typically have a few features to support the exchange of data, including:

- **Security measures**: Data exchange portals have security measures in place to protect the selected data, including encryption, authentication, and access controls
- **Data management**: The ability to support a variety of data formats, including text, spreadsheets, and database formats
- **Integration with other systems**: Data exchange portals can be connected to or integrated with other systems; for example, other data markets or third-party data systems, so that data can be easily exchanged between these different systems
- **Collaboration tools**: As tools for collaboration with other users, data exchange portals include, for example, the option to leave comments or also to leave feedback, in addition to the option of pure data exchange.

4.1.2 The Peculiarity of Data

The uniqueness data exchange portals lie not only in the technology itself, but also in the nature of the data that are exchanged. These can be easily replicated and used simultaneously. (Koutroumpis et al., 2013). Additionally, data only holds value or relevance when it is used in its specific context or combined with other data. The traceability of data lineage is particularly challenging, as it is nearly impossible to trace the exact path of the data once it has been extracted from a dataset or database, combined with other data, or supplemented. This is further compounded by reluctance to share data, where individuals or institutions are unwilling to share or provide data because of concerns regarding trustworthiness or because of missing economic incentive to do so or because of unclear situation of origin or usage rights. The true value of data is only revealed when it is shared (Koutroumpis et al., 2013).

To ensure the proper handling of data, it must be accompanied by information about its origin, to demonstrate credibility, quality, and security, which is usually provided by metadata. As such, the best data exchange portals have functions to store this metadata (Spiekermann et al., 2018).

To address some of the challenges in handling data, certain requirements must be met by the portals (Koutroumpis et al. 2017):

1. Establishing boundary conditions that allow only legitimate users to participate in all data transactions
2. Establishing criteria for data usage
3. Monitoring mechanisms to track abnormal activities

4.1.3 Types and Stakeholders of Data Exchange Portals

Data Exchange Portal - Type

Data exchange portals like TRUSTS were initially seen as a straightforward solution for ensuring the uploading, updating, and continuous access to data by various people and institutions. A description of this can be found in the following statement: "platforms that connect providers and consumers of data sets and data streams, ensuring high quality, consistency and security. The data suppliers authorize the marketplace to license their information on their behalf following defined terms and conditions" (Smith et al., 2016).

These services, known as data marketplaces, create value for their customers in several ways, like other digital marketplace platforms (Smith et al., 2016). Firstly, the search process for data is simplified, as users do not have to search the offerings of individual data providers on their websites. Secondly, access to a wide

range of data content is provided, allowing for informed decisions. Thirdly, the trading process is made more convenient through automated data exchange with standardized data formats. Finally, there is a greater scope for building relationships through better alignment between data supply and demand. For example, many open exchange portals can be found, in contrast to a small number of commercial portals.

As a crucial part of modern business, data exchange portals are mainly used to facilitate the flow of information between different systems and organizations. To enable efficient exchange, it is important to understand the differences between the various types of portals. These include Electronic Data Interchange (EDI), File Transfer Protocol (FTP), cloud data exchange, web service portals, or simply "marketplaces".

- **Electronic Data Interchange**: These portals are mainly used for connection and exchange, especially in the B2B area for invoices or orders; this format facilitates the easy transfer of the necessary data, from one system to another
- **File Transfer Protocol**: These allow the exchange of larger amounts of data; for example, images or videos between computers using the Internet or other networks
- **Cloud data exchange portals**: These are used to exchange data between different cloud-based systems. For example, they synchronize data between systems or transfer data from one to another
- **Web service portals**: Data is exchanged between systems using APIs (Application Programming Interfaces). Different systems communicate via a standardized and defined path in real time, or transmit data volumes
- **Data exchange portal**: These portals offer data for exchange or purchase, or simply enable companies as well as individual persons to store it permanently.

Considering literary sources, Smith (2018) points to three categories, which also span those mentioned above:

- **Personal Data Marketplaces**: these allow individuals to disseminate, sell or acquire data via a platform; examples include social media, streams, which draw on the above types, among others
- **Sensor Data Marketplaces**: Examples include data collection on weather or pollution levels to provide users with the information they need in real time
- **Business Data Marketplaces**: These marketplaces allow for the classic business-to-business data exchanges.

Data Exchange Portal – Stakeholders (Collector, Manager, Aggregator)

In general, data exchange portals like TRUSTS are multilateral hubs and multi-sided platforms that connect data sellers and buyers and facilitate data exchange. These portals only orchestrate data exchange through services such as search/discovery, transaction validation, transaction history, and payment gateway. Functionally, multilateral data marketplaces enable the linking of disparate data sets from different data owners through easy search and discovery, standardization of their formats, and their subsequent aggregation into meaningful data products (Koutroumpis et al., 2017). This requires a regulatory environment, communication standards, data protocols, and procedures for data import, storage, transformation, aggregation, analysis, and delivery functions. Data exchange platforms can range from simple information systems to complex organizations. In their simplest form, they are constructs in which individuals provide data and others consume them (Koutroumpis et al., 2017).

Data provision: On the data exchange platform, the information and data are compiled and offered. This process can be further divided into different steps corresponding to specific roles, such as the data collector, the data manager, and the data aggregator. A Data Collector collects the data and makes it available. The data manager then takes care of cleaning, cataloguing, and providing the data in an interpretable form. The data aggregator compiles the data provided from a wide variety of sources (Leiponen et al., 2016).

Data consumption: The data can ultimately be obtained via the data exchange portal for search and actual use, also known as consumption. Depending on the data or the portal, financial compensation may be required (Leiponen et al., 2016).

4.1.4 Components of a Data Exchange Portal

The structure of TRUSTS data exchange structure is therefore not monolithic, but can be seen, as shown in the figure below, as a collection of different functional blocks, some of which are implemented by different systems. The blocks shown in light gray in the figure above represent existing systems (e.g., in a company) that are to be merged by means of the portal-specific functions shown in dark grey. The existing systems can be roughly divided into three categories (with regard to their integration into a portal):

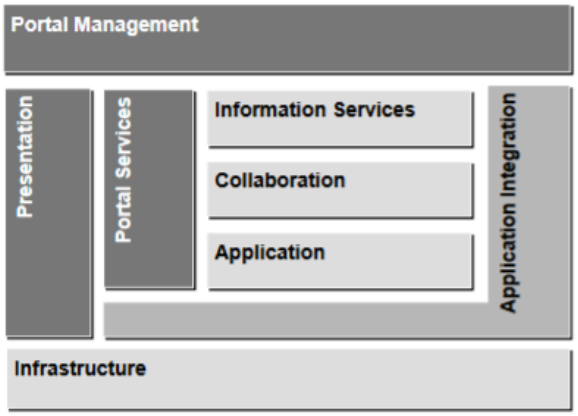

Figure 4: Components of a data exchange portal (Rütschlin, 2001)

- **Information Services**: Classic information such as news, documentation, business information services (such as weather, stocks, etc.), web content, information generally managed by a content management system, and the like
- **Collaboration**: E-mail, calendars, groupware in general, but also workflow systems
- **Application**: Conventional applications (some of which are already web-enabled) that have either been developed in-house or purchased
- More or less orthogonal to the former are the **integration architectures**, with which previously isolated individual systems are made interoperable or simply suitable for use in the Internet/Intranet. The block occupies a certain special position in the diagram. The whole architecture runs on a certain infrastructure. This includes (besides the operating system and hardware) systems such as application servers, web servers, directory and transaction services, but also certain security services; essentially, all the structural services that originate from the Web environment or are connected to it can be connected to it via adapters/connectors.
- The TRUSTS platform also includes a **management part**, which handles tasks such as (global) user administration and monitoring
- A further block takes over the device-dependent **presentation** of the contents and applications to the user and the typical portal functions such as personalization, search, content management and navigation are combined under the portal services.

In summary, a portal like TRUSTS can be seen as an access point for a user, in which all the information and applications relevant to him or her are offered (regardless of their location). From a technical point of view, it appears as a presentation layer of various sources, whereby the actual task is an all-encompassing integration of information and applications. The portal itself only plays a role in this process through provided and already existing components (Rütschlin, 2001). Another threat is the fact, that the access to portals is possible from almost any location is not always compatible with a high level of confidentiality (Rütschlin, 2001).

4.2 Process of Threat Analysis

4.2.1 Phases of the Threat Analysis

Considering Bodeau et al. (2018), threat modelling can be defined as a process for identifying, analysing, and assessing potential threats to an organization or system. This process involves several different phases and steps. It is about developing and applying a possible representation of threats: from within or from outside, through technical or data-related failure. Generally, the process can be carried out in different ways, depending on the context. By identifying and rating threats based on a comprehensive understanding of the architecture and implementation of the relevant application, organisations can address threats with appropriate countermeasures in a logical order, starting with the most significant risks (Meier et al., 2003). As threat analysis helps organizations identify and prioritize potential risks, it is an important part of risk management. To stay prepared and proactive in addressing potential threats, several steps (involved in the process) are necessary:

1. **Identify security objectives**: This step involves the identification of the valuable assets that the systems must protect.
2. **Assess the possible impact on the applications**: In this step, the organization evaluates the likelihood that there will be an effect on those objectives; a documentation of the application, including subsystems, boundaries or the data flow will be created.
3. **Decompose the applications**: In this step, the organisation decomposes the architecture of its application, including the underlying network and host infrastructure design, to create a security profile for the application. The aim of the security profile is to uncover vulnerabilities in the design, implementation, or deployment configuration of the application.
4. **Identify threats**: Keeping the goals of an attacker in mind, and with knowledge of the architecture and potential vulnerabilities of the application, the organisation identifies the threats that could affect the application.
5. **Document the threats**: The organisation documents each threat using a common threat template that defines a core set of attributes to capture for each threat
6. **Rate the threats**: The organisation rates the threats to prioritize and address the most significant threats first. These threats present the biggest risk. The rating process weighs the probability of the threat against damage that could result should an attack occur. It might turn out that certain threats do not warrant any action when the organisation compares the risk posed by the threat with the resulting mitigation costs.

This procedure allows a clear understanding of all occurring threats, which need to be addressed. The threat analysis is ultimately based on the architecture of the various (affected) applications and results in a list of the possible threats that may affect them. Of course, the threat modelling process cannot be standardized and is highly dependent on different contexts (like architecture, type of data and so on). The crucial aspect is the formulation of the context, in which the treat modelling will be carried out (Meier et al., 2003).

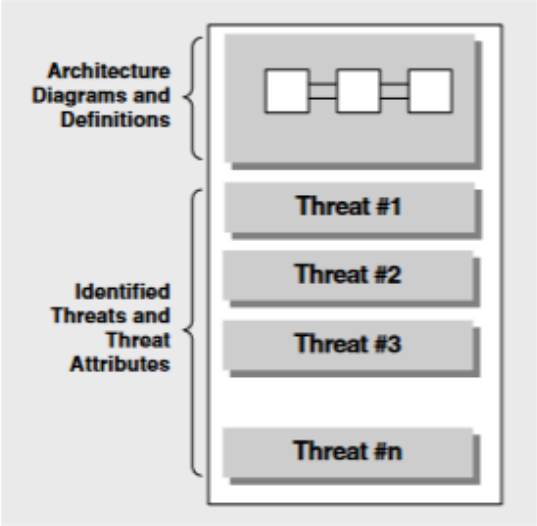

Figure 5: Components of a threat model (Meier et al., 2003)

Using the six-stage process illustrated above, the threat modelling process should not only be a one-time process. Rather, it should be an iterative loop, starting from an early phase of the design of the application or the data model, continuing throughout its whole life cycle. As it is impossible to identify all possible threats in a single moment, and that the applications will never be a static construct (they will be enhanced, adapted, or changed depending on the business requirements), the threat modelling process should be repeated on a regular base, when the design process evolves (Meier et al., 2003). This could be done at regular intervals to consider all evolutions or at points in time whenever major updates are made.

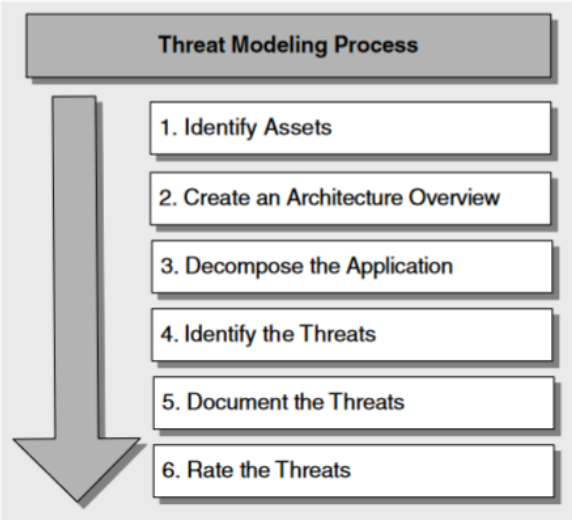

Figure 6: Iterative threat modelling process (Meier et al., 2003)

4.2.2 Framework and Definition of Potential Influencing Factors

Before starting an investigation on threats of data exchange portals, some more details about the frameworks or influencing factors of threat models need to be figured out.

Potential Influencing Factors on a Threat Model

The context of the technological and operational environment needs to be analysed. So, there could be:

- Undesirable events (the **threat**)
- Forces or actors causing the event (**threat source**)
- Structured accounts of how the event could cause the harm (**threat scenario**)
- The resulting harm (**consequence**)

As fifth aspect, **accidental sources** are those which intend no harm but can have various effects on the system. These depend on all connection points, interfaces and components in the system which can only go wrong by accident. Ultimately, there are mostly **malicious sources** that can influence or destroy other aspects in the system. These can be individuals, groups, or organizations that seek to cause significant damage to the organization in question.

Another influencing factor of a threat model is the nature of the assets which need to be protected. Different types of assets may be subject to different types of threats, and the risk profile of the assets will influence the types of threats that are prioritized in the threat model. For example, an organization with sensitive data (e.g., sensitive government data, financial data vs. customer data, etc.) may be more concerned with cyber threats such as data breaches or malware attacks, while an organization with physical assets such as buildings or equipment may be more concerned with physical threats such as theft or vandalism. Taking into consideration the operating environment of the organization or system, the level of risk may vary depending on the sector in which the organization operates, the geopolitical context, and other external factors. For example, an organization operating in a high-risk sector such as financial services or defence may have a higher risk profile and need to prioritize different types of threats compared to an organization operating in a lower-risk sector. These influencing factors should not be confused with the actual categorization of threats. These are discussed below (Bodeau et al. 2018). In conclusion, there are several influencing factors and components that play a role in the development and effectiveness of a threat model. By considering the nature of the assets being protected, the operating environment, and key components such as threat identification, risk assessment, and mitigation, organizations can develop effective tailor-made threat models to protect their assets. Of course, especially the mentioned key components are highly related to the different steps of the threat modelling process.

Various frameworks exist around threat analysis. By comparing the various aspects of these frameworks, similarities but also differences become apparent. These are reflected in the following questions:

- **What is being looked at?** This is the view from the system itself to the national or international context of the system or data exchange portal.
- **How do we conduct the threat analysis?** As a rule, the general and relevant threats that may affect the system or data exchange portal (as well as the "assets") are considered.
- **Why is the threat analysis carried out?** In the context of classic risk management, the goal is to identify the possible threats (Bodeau et al. 2018).

A threat model for TRUSTS can be targeted at multiple levels, broken down in an increasing order of magnitude:

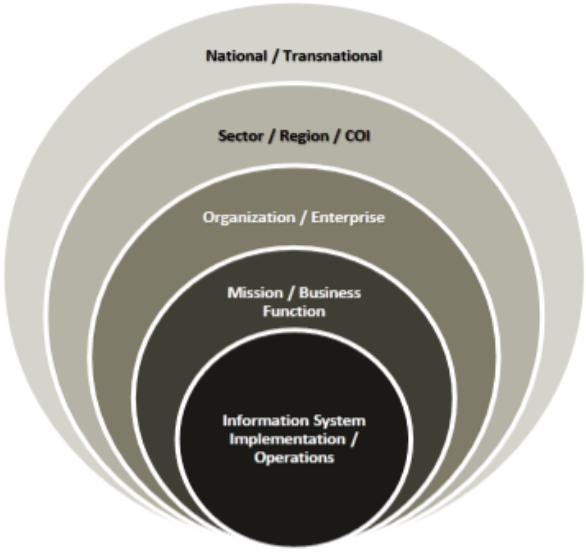

Figure 7: Possible Scope of a threat model (Bodeau et al. 2018)

1. **Level of system implementation**: influencing the selection of specific security controls or procedures; depending on the stage, the threat model knows about decisions or contributes to their design.
2. **Mission level**: influencing the elements of the business function, i.e., enterprise architecture or information architecture.
3. **Level of the organization**: as an essential component of an organization's risk framework, the threat model reflects assumptions about its threat environment.
4. **Level above the organization**: The threat model reflects a common structure for sharing threat information and can support the development of multi-participant exercises. This can also refer to national or international level, beyond the company (Bodeau et al. 2018).

A threat analysis is thus a standard requirement available to a provider of network-enabled software, systems, or devices. Considering the above mentioned six step appraoch, the modelling of a threat model for risk assessment (the modelling of TRUSTS) can be approached from thee directions:

- First, by modelling the threat in general, this is then applied to the relevant environment
- Second: A modelling of the systems, data and boundaries in the environment is done. This is followed by determining which threats these are relevant to
- Third: By identifying the assets or sore points of an organization that could be affected. These are then assessed and characterized based on the situation (Bodeau et al. 2018).

The approach to conducting a threat analysis can vary depending on the specific context and goals of the analysis. For example, a threat-oriented analysis would focus on identifying and analysing potential threats to the system or data exchange portal, while a system-oriented analysis would focus on understanding the internal workings of the system and its associated controls. Similarly, an asset-oriented analysis would focus on identifying and protecting the assets that the system or data exchange portal is responsible for safeguarding.
It is important to clarify the focus and objectives of the analysis at the beginning of the process, as this will determine the weighting and order of activities. For example, if the primary goal is to identify and mitigate potential cyber threats, then the analysis may focus heavily on assessing the system's security controls and vulnerabilities, while if the primary goal is to protect sensitive data, then the analysis may focus more heavily on identifying and protecting the assets (e.g. data) that the system is responsible for safeguarding.

Additionally, it is also important to consider the organizational context and the potential impact of identified threats on the organization's operations, reputation, and bottom line. This will help to prioritize the identified threats and determine the appropriate response to mitigate or prevent them.

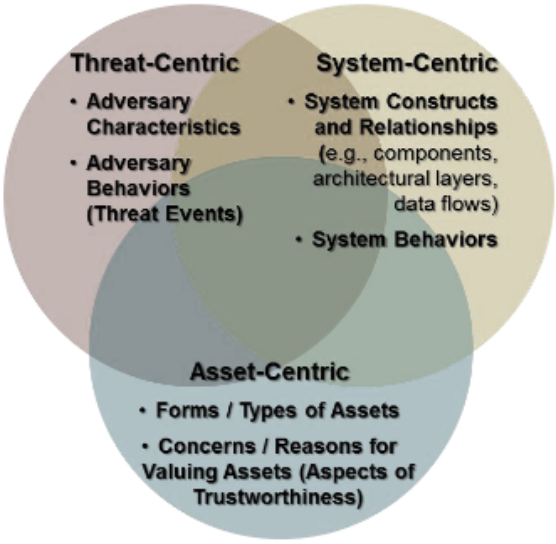

Figure 8: Threat Modelling Approach (Bodeau et al. 2018).

Frameworks for the Support of Design Analysis and Testing

When carrying out a threat assessment, users have a wide range of different frameworks to choose from for guidance. Each of them works according to its own principles and steps for optimal identification, assessment, and defence against threats. The following is an overview of available frameworks.

NIST: Developed by the National Institute for Standards and Technology, this framework consists of four components: risk framing, risk assessment, risk response and risk monitoring. Threat modelling is considered part of the first component - risk framing.

STRIDE: As an acronym, STRIDE refers to “Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege.” At first glance, STRIDE is suitable as a special method for identifying threats and is independent of the respective system architecture or specifications. For the actual threat assessment, STRIDE needs the support of another framework, namely DREAD (Kamatchi & Ambekar, 2016)

DREAD: This model is used to calculate the risk according to the following aspects.

- **Damage potential**: How great is the damage if the vulnerability is exploited?
- **Reproducibility**: How easy is it to reproduce the attack?
- **Exploitability**: How easy is it to launch an attack?
- **Affected users**: As a rough percentage, how many users are affected?
- **Discoverability**: How easy is it to find the vulnerability?

OCTAVE: This framework proposes a structured approach, especially for the identification of an organization´s critical assets, assessing its vulnerabilities and threats, and for determining the appropriate countermeasures to mitigate those threats. It consists of a series of steps for conducting the risk assessment, identifying the critical assets and their dependencies for the development of a risk mitigation plan.

Of course, the above-mentioned aspects could be extended easily to manage specific needs just by adding e.g., questions about reputation – such as, if there is a risk to reputation, which could lead to the loss of customer trust (Meier et al., 2003).

Frameworks for the Support of Information Sharing and Security Operations

When it comes to the exchange of information, there are three widely recognized models or frameworks that help identify and manage the risks and threats that exist in a technical and operational environment. These include STIX (Structured Threat Information eXpression), the OMG Threat/Risk Standards Initiative (Object Management Group), and the Cyber Threat Framework (CTF). These frameworks provide a structured approach to identify and understand the potential cyber threats and vulnerabilities in each environment and help organizations to develop and implement effective security solutions. These industry-standard models and frameworks that address the risks and threats that exist in each technical and operational environment, particularly with regard to the exchange of information:

- STIX (Structured Threat Information eXpression) is an open-source framework developed by the Cyber Threat Intelligence Technical Community (CTI TC) to enable the sharing of threat intelligence across different organizations and platforms. STIX provides a common format for describing cyber threat intelligence, including information on indicators, observables, and attacks.
- The OMG Threat/Risk Standards Initiative is a framework developed by the Object Management Group (OMG) to provide a common approach to threat and risk modelling. The framework focuses on identifying and modelling threats and risks associated with different types of systems and environments, and it provides guidelines for developing threat and risk models that can be used to support the development of security solutions.
- The Cyber Threat Framework (CTF) is a framework developed by the National Institute of Standards and Technology (NIST) to provide a common language and structure for describing cyber threats. The CTF provides a framework for identifying, describing, and communicating cyber threats and vulnerabilities, and it can be used to support the development of security policies, standards, and guidelines.

These models and frameworks are widely used in the industry and can be used to help organizations understand and manage the risks and threats they face in their technical and operational environments. They provide a common understanding of the cyber threat landscape and can be used to develop and implement effective security solutions. (Meier et al., 2003).

4.2.3 Frameworks Selection

All the frameworks mentioned so far serve as a guide for the application of the threat modelling process. Today, hybrid or customised approaches are increasingly used, tailored in detail to specific requirements and expectations. Often, a variety of information is provided that can be used by stakeholders when using the threat model in different environments. Many frameworks provide general guidance on how to proceed, but rarely include detailed tasks or activities. To develop these activities, the person responsible must have a solid understanding of the area in which they are working as well as the associated risks. Only in this way can clear activities be set up and clear measures be taken. Furthermore, the process of creating a threat model is highly dependent on the context and its level of detail. The more detailed the description of the context is, the more effective the threat modelling process will be.

Bodeau et al. (2018) highlights the issue that there is no clear framework for modelling the threat model that encompasses all points and any context in the processing. Threat models need to be adapted to different purposes and contexts so that they can be used at multiple levels and scales. Therefore, Bodeau et al. (2018) proposes a classification in which threats are categorized according to the level of detail of the threat models.

Threat modelling is an essential aspect of risk management in today's digital age. With the increasing reliance on technology and the internet, it has become crucial to understand and identify potential threats that may affect a system or data exchange portal. In this essay, we will discuss the three different types of threat models: high-level, detailed, and instantiated.

High-level threat models are a broad categorization of commonly described threat events that support risk profiling, intelligence gathering, or high-level risk assessment. These models are useful for identifying general threats that may affect a system or data exchange portal. They provide a high-level overview of the potential risks and can be used to prioritize the areas that require more detailed analysis. High-level threat models are often used to identify areas that need further research and to develop more detailed threat models.

Detailed threat models, on the other hand, are more specific and address generally described threat events that support a high-level risk assessment or within a specific domain. These models provide a deeper understanding of the potential threats and can be used to identify vulnerabilities and potential attack vectors. They also support the search for information and can be used to develop countermeasures and mitigation strategies. Detailed threat models are often used in specific industries or domains, such as finance or healthcare, where the potential risks are well understood.

Instantiated threat models are the most detailed and specific type of threat model. These models help develop detailed threat scenarios that can be used to develop playbooks or to address specific situations facing risks. They provide a clear understanding of the potential threats and can be used to develop detailed response plans. Instantiated threat models are often used in high-stakes situations, such as in critical infrastructure or military operations, where the potential risks are well understood, and the response must be immediate and effective.

It is worth noting that these models depend heavily on the respective system architecture and are often developed by the company itself. They are rarely passed on to external parties such as scientific institutes, simply to protect the company's own data situation and internal information.

In conclusion, threat modelling is an essential aspect of risk management that helps identify and understand potential threats that may affect a system or data exchange portal. The three types of threat models: high-level, detailed, and instantiated, provide different levels of detail, and can be used for different purposes. High-level threat models provide a broad overview of potential risks, detailed threat models provide a deeper understanding of specific threats, and instantiated threat models provide detailed threat scenarios that can be used to develop response plans. It is important to understand the different types of threat models and how they can be used to effectively identify and mitigate potential risks. Of course, these models depend heavily on the respective system architecture and are often developed by the company itself; they are rarely passed on to external parties, such as scientific institutes; simply to protect the company's own data situation and internal information

4.3 Preliminary Stages and Preparation of the Threat Analysis

4.3.1 Basic Requirements of the Investigation

Before beginning the process of risk analysis, it is important to establish a solid foundation for its success by taking the necessary preparatory steps. This includes determining the scope of the analysis, identifying the relevant stakeholders, and gathering relevant information about the system or data exchange portal being analysed. Additionally, it is crucial to establish a clear methodology for conducting the risk analysis, including determining the specific threats that are likely to affect the system or portal and the assets associated with it.

To ensure the security of a data exchange platform, a comprehensive information security process must be implemented. This process should be structured and cover all aspects of information security, including the roles and responsibilities of individuals involved. It may involve conducting interviews, reviewing documents, and analysing data related to the assets to be protected. The goal is to gather as much relevant information as possible to understand the values to be protected and anticipate potential threats. Additionally, a scope for the security concept must be defined. One effective method for this is to conduct a structural analysis. This may include creating important information such as business processes, network diagrams, and a list of key applications or dependencies.

A "security concept" refers to a comprehensive plan or strategy for protecting an organization's assets, including information and systems, from potential threats. It outlines the measures and procedures to be taken to ensure the confidentiality, integrity, and availability of data and systems. (Federal Office for Information Security (BSI), 2017). The assessment of the protection needs for business processes, applications, and IT systems, including the data exchange portal and associated information flows, is a critical step in determining the appropriate level of security measures. An effective method for classifying these needs is to categorize them as "normal," "high," or "very high" based on the level of potential risk and impact. For each identified target object, it is crucial to determine how the appropriate basic protection building blocks should be arranged, if available. This includes identifying necessary target objects and prioritizing them based on the level of risk and impact.

The preliminary work for the risk analysis should include the development of a comprehensive policy for managing risks. This policy should address key aspects such as the handling of risks and should be informed by guidelines and best practices established by organizations such as the Federal Office for Information Security. The aim of this preliminary work is to establish a comprehensive understanding of the potential risks and vulnerabilities associated with the data exchange platform, and to develop an effective strategy for mitigating these risks and protecting the organization's assets. This process should be carried out in a systematic and structured manner and should involve input from a wide range of stakeholders and experts. Ultimately, the goal is to ensure the confidentiality, integrity, and availability of the organization's data and systems, and to protect against potential threats. (BSI, Federal Office for Information Security, 2017):

- Under what conditions must a risk analysis be carried out in each case?
- What methodology or standard is used to identify, assess, evaluate, and address the risks?
- How is the chosen methodology adapted to the specific concerns of the institution?
- What are the risk acceptance criteria?
- Which organizational units are responsible for which risk analysis subtasks?
- Are risks assigned to the respective risk owners?
- How are risk analyses integrated into the security process, for example, before or after the implementation of IT baseline protection requirements?
- What reporting obligations exist in the context of risk analyses?
- In what time frame must the risk analysis be completely updated?

4.3.2 Investigation Objects during the Analysis (Structure Analysis)

The objects to be examined during a threat analysis are all relevant components of the threat. In the process, all business processes, critical information, and applications are identified, or the affected rooms and networks are recorded. A data exchange portal may involve the following aspects (Rütschlin, 2001):

1. Portal Management
2. Presentation
3. Portal Services
4. Information Services
5. Collaboration
6. Application
7. Infrastructure
8. Application Integration

In the traditional approach, the identification of applications is the initial step in determining the various other affected objects, such as assets within a specific application or environment. This approach is based on the understanding that the selection of applications drives the selection of the other objects that will be impacted by those applications. This method allows for a comprehensive understanding of the assets that are involved in the application and the potential risks associated with them.

However, it is important to note that this approach is not limited to just identifying the applications, but also includes conducting a thorough analysis of the different objects and their associated risks. This analysis

should include a review of the business processes, IT systems, and data flows that are affected by the applications. This will help to identify the specific assets that need to be protected and the potential threats that they may face. By taking a holistic approach and considering all affected objects, it is possible to develop a comprehensive security strategy that addresses the unique needs of each individual object. This includes identifying the appropriate protection measures that should be implemented for each object and determining how these measures should be arranged to provide the most effective level of security.

The traditional approach of identifying applications as the starting point for determining affected objects allows for a thorough understanding of the assets involved and the potential risks associated with them. This information is crucial for developing a comprehensive security strategy that effectively protects the organization's assets from potential threats.

The structural analysis is divided into the following subtasks:

- Capturing the associated business processes, applications, and information
- Creation of a network plan
- Listing of all IT relevant objects
- Recording of all necessary rooms and buildings

To reduce complexity and ensure effective management, it is important to group similar objects together in logical groups. This process of grouping allows for a more efficient and organized approach to identifying potential risks and implementing appropriate protection measures. The formation of these groups can be carried out in several ways, depending on the specific needs of the organization. One common method for grouping similar objects is based on their functional or operational characteristics. For example, all objects related to a specific business process can be grouped together, or all objects that are used in a particular IT system can be grouped together. This approach allows for a clear understanding of the assets that are involved in a specific function or process, and the potential risks that they may face.

Another approach is to group objects based on their level of criticality or importance to the organization. This can include grouping objects that are high-value assets, such as sensitive data or critical systems, separately from objects that are less critical. This approach allows for a more focused approach to protecting critical assets and addressing the most pressing risks. The grouping of similar objects can also be based on the level of risk or vulnerability that they pose. Objects that are deemed to be at high risk of potential threats can be grouped together, and appropriate protection measures can be implemented to mitigate these risks.

The specific method used for grouping will depend on the needs of the organization and the specific risks that need to be addressed. This approach allows for a more comprehensive and organized approach to identifying potential risks and implementing appropriate protection measures to secure the organization's assets. The groups can be formed as follows:

- Same type
- Similar tasks
- Similar general conditions
- Similar protection requirements
- Similar configuration (mostly for technical objects)

The foundation for determining the need for protection of various objects is the potential damage that can be caused to the relevant sub-objects in their entirety. To accomplish this, a thorough analysis of the potential impacts of damage to the objects must be conducted. For instance, in the case of an IT system, it is important to consider the effects of damage not just on the system itself, but also on the applications that are operated on it and the associated information. This includes assessing the potential impact on business processes, data integrity, and the availability of information. By considering the full range of potential consequences, it is possible to develop a comprehensive understanding of the need for protection of the IT system and the associated objects.

It is essential to consider the likelihood of potential damages occurring. To determine the potential damage, it is necessary to conduct a risk assessment that considers the potential threats and vulnerabilities. This includes identifying potential risks and assessing their likelihood, as well as the potential impact on the organization if the risk materializes.

Determining the need for protection of various objects requires a thorough analysis of the potential damage that can be caused to the sub-objects in their entirety. This includes assessing the potential impact on business processes, data integrity, and the availability of information, as well as considering the likelihood of potential damages occurring. By conducting a comprehensive analysis of the potential threats and risks and impacts, it is possible to develop an effective security strategy that effectively protects the organization's assets.

4.4 Different Types of Threats for Data Exchange Portals

Based on the understanding of various threat modelling frameworks, we will now take a closer look at the potential risks associated with data exchange portals. While data exchange portals offer many benefits, there are risks present in both the infrastructure (software and hardware) as well as the data itself or those emanating from individual users.

4.4.1 Determination of General Threat Types

The representation of possible threats can take place quite differently and in different formats. The following is therefore merely an exemplary mind map elaborated according to the explanations of Bodeau et al. (2018).

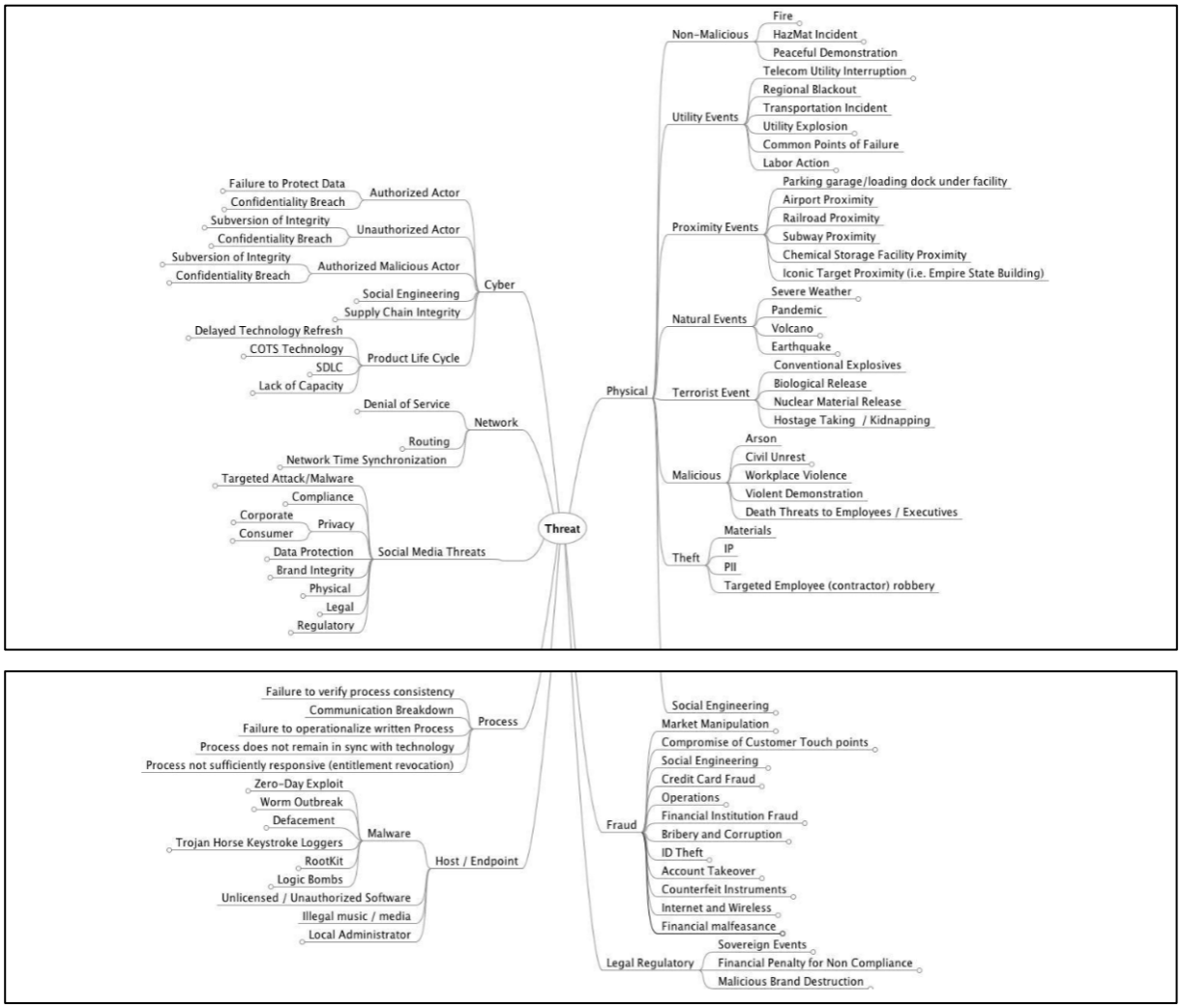

Figure 9: Threat Model example - Mind Map Bodeau et al. (2018).

Starting from many individual hazards, these can be summarized in some elementary hazards, i.e., superordinate groups. Elementary hazards are:

- Product neutral (always), technology neutral (if possible, certain technologies influence the market to the extent that they also influence the abstracted threats)
- Compatible with comparable international catalogues and standards

The following are some threats that should be considered when operating a data exchange portal:

No.	Threat
1.	Fire
2.	Unfavourable environmental conditions
3.	Water
4.	Soiling, dust, corrosion
5.	Natural catastrophes
6.	Catastrophes in the environment
7.	Major events in the environment
8.	Disruption or malfunction of power supply
9.	Failure or malfunction of communication networks
10.	Failure or malfunction of supply networks
11.	Failure of malfunction of service providers
12.	Electromagnetic interference
13.	Interception of compromising radiation
14.	Espionage
15.	Line tapping
16.	Theft of devices, data media and documents
17.	Loss of devices, data media and documents
18.	Poor planning or lack of adjustment
19.	Disclosure of information that should be protected
20.	Information from unreliable sources
21.	Manipulation of hardware or software
22.	Manipulation of information
23.	Unauthorised entry into IT systems
24.	Destruction of devices or data media
25.	Failure of devices or systems
26.	Malfunctions of devices or systems
27.	Lack of resources
28.	Software vulnerabilities or errors
29.	Unauthorised use or administration of devices and systems
30.	Incorrect use or administration of devices and systems
31.	Misuse of authorisations
32.	Loss of personnel
33.	Attack
34.	Coercion, extortion or corruption
35.	Identity theft
36.	Repudiation of acts
37.	Misuse of personal data
38.	Malware
39.	Denial of services
40.	Sabotage
41.	Social engineering
42.	Importing messages
43.	Unauthorised entry into rooms
44.	Loss of data
45.	Loss of integrity of information that should be protected
46.	Harmful side effects
47.	Violation of laws or contracts

Table 6: Sample of threats for data exchange portals

Cybersecurity threats, specifically cyber-attacks, can be considered as the most significant threats to data exchange portals. Hackers or other malicious actors may attempt to gain unauthorized access to the portal, steal sensitive information, or disrupt the operation of the platform. This poses a significant threat, particularly for the exchange of confidential or protected data.

To mitigate this threat, a comprehensive security strategy should be implemented. Strong security measures, such as two-factor authentication, should be a central component of this strategy. Two-factor authentication is a process where a user must provide two forms of identification, one of which is typically a password and the other is a unique code generated by a device or application, to gain access to a system. This process helps to ensure that only authorized users can access the data exchange portal and helps to prevent unauthorized access. Regular monitoring and auditing of the security measures implemented should be conducted to identify and address any potential vulnerabilities. By continuously monitoring the system, any suspicious activities or anomalies can be detected, and appropriate measures can be taken to mitigate the risk. This includes conducting regular penetration testing and vulnerability assessments to identify any weaknesses in the system and implementing necessary fixes.

Incident response plans should be developed and tested in advance to ensure that in the event of a security breach, the appropriate measures can be taken to minimize the damage and limit the extent of the intrusion. It is also important to have a plan for communication with relevant stakeholders, such as customers, partners, and authorities, in case of a security incident. While the risk of cyber-attacks is significant, implementing robust security measures, regular monitoring, and incident response plans can help to mitigate the risk and protect the data exchange portals. By taking a proactive approach to cybersecurity, data exchange portals can ensure the safety and security of sensitive information and mitigate the risk of unauthorized access or data breaches.

Smith (2017) also confirms the threat of cyberattack (no. 33), which in turn can be divided into several stages. Each of these steps can include intermediate attacks that form the building blocks for a more comprehensive cyberattack. The seven steps of a cyber-attack build up as follows (D. A. Smith, 2017):

- **Reconnaissance:** Before a fully-fledged cyberattack, the attacker identifies a target and explores the information related to the target.
- **Scanning:** After the identification of the target, the attacker searches for vulnerabilities by scanning the systems through attacks like resource enumeration and browsing.
- **Access and Escalation**: Once the weak spot is identified, then attacker tries to gain access to the system and then escalate the privileges to move freely with the system environment (e.g., password attacks).
- **Exfiltration**: The attacker now attempts to access sensitive assets like data and tries to extract it (e.g., storage attacks
- **Sustainment:** The attacker seeks to remain undetected and have unrestricted access by installing malicious programs like root kits which allows the attacker to return as and when desired.
- **Assault**: Now, the attacker can sabotage the system either by modifying the system or disrupt it entirely by disabling it. This means the attacker has full control of the system and it is too late to defend it.
- **Obfuscation**: This step happens when the attacker leaves a signature behind in the system to brag about his/her conquests. This usually involves confusing or diverting forensic investigation through log cleaners, spoofing, misinformation, zombie accounts, Trojan commands etc.

4.4.2 Determination of Extended Threat Types and Aspects to be Considered

In addition to the traditional and commonly identified threats, there are other potential risks that can impact data exchange portals. One such risk is the possibility of data privacy breaches or data mishaps resulting from incorrect use, operator errors, or misconduct. Accidental disclosure to unauthorized third parties can lead to unauthorized access to the portal and compromise sensitive information. To mitigate this threat, it is crucial that the respective portals provide clear guidelines for secure usage to their users and implement measures for monitoring and detection. Moreover, the risk of data loss or corruption should also be considered. This can occur due to technical reasons, such as server failures or software errors, but also because of human error. To address this risk, robust backup and recovery systems should be established and regularly tested.

Additionally, monitoring and troubleshooting procedures are essential to ensure timely detection and resolution of potential issues.

Another potential threat to data exchange portals is legal or regulatory risks, particularly if sensitive or regulated data is involved. Issues related to data privacy, such as failure to properly protect personal data or compliance with industry-specific regulations, can compound these risks. To manage these threats, data exchange portals should ensure compliance with all relevant laws and regulations and should have processes in place to regularly review and update their practices as needed. This includes conducting regular risk assessments and implementing appropriate security measures to mitigate identified risks. To ensure the safety and security of the data exchange portals, it is also important to train and educate the users on how to use the platform securely and how to detect and report any suspicious activities or incidents. Regularly conducting security awareness training can help to minimize the risk of human errors and misconducts.

While the traditional and commonly classified threats are important to consider, it is equally crucial to also acknowledge and address the other potential risks that can impact data exchange portals. By implementing robust security measures and regularly reviewing and updating their practices, data exchange portals can effectively protect sensitive information and ensure compliance with legal and regulatory requirements.

A successful attack at various stages of hacking can cause damage to the data stores. In terms of all assets, i.e., data, a data breach leading to the disclosure of proprietary data products published by the providers on the platform could result in fatal damages to the data marketplaces in terms of financial losses, reputational losses, and customer losses. If the data involved is personal data collected from users of the services provided by the data providers, the data breach may result in a soft privacy breach, which in turn has regulatory implications for the data marketplace. Soft privacy refers to the breach of privacy by a company that is in possession of personal data purchased from other companies that collect it directly from users. To protect the data on the data storage, techniques such as storing the data in encrypted form can be used. Additionally, servers need to be secured with firewalls, anti-malware, intrusion prevention systems and system monitoring, which are the basic infrastructure for security in organizations.

General or more advanced cyber-attacks with a view to data exchange portals show up as follows:

- ***Botnet:*** A botnet is a network of remotely controlled machines used to launch wide-scale denial of service attacks against specifically targeted resources (Zhang et al., 2011).
- ***Denial of Service:*** The attempt to deny users access to data or services of the system (Zlomislic et al, 2014).
- ***Eavesdropping attacks:*** Attackers attempt to intercept and analyze network packets in the communication channel; this allows them to determine information that may be relevant for attacks (Fu, 2005).
- ***Injection attacks:*** This is when the attacker injects malicious input into a program. SQL attacks in particular are considered dangerous because the attacker gains access to the database by inserting a malicious value into an input field. Subsequently, further malicious values can be injected (Muscat, 2019).
- ***Malicious codes:*** Attacks in which malicious codes or scripts are executed by programs or systems and bring undesired effects (Al-Mohannadi et al., 2016).
- ***Man in the middle:*** The attacker fools the senders and receivers into believing that the connection is secure, thus compromising the confidentiality and integrity of the data in the communication channel (Conti et al., 2016)
- ***Password attacks:*** The attacker attempts to identify a password or encryption; in the worst case, the data is altered in such a way that the actual user is denied access and countermeasures must be taken (Hansman & Hunt, 2005).
- ***Malware/viruses:*** With the goal of replication, data manipulation or destruction, viruses are placed, for example, to limit the usability of the portal (Bishop, 1991).

It is important to consider the potential risks associated with data management and data handling within data exchange portals. This includes issues such as data integrity, data confidentiality, and data availability. Data integrity refers to the accuracy and completeness of the data, as well as its ability to maintain its original form and meaning throughout the data exchange process. Data confidentiality refers to the protection of sensitive information from unauthorized access or disclosure, while data availability refers to ensuring that

the data is accessible to authorized users as and when required. To address these potential risks, it is crucial to implement robust security protocols and measures to ensure the protection of data within the data exchange portal. This includes implementing access controls, encryption, and monitoring mechanisms to detect and prevent unauthorized access or use of the data. Furthermore, it is important to conduct regular security assessments and vulnerability scans to identify and address any potential vulnerabilities or weaknesses in the data exchange portal. Additionally, compliance with relevant regulations and industry standards must be ensured to mitigate legal risks and potential non-compliance penalties.

In addition to these technical measures, it is also important to implement robust data management processes and procedures to ensure the quality and integrity of the data. This includes implementing data validation, data cleansing, and data quality checks to ensure that the data is accurate and reliable. Furthermore, it is important to establish data governance policies and procedures to ensure the proper management and handling of data within the data exchange portal. The protection of data within data exchange portals is a complex task that requires a multi-faceted approach. It is essential to consider both technical security measures and data management processes and procedures to ensure the confidentiality, integrity, and availability of the data.

These issues are important to consider as they can have a significant impact on the overall effectiveness and success of the data exchange portal. Some areas which could be impacted are:

- ***Authentication:*** This is intended to give only legitimized customers access to the services of the exchange portal; this is usually ensured by logins (username and password);
  the aim is to grant customers appropriate rights. For example, by differentiating between customers. Regular checks of the configurations must ensure that the rights and roles are assigned correctly and that the password guidelines are adhered to.
- ***Server Operation and Availability:*** The brokerage service component aims to provide platform services to customers through its two business functions: Data Management and User Interaction.
- ***Data management service:*** This takes care of all background processes responsible for providing the platform services of the marketplace. These include data cataloguing and tracking; the integrity and constant availability of this service must be listed as a dimension, which can relate to a threat / Asset that can be compromised; this can be caused by malware.
- ***Web application deployment:*** These threats mainly affect web applications; targeted attempts are made to manipulate the source code of the page and thus compromise its integrity; encryption or certifications help to avoid the risk.
- ***Attack on the transaction management service:*** An attack on the transaction management services primarily affects the core business of the data exchange portal; in addition to the loss of data, tracking would not always be possible. In this case, an external attack could also be prevented by appropriate antivirus protection or firewalls, while regular audits monitor the functional capabilities.

4.5 Possible Impact Analysis and Deployment of Counter Measures

Possibilities for a Threat Impact Analysis

In addition to a list of threats that apply to various application scenarios, it is now necessary to evaluate them and to record the threats combined with their risk. The following is not intended to provide an assessment of all the threats mentioned, as this generally depends on the case and situation. Rather, a procedure and general standard is to be specified, with which elimination of the threats is to be started and which, if necessary, are even to be neglected (Meier et al., 2003).

It is essential to understand that the threat to data exchange portals is multi-faceted and can encompass not only external cyber-attacks, but also internal factors such as human error or data mishandling. To effectively mitigate these risks, a comprehensive and systematic approach must be taken to address both the likelihood and potential impact of a given threat. This includes implementing robust security measures, regularly monitoring, and auditing for vulnerabilities, and establishing policies, procedures, and standards for data governance, quality, and security.

Simple scales (between 1 – 10) can be used to measure the probability. A 1 stands for a very unlikely threat. A 10, on the other hand, stands for almost certain. Similarly, a scale for the possible damage can be used; here, too, 1 stands for minimal damage and 10 for a possible total failure or loss. Ultimately, this results in a scale of 1 – 100 for categorizing threats. Furthermore, a division into, for example, three areas is possible to strengthen the clarity of the identified risks (Meier et al., 2003).

- **High:** The threat poses a significant risk and should be addressed immediately
- **Medium:** The threat poses a high risk and should be addressed; but less urgently
- **Low:** Depending on effort and cost, it may be decided to ignore these threats and only address them if they cannot be solved otherwise.

DREAD

To enable a more detailed threat assessment and thus also ensure a consensus among all stakeholders, Meier et al. (2013) suggest also adding further assessment dimensions that help to determine what the security threat impact really is.

The following questions are analysed:

- Damage potential: How great is the damage if the vulnerability is exploited?
- Reproducibility: How easy is it to reproduce the attack?
- Exploitability: How easy is it to launch an attack?
- Affected users: How many users are affected (as a percentage)?
- Discoverability: How easy is it to find the vulnerability?

The questions can thus be expanded, but also modified. These questions are also assigned a score of 1 (low), through 2 (medium) and 3 (high). Subsequently, all five questions result in a scale with scores from 5-15. Furthermore, the ranges of high risk are also used here with scores of 12 - 15, 8 - 11 as medium risk and 5 - 7 as low risk (Meier et al., 2003).

For the rating of risks, already simple rating tables can be used:

	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

Table 7: Thread Rating Table (Meier et al., 2003)

Options for Dealing with the Identified Threats

When it comes to identifying and managing risks, it is important to establish acceptance criteria and consider all potential options for dealing with those risks. This process can be complex, as different types of risks may require different approaches. For example, some risks may be able to be avoided by eliminating the cause of the risk, while others may require a change in framework conditions to reduce the risk. Once the possible risks of a threat have been identified, it now remains to establish acceptance criteria or the actual options for dealing with them. For example, it can usually be assumed that the acceptance of "low" or "minor" risks is predominant in companies. Risks can thus (Meier et al., 2003):

- be avoided (this leads to an exclusion of the cause of the risk)
- be reduced (this leads to a change in the framework conditions that contributed to the classification of the risk)
- be transferred; sharing the risks with another party
- accepted, because possible opportunities, which accompany the risk, are to be used
- Especially regarding risk avoidance, risk reduction and risk transfer, an organisation must define possible risk acceptance criteria and treat them accordingly. (Federal Office for Information Security 200-3 (BSI) (2017)

When it comes to managing risks, it is important to consider a variety of options and factors before deciding. One way to approach this is by asking a series of questions that help to evaluate the potential effectiveness and feasibility of different risk management strategies. These questions include:

- **Risk avoidance:** How reasonable is it to avoid a risk by restructuring processes or systems?
- **Risk reduction:** How effective is it to reduce a risk by implementing additional safety precautions?
- **Risk transfer/risk sharing:** How sensible is it to transfer the risk to another organization through insurance or outsourcing?

It is important to keep in mind that when handling risks, the risk classification for the affected objects must be constantly adjusted. These new requirements not only impact the analysed object, but also influence others. Additionally, it should be considered whether the **acceptance of the risk** is meaningful or not. The classification and treatment steps must be carried out until the risk meets the goals and objectives of an organization; this provides traceable documentation that the organization is aware of the residual risk. Ideally, an organization should only accept "low" risks. (Federal Office for Information Security 200-3 (BSI) (2017).

5 TRUSTS Monitoring & Surveillance Mechanisms for IPR Protection

5.1 Introduction

This section discusses how to achieve data security in the context of data sharing. Intellectual property (IP) is the lifeblood of every organization. IP protection is a complex duty with aspects that fall under the horizon of legal, IT, human resources, and other departments.

Drawing a concrete IP mapping and planning of exploitation activities first requires the identification of the IP assets: all expected IP values within the project must be identified, listed, named, and analysed, in a systematic way, to have a sort of project IP portfolio. For this purpose, the Consortium needs to create an IPR Repository which will further evolve to the "Exploitable Results". This repository will eventually represent the living IPR database during the project's implementation. It will basically identify project intangibles and retrace their ownership, being also functional to help the partners to recognize their IP assets and ascertain the existence of third parties' rights.

For each project result, key elements should be identified, like partners directly contributing to its development, background needed and owner, rights to use such result and license scheme. This will pave the way to a further identification to those exploitable results and will allow the partners to have the most complete information to decide about their sustainability once the project is finished.

5.2 Technical Measures to Protect IPR in Data Sharing

To ensure the efficient management of IP it is advisable to adopt a timely process and a flowchart able to identify IP results, as well as to discuss and agree on their handling and protection. During project lifecycle it is essential that information on IP is reliable and can indeed be collected and used. Each partner shall update that system on a regular basis on any new foreground and IP generated. Once collected all the partners' inputs in the IPR Repository, in Consortium meeting the innovation status update shall be presented to the Project Coordinator and contribute to clarify how to protect each IP output, disseminate it and exploit it.

Artificial intelligence (AI) is a field of scientific research whose origins date back to the mid-20th century. The objective is an ambitious one: to understand how the human cognitive system works to reproduce it and so create comparable decision-making processes. It is making it possible, for example, to automate the analysis of clinical samples, or to adjust traffic lights in response to road traffic flows without human intervention. The potential of this technology, in terms of innovation, is therefore enormous, and it is important that the EU adopt an operational legal framework for the development of European AI and public policies that are corresponding with the issues at stake, particularly with reference to the training of people in Europe and financial support for applied and fundamental research. This framework must necessarily include thinking about IPRs to encourage and protect innovation and creativity in this area.

The technological revolution – the data economy and society, the turn to AI, the growing importance of innovative technologies such as blockchain, and the IoT as well as the development of new business models such as the platform economy, and the data and circular economy - offers a unique window of opportunity to modernise the approach to protect intangible assets. In recent decades, there has been considerable progress in creating a single market for IP, yielding many benefits for the EU economy. An array of tools is available to bring innovative solutions to society.

Lastly, given the essential role of data and its selection in the development of AI technologies, several questions arise concerning the accessibility of such data, in particular dependence on data, lock-in effects, the dominant position of certain undertakings and, in general, insufficient data flow. It will therefore be important to encourage the sharing of data generated in the EU to stimulate innovations in AI[13].

[13] https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_EN.html

Securing the IP both physically and digitally is necessary. Locking the rooms where sensitive data is stored, whether it is the server farm or the musty paper archive room[14] is necessary.

Cryptography is a crucial enabling technology for IP management. The goal of encryption (as illustrated in figure 4) is to scramble/encrypt objects so that they are not understandable or usable until they are unscrambled/decrypted. Encryption facilitates IP management by protecting content against disclosure or modification both during transmission and while it is stored. If content is encrypted effectively, copying the files is nearly useless because there is no access to the content without the decryption key.

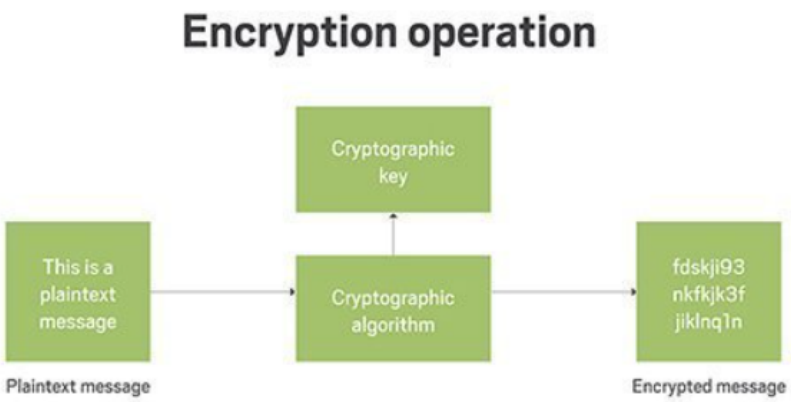

Figure 10: Encryption: How algorithms and keys are used to make a plaintext message unintelligible

When it comes to personal data, common trading practices for non-private data are prohibited, so TRUSTS become a data market for non-private data and services market and services provider for personal private data. According to TRUSTS Deliverable 4.1 "Algorithms for Privacy-Preserving Data Analytics", throughout the centuries *cryptographic ciphers* have been designed to protect stored data or, with the emergence of modern information transmission, also to protect data in transmission.

Sometimes the data to be shared contains personal or confidential information. In these cases, it needs to be checked whether the owner of the data has the right to share those parts of the data or whether those parts need to be removed or masked in some way. This is called data **anonymization**.

Personal or confidential information in this context usually refers to the following types:

- Personal data such as names, addresses, id numbers,
- Financial or other sensitive data on natural persons or legal entities,
- Identifiers and data that can lead back, by aggregation, to the identity of an individual such as an IP address in combination with a timestamp,
- Special categories of personal data such as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data that uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" as per Article 9[15] of the GDPR.

[14] https://www.csoonline.com/article/2138380/intellectual-property-protection-10-tips-to-keep-ip-safe.html
[15] EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)

The simplest course of action is to remove these fields from the data before publication. There are cases though where the simple removal results in the loss of utility and value of the data up to a point where sharing is no longer desirable.

The data and metadata related to the datasets imported to the application are all stored locally, in the user's machine which is running the application.

Federated Learning (FL) is a rather new and very popular technique (already being used by TRUSTS UC1) that has been introduced by Google (McMahan, et al., 2017) and follows the principle of bringing the algorithm to the data in comparison to sending data to a remote evaluation somewhere. Thus, it is a decentralized learning protocol where private and sensitive data never have to leave their local storage location, instead only model parameters are transmitted and updated on a central server (e.g., service provider) or cloud. In a first step local devices (mobile phones, computer nodes, etc.) download the machine learning model from the central server, perform a training step with local data and send back the updated weights or model parameters to the server where all contributions are merged.

Following the assumption that the goal of any ML problem is to find a single model that best predicts our desired outcome, and since we can often not produce a model that is most accurate in all cases, ensemble methods take a myriad of models into account, and average these models to produce one final model. Thus, the common approach to use **ensemble learning** is to train several models on the same dataset and aggregate the results using one single ensemble model.

In addition to TRUSTS privacy preserving other implementations, this approach is followed in collaboration with TRUSTS UC1 owners "The Anti-Money Laundering compliance use case". The main idea is also related to federated learning. An applied ensemble model to aggregate distributed ML results for predicting/classifying the same problem, trained on different local datasets at servers of the involved parties. This approach allows parties to collaborate with others to jointly solve a problem, without exposing their private data to each other and thus preserving the data privacy. Depending on the parties' datasets, and their description, whether they have the same feature set or different feature set. In UC1, the parties should share their trained model between each other to retrain the ensemble model avoiding the need of sharing their data for that purpose. Only the results of local evaluations are aggregated, the actual training data is not shared with others.

However, **access to confidential data** can be further regulated by[16]:

- Requirements for usage of specific authentication/authorisation procedures.
- Limiting access to approved users.
- Limiting access by only enabling remote analysis, but not the download and local processing of data.
- Removal of confidential data at least for the given period.

Which access type and corresponding regulations should apply in general depends on the mutual agreement between the user and the data owner, which should be documented in a particular licence format. Access regulations should always be proportionate to the kind of data involved and the required confidentiality.

[16] Support Centre for Data Sharing: Secure data sharing step by step

5.3 The IDS Metadata Broker as Matching Mechanism and Gatekeeper between Data Provider and Data Consumer

One mechanism to enable the above-mentioned IP mapping for representing the IPR database during the project`s implementation is the IDS metadata broker. The IDS metadata broker is defined by the IDSA as an "intermediary managing a metadata repository that provides information about the data sources available in (…) [a Data Space]; multiple Broker Service Providers may be around at the same time, maintaining references to different, domain-specific subsets of Data Endpoints"[17]. It is considered as an optional component of a data space built according to the IDS Reference Architecture Model (IDS RAM)[18] (Depicted in figure 5) and can be also described as a specialized IDS Connector. The communication between a connector and a meta data broker is therefore based on the same principle as a communication between to connectors, but is enriched by at least two additional functionalities:

- Indexing services for an effective and efficient respond to queries and present known Connectors and other resources.
- Interfaces for Users or IDS-Messages to ensure access to the stored information.

Therefore, it can be said, that the activities of such a broker are mainly focused on receiving and providing metadata to make the existing data findable. For this purpose, the broker is meant to provide an interface for the data provider to send their metadata, which is needed to be stored in a repository. The metadata should be then able to be queried by data consumers in a structured manner. The IDS metadata broker consists, next to the IDS Connector[19], of a service for data source registration, publication, maintenance, and query, based on an index, and may provide further additional services that must be described by the IDS Information Model[20]. The metadata broker is not involved in the process of data exchange.

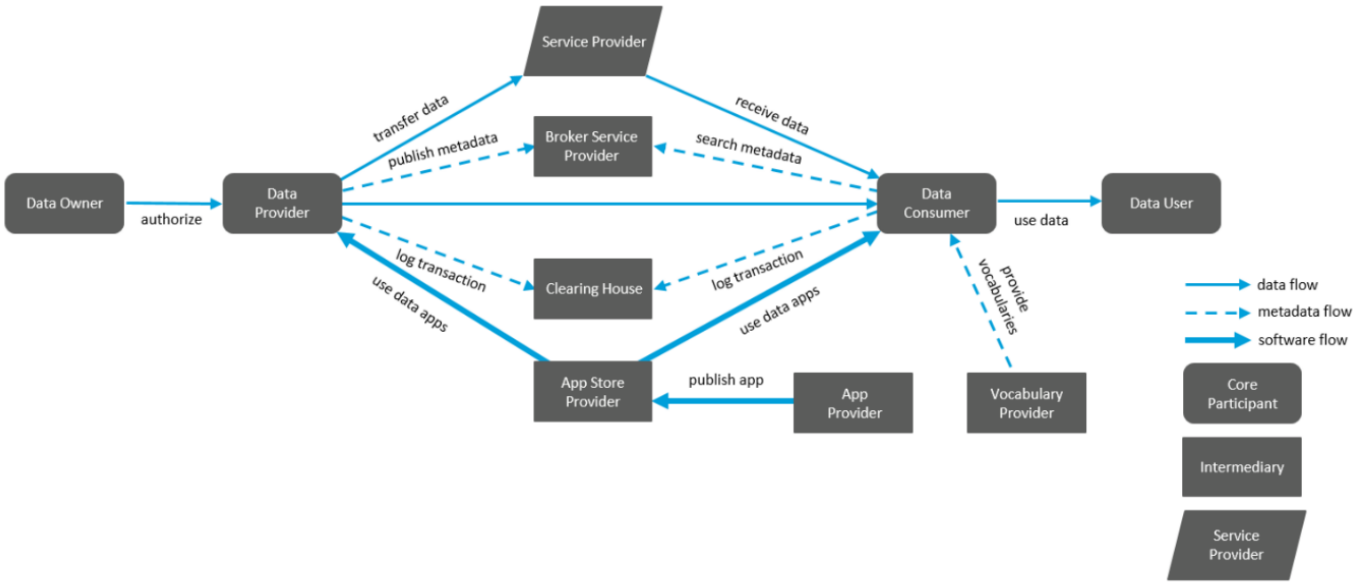

Figure 11: Roles and interactions in a data space[21]

[17] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary#broker-service-provider
[18] https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf
[19] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary#connector
[20] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary#ids-information-model
[21] https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf

The communication between IDS Connectors and an IDS metadata Broker is message oriented. There are two categories of broker messages:

- Publishing Messages (delivery of Meta Data to the index services) and
- Query Messages (query of Meta Data from the index service)

and is based on the general IDS communication between two Connectors, which is specified by The IDS Communication Guide and The IDS Handshake[22]. A more detailed overview on the metadata broker specifications is provided in the IDS Whitepaper "Specification: IDS Meta Data Broker"[23]. The Whitepaper specifies the following types of requirements an IDS metadata broker should fulfil functional, message, behavioural, business, information, interface, conditional and the communication with a connector. Further, it lists the two IDS metadata broker profiles, enhancing the basic broker functionalities by improved information management and usage policies which are called:

- the advanced information profile and
- the usage control profile.

The latter will be taken up again in the following chapter since it is of great relevance for the protection of IPR. The criteria catalogue for the IDS metadata broker can be requested at the IDSA directly here.

In a wider context, the position paper "design principles for data spaces"[24], that has been published this year by the EU funded project "OPEN DEI", is assessing a broker-like component as a requirement and a mandatory building block for data spaces, calling it "data-sharing publication". It is specified as a technical building block facilitating value creation and necessary to ensure data sovereignty.

5.4 IDS Metadata Broker and IDS Connector as Instance of Access and Usage Control

Applications of the IDS metadata broker

This kind of central service for the publishing and searching for data is also envisaged to be used in the "Mobility Data Space", which is meant as a first open data space for trusted data exchange and processing within the mobility sector, to enable new mobility offerings, as for instance seamless travel[25], It is conceptualized to offer access to real-time traffic data, to sensitive mobility data, and to link existing data platforms to each other. The Mobility Data Marketplace (MDM) is a platform that already covers some of the concepts of the Mobility Data Space. Here, the IDS metadata broker concept is used and described as "Data Representation and Data Marketplace" and holds the function of a "central service for the publishing and searching of data, with interfaces for humans and machines"[26], Figure 6 depicts the platform's architecture and its components.

[22] https://industrialdataspace.jiveon.com/docs/DOC-2524
[23] https://internationaldataspaces.org/wp-content/uploads/IDSA-White-Paper-Specification-IDS-Meta-Data-Broker.pdf
[24] https://design-principles-for-data-spaces.org/
[25] https://www.mobility-data-space.de/content/dam/ivi/mobility-data-space/documents/Mobility_Data_Space_2020_EN_neu.pdf
[26] ibid

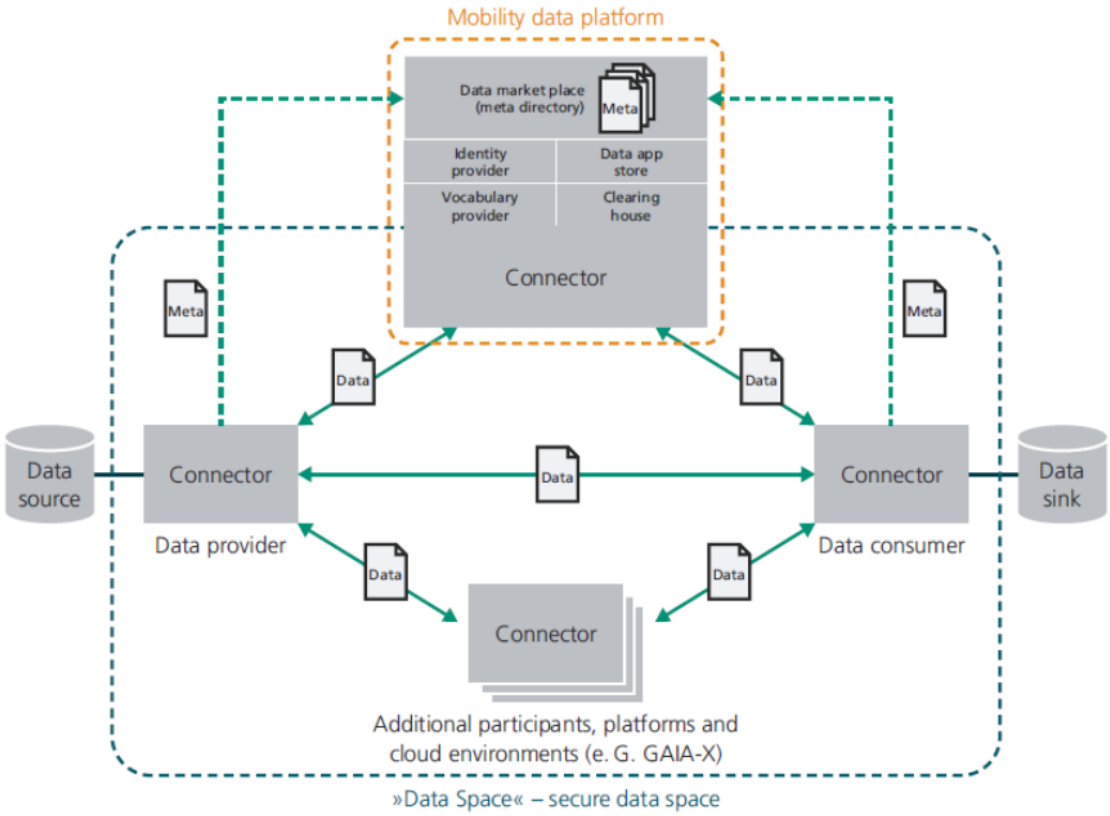

Figure 12: A data platform in the Mobility Data Space extended by IDS components

The IDS Connector as instance of access and usage control

The IDS has been working on a concept for the technical enforcement of usage policies and is described under the concept of usage control as part of the IDS Connector. Since the IDS meta data broker is a specialized IDS Connector, the usage control functionality can be implemented here as well and is then being called "usage control profile" of the metadata broker. In general, the usage control allows data providers to add to their data usage policy information that are defining how a data consumer should or should not use the data[27]. This concept is an extension to access control (see figure 7), which defines, who is allowed to access data, but once the data has been shared, the owner has no (technical) mechanism to enforce the policies anymore. The ability to enforce usage policies on the data stays at a contractual level and has therefore a limited influence on what is done with the data in the future. An exemplary case is depicted in figure 8, showing the extended access control by specific usage policies. The concept of usage control defines here that a dataset that is shared within a data space could only be shared under certain conditions and ensures technically, that these usage policies are followed by the data consumer.

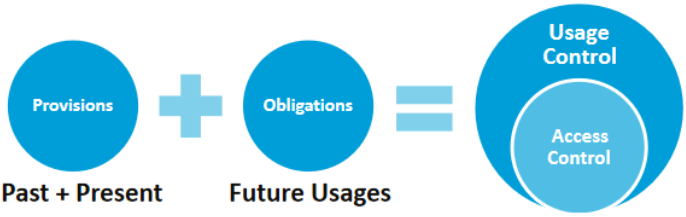

Figure 13: Data usage control – an extension of data access control28

[27] https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf
[28] ibid

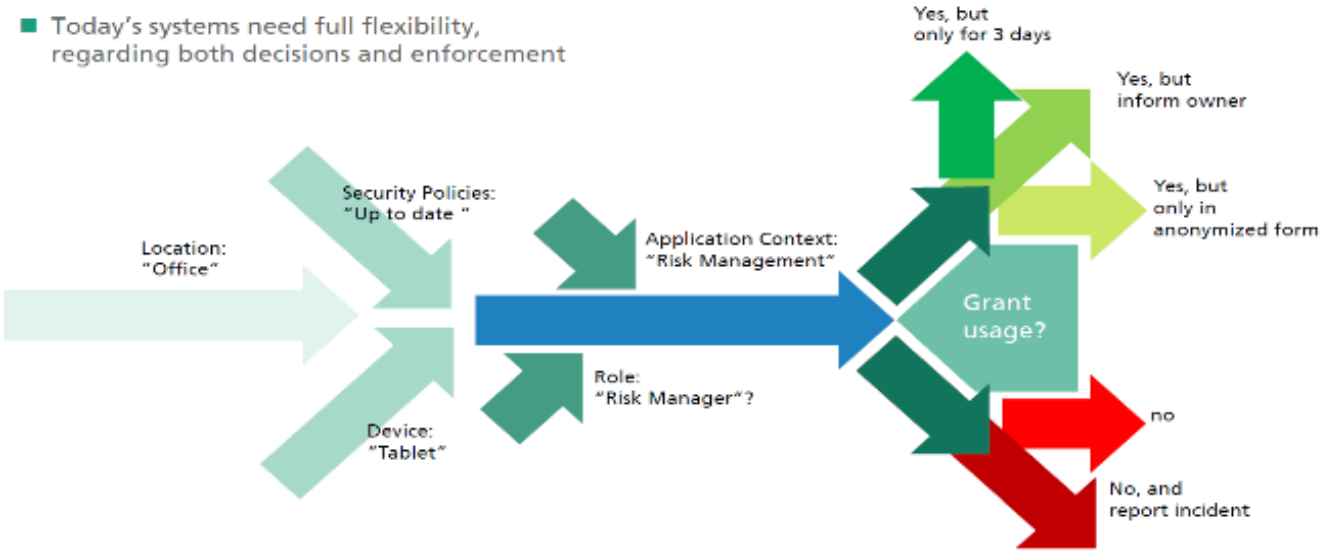

Figure 14: Example of usage control and their technical enforcement29

Security requirements that cannot be achieved by data access control, but require usage control are listed as the following table:

Security Requirement	Description
Secrecy	Classified data must not be forwarded to nodes which do not have the respective clearance
Integrity	Critical data must not be modified by untrusted nodes, as otherwise its integrity cannot be guaranteed anymore.
Time to Live	Data must be deleted from storage after a certain period.
Anonymization by Data Aggregation	Personal data may be used only in an aggregated form by untrusted parties. To do so, a sufficient number of distinct data re-cords must be aggregated to prevent deanonymization of individual records.
Anonymization by Data Substitution	Data allowing personal identification (e.g., faces in video files) must be replaced by an adequate substitute (e.g., pixelized) to guarantee that individuals cannot be deanonymized.
Separation of Duty	Two datasets from competitive entities (e.g., two automotive OEMs) must never be aggregated or processed by the same service.
Usage Scope	Data may only serve as input for data pipes within the Connector; it must never leave the Connector and be sent to an external endpoint

Table 89: Security requirements that require usage control[30]

[29] International Data Spaces Association
[30] https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf

The specifications of the IDS metadata broker with the usage control profile considers the following requirements:

Requirements for the IDS metadata broker usage control profile
An IDS Meta Data Broker may be able to negotiate or at least provide data exchange agreements, as long it has the legal rights to do so.
An IDS Meta Data Broker may filter or prohibit access to indexed metadata if an IDS Meta Data Broker has indications that the respective Data Sovereign has an interest in doing so. Such an interest can be encoded through IDS Usage Control Contracts, limiting access also of metadata to certain constraints.
An IDS Meta Data Broker may implement Usage Control engines, which can interpret and enforce IDS Usage Contracts as specified by the IDS Information Model.
An IDS Meta Data Broker may indicate that a certain rule or contract inhibits access or pretend that the requested information does not exist.

Table 910: Requirements for the IDS metadata broker the usage control profile31

As soon as the Metadata Broker fulfils these specifications (see table 7), it functions not only as a search and find function, but also as a gatekeeper that prevents prohibited access to index metadata and prevents the improper use of metadata.

IDS Connector security levels:

Both, the IDS Broker as well as the IDS Clearing House (which will be issued in the following chapter), are based on an IDS Connector Architecture. For those Connectors there are currently three main security levels defined: “Base” which ensures a minimum level of trust, “Trust”, providing an extended security profile and “Trust+” ensuring a high security level by hardware-based trust anchors (description see table).

Name	Level of security	Description
Base	Minimum level of trust	The Base profile includes basic security requirements: limited isolation of software components, secure communication including encryption and integrity protection, mutual authentication between components, as well as basic access control and logging. However, neither the protection of security related data (key material, certificates) nor trust verification are required. But it does not require the protection of security-relevant data (key material, certificates) or trust verification. Persistent data is not encrypted and integrity protection for containers is not provided. This security profile is therefore intended for communication within a single security domain.
Trust	Extended security profiles	This profile includes strict isolation of software components (apps/services), secure storage of cryptographic keys in an isolated environment, secure communication including encryption, authentication and integrity protection, access and resource control, usage control and trusted update mechanisms. All data stored on persistent media or trans-mitted via networks must be encrypted.

[31] https://internationaldataspaces.org/wp-content/uploads/IDSA-White-Paper-Specification-IDS-Meta-Data-Broker.pdf

Name	Level of security	Description
Trust+	High security level	This profile requires hardware-based trust anchors (in the form of a Trusted Platform Module (TPM) or a hardware-backed isolation environment) and supports remote integrity verification (i.e., remote attestation). All key material is stored in dedicated hardware isolated areas.

Table 1011: Overview on IDS Connector Security Profiles32

The question on when to use which security profile is to be answered by the data provider and data consumer depending on their own security requirements for data sharing. It is to mention, that in the IDS Association is currently working on a refinement of those profiles, considering recent market requirements, as for instance cloud profiles. Whether a connector is fulfilling all required specifications for a certain security profile needs to be proven by the IDS certification scheme, which is an approach for ensuring trust independently and transparently. Here, an independent instance, the Evaluation Facility, tests the components to ensure that they meet the security level's specifications[33].

5.5 The IDS Clearing House as Monitoring Instance of Transactions and Indicator of Fair Use

To enable a sharing of data assets while keeping the control over the data assets at the same time, the IDS Reference Architecture includes an optional component, that provides a set of clearing and settlement functions – the IDS Clearing House. It serves as an Intermediary, mediating between a data provider and a data consumer, ensuring, that both parties stick to the contractual obligations. Those obligations may be:

- the data provider shares data with the data consumer according to usage contracts and data usage policies defined or
- the data consumer uses data according to usage contracts and data usage policies defined and affects payment to the data provider as agreed.

In the International Data Spaces approach, clearing activities are separated from broker services, since these activities are technically different from maintaining a metadata repository. Nevertheless, it is possible that the role of the clearing house and the role of the broker service provider are provided by the same organisation, as both roles must act as trusted intermediaries between data provider and data consumer.[34]

The Clearing House has functionalities that touch the data exchange and sharing process before the process starts with:

- clearing functions, during the sharing process
- monitoring and logging functions, and after
- settlement functions.

[32] https://internationaldataspaces.org/wp-content/uploads/IDSA-Strategy-paper-certification-scheme-V.2.pdf
[33] See „IDS Whitepaper Certification – Framework for the IDS Specification Scheme, V02" for Details.
[34] https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf

The following table depicts the details of the functions:

Function name	Stage of usage	Function description
Clearing functions	Prior to sharing data	Clearing of data-sharing transactions: Legal: Verifying usage contract and data usage policies Financial: Verifying payment conditions Technical: Enabling execution of transaction and binding transaction to an instance of a data-sharing agreement and usage contract
Monitoring and logging functions	Prior to and during sharing data	Settlement functions: Discharging of data-sharing transaction Logging of transaction's metadata Tracing data provenance Monitoring and reporting of data transaction Auditing and tracking of data transactions for determining accountability and resolving possible conflicts Billing and invoicing of data transactions
Settlement functions	After sharing data, or in case of not sharing any data (for conflict resolution)	Settlement functions for conflict resolution: Investigating claim on violation of usage contract and/or data usage policy Enforcing action upon violation of usage contract and/or usage policy Legal: Escalate to a court Technical: Block a participant via Identity Provider or downgrade its degree of trust using Dynamic Trust Management (DTM)[35] Financial: Request financial compensation

Table 1112: IDS Clearing House Functions Overview[36]

During the data transfer or directly afterwards, the details of the transaction are logged in the Clearing House by both the data provider and data consumer, so that the billing or conflict resolution can be executed trustworthy: since the Clearing House is a decentralized and independent service that logs transactions, activities and is able to log also the specific conditions/usage policies under which data is allowed to be shared, it has the functionality to track and to monitor that IPR is being protected. The Clearing House can for instance track how many times data has been used, in case that a specific number of uses has been defined as a usage constrain. The Clearing House may then function as an instrument for conflict resolution if a violation has been reported by one of the involved parties.

[35] Dynamic Trust Management (DTM): Service for continuous Monitoring of network security behavior. For More Details See IDS Reference Architecture or Whitepaper Clearing House

[36] Source: https://internationaldataspaces.org/wp-content/uploads/IDSA-White-Paper-Specification-IDS-Clearing-House.pdf

Also, the IDS Clearing House is a specialized IDS Connector, just like the IDS meta data broker, which is why the connector-part of the Clearing House is responsible for the communication with other IDS Connectors. In general, a Clearing House should meet the following requirements regarding business service architecture:

Distributed implementation, business service orientation and interoperability between various clearing houses and with other intermediary roles (see Whitepaper IDS Clearing House).

For an IDS Clearing House to execute financial clearing, it should be able to financially clear a message and check the validity of the financial clearing via processes that are not in the scope of the IDS Reference Architecture.

6 Managing Intellectual Property Rights (IPR) within a TRUSTS Operating Company (OpCo): Organizational and Operational Considerations

6.1 Introduction and Overview

In today's digital age, data is an asset that is increasingly used to inform business decisions and drive innovation. However, the costs of collecting, storing, and maintaining data can be significant and it is increasingly important to find ways to share these costs and revenues among stakeholders. The TRUSTS project has developed a concept and prototype for sharing data through a data market or taking data from other data markets. In this chapter we present a concept for sharing the costs or revenues fairly among the contributors and stakeholders and describe possibilities to open this concept also to data producers and data consumers. This chapter looks at the IPR aspects of this cost and revenue sharing and a possible methodology to implement it.

The chapter considers the organisational and operational aspects of IPR protection. This chapter complements the (technical) mechanisms for the protection of data to be exchanged described elsewhere (e.g., WP3/4), and focused on the internal aspects of IPR: how should intellectual property – and this means the intellectual property of the software used in the TRUSTS platform by the TRUSTS consortium partners – be protected and costs / revenue be shared?

Three aspects of the protection of IPR of the TRUST consortium are at stake:

a) Organisational aspects of IPR protection for the TRUSTS operating company (OpCo) (Section 6.2).
b) Economic mechanisms for cost and revenue sharing within the TRUSTS consortium (Section 6.3).
c) Legal tools for the protection of data exchanged via the TRUST platform (chapter 7 with contractual tools such as TR and COC).

Point b) involves a mechanism for cost distribution – but also, in perspective, a mechanism for the distribution of the resulting profits.

If the TRUSTS platform is built and operated by a TRUSTS operator, this operating company (TRUSTS OpCo) will find itself in an economically challenging situation. On the one hand, data markets are still a young group of economic exchange venues, and on the other hand, numerous technical and organisational aspects related to the operation of a data platform for the establishment of data markets still need to be clarified. The question of the business model and monetisability will be addressed in other tasks of this work package. Overall, the conception and establishment of an operating company is an extremely complex undertaking from an organisational, economic, legal, functional, and technical perspective.

6.2 Navigating the Challenges of Managing Intellectual Property Rights (IPR) for Services and Software Components for Future TRUST Platform Implementation

Overview of the Chapter

In this chapter the challenges of managing intellectual property rights (IPR) for services and software components in the implementation of the TRUSTS platform are discussed. It mentions different options for protecting IPR in a data platform like TRUSTS, such as protection through contracts, access mechanisms, technical security systems, monitoring of user behaviour, encryption, and watermarking. It also highlights the importance of a further elaborated concept to support these options and the importance of cross-system mapping of data assets, actualization of metadata from decentralized data storage and data networks, and interaction of automatic digital contracts and data assets for the future TRUSTS platform. The text also discusses the challenges of dealing with the timeliness of metadata, marking options, and the need for a system for dealing with the inaccessibility of certain data assets.

TRUSTS Operator Organizational Measures to Protect IPR

One of the goals of the TRUSTS project was the conception of an operating company (TRUSTS OpCo), which will continue the prototypical operation after completion of the project and transfer it to future productive operation. In this chapter, the aspects of organizational measures are outlined. In other WPs of the TRUSTS project, the relevant aspects for setting up a TRUST platform are considered (technology, legal, business, operation, etc.). As described earlier, in principle there are the following options for protecting intellectual property in a data platform like TRUSTS:

1. Protection through (user) contracts
2. Protection through contract-based access mechanisms to data
3. Protection through technical security systems for transmission and storage
4. Protection through monitoring of user behaviour and corresponding alarm mechanisms
5. Protection through encryption and / or watermarking of data
6. Protection by the nature of the data (e.g., loss of value in the case of obsolete data)

To be able to protect the IPR of the users of the TRUSTS platform even better in the future, a further elaborated concept is necessary to ensure these six aspects mentioned above can be supported in the long term. The 6th point is outside the sphere of influence of the TRUSTS OpCo because it concerns the data provider itself. Points 1-5, on the other hand, are within the sphere of influence of the TRUSTS OpCo and should be given special consideration and attention when setting up the TRUSTS OpCo. For the more technical users of the future TRUSTS platform, points 3, 4 and 5 are probably the most interesting ones. IP infringement incident reporting and sanctioning can and should be a service of the TRUSTS OpCo. For this purpose, the systems mentioned in chapter 4 must be enhanced, implemented and operational.

From IPR's point of view, three fundamental aspects are important to the further development of the TRUSTS platform:

a) Cross-system mapping of data assets

b) Actualisation of meta data from decentralised data storages and data networks

c) Interaction of automatic digital contracts and data assets

Cross-system Mapping of Data Assets

For the data providing customers of the TRUSTS OpCo, it is crucial to have all information offered by the data provider on data assets, data projects, data releases, contracts, as well as monitoring and quality indicators, mapped in one place in a knowledge graph to enable further operations. This knowledge graph should contain functions for an automatable metadata management, by means of which the data providers can manage and control their offered data assets on the provider side even better. In chapter 3.2, the FAIR principles were introduced (Findability, Accessibility, Interoperability, Reusability). Decisive for their implementation is metadata, which enriches the corporate data with contextual information: Content, definition, origin, etc. By mapping the entire data lifecycle, from data creation to data release, a new approach to quality control and monitoring of data assets can be established (Boeckhout et al. 2018). The IDSA is already in the process of conceptual implementation with the approach mentioned in chapter 4.

Actualization of Meta Data from Decentralised Data Storage and Data Networks

The conceptual approach in the TRUSTS project provides that data is held in a decentralized manner within the data providers' servers and not centrally at one location as in conventional data platforms. Because of this, necessities arise with regard to synchronization mechanisms and availability. If a data provider is not accessible (for whatever reason) or a data asset offered is not accessible (e.g., sensors are offline), then this information is important for TRUSTS. The future TRUSTS OpCo must therefore develop a system for dealing with the timeliness of the metadata and for determining which marking options are necessary. For example, it may be important to subject certain real-time data in the data catalogue to a recurring, higher-frequency checking mechanism. The price of decentralisation is therefore a higher effort in keeping the metadata up to date. This aspect could become more important, especially for demand and providers of real-time data. If the data are taken from data networks (for example in a Gaia-X environment), the complexity increases accordingly.

In order to ensure the real-time exchange of data assets between individual network partners, consideration should be given to developing a peer-to-peer synchronisation mechanism to ensure that metadata are up to date. Here, it is particularly important to obtain ongoing information about availability, releases, contracts, etc. The IDSA is working on corresponding concepts and interfaces for data exchange.

Interaction of Automatic Digital Contracts and Data Assets

By implementing policies and contracting that can be automated, data exchange could be made even more efficient in the future. Further automation of contract formation and execution with standard and default smart and an overall improvement of the policy engine could be an important task for the future TRUSTS OpCo. The research conducted on smart contracts during the TRUSTS project showed that if more contracts can be automated, more user requirements can be met. The automated creation, distribution and reconciliation of contracts is an important function. The TRUSTS platform has already achieved promising results, but for a sustainable, self-supporting, or industrially productive system it seems necessary that these functions are further expanded. In the future, the TRUSTS data ecosystem could consist of decentralized software components that network with each other and form a consensual network that constitutes the basis for digital contracts.

Each component could provide decentralised data assets and collect the associated metadata and metrics (availability, quality, etc.) for each data asset. The information could then be stored in a database optimised for data exchange and selectively made available to other participants in the network. Based on the decentrally collected information (from local resources or decentral sensors or by other means), digital contracts are mapped that regulate data access, data exchange and data use. Through the access of the individual components to the decentralised data stocks, individual clauses such as rule-based or time-limited data release can be enforced automatically (e.g., auto-contracting, or smart contracting).

Implications and Recommendations from TRUSTS Platform Development

There are substantial gaps in the knowledge base available to policy makers who must grapple with the problems raised by digital intellectual property (National Research Council. 2000). IP will surely survive the digital age, although substantial time and effort may be required to achieve a workable balance between private rights and the public interest in information. Major adaptations may need to take place to ensure that content creators and rights holders have sufficient incentives to produce an extensive and diverse supply of intellectual property. A good mechanism is one that provides the degree of disincentive desired to discourage theft but remains inexpensive enough so that it doesn't greatly reduce consumer demand for the product.

When it comes to protecting intellectual property rights (IPR), it is crucial to take a proactive approach to deter and prevent future violations. One way to do this is by working together as a team to identify and address potential issues. One important aspect of this is monitoring the marketplace, both online and offline, to stay informed about the products being offered and the reputation of the providers.

One way to stay informed about potential IPR violations is to analyse customer and end-user reviews on products related to the company's intellectual property (IP) products. This can provide valuable insight into any issues that customers may be experiencing, such as counterfeits or infringing products. By monitoring these reviews, the company can quickly identify and address any potential IPR violations.

Another important step in protecting IPR is performing due diligence on providers. This means carefully researching and evaluating potential partners, suppliers, and other third-party vendors to minimize the risk of IPR violations. This can include checking for any history of IPR violations, as well as verifying that the provider has the necessary licenses and permissions to use any IP-related products and services. By taking these steps to screen potential partners and vendors, the company can ensure that they are doing business with trusted partners who are committed to protecting IPR.

The objective of these efforts is to create a marketplace that is safe and trustworthy for both the company and its customers. By monitoring customer reviews, performing due diligence, and working together to deter and prevent IPR violations, the company can ensure that its IP products are protected and that it is doing business with trusted partners who share this commitment to protecting IPR.

Digital Platforms are Uniquely Positioned to Create and Capture Value in the Digital Economy.

Following the D2.2 analysis and the overall results, all the interviewees expressed their eagerness for the TRUSTS results, since all agreed that getting access to a trusted data marketplace that will be able to accommodate a big number of data and services, respecting and conforming to the European laws and regulations about data privacy and management, would be a very useful tool in their daily work operations. The findings that emerged by the interview analysis are summarized in the following requirements remarks.

Secure and Legally Compliant Exchange of the Datasets and Services is Required.

Many of the interviewees argued on the assurance that the TRUSTS platform should provide in respect to the integrity of the transactions performed between the producers and the consumers, as well as the need for a legally compliant secure framework that will ensure the protection of the data that are made available in terms of privacy and infringement protection. Also, compliance with European Central Bank (ECB)'s regulations for financial data is required. Furthermore, many interviewees considered that this conformance capability should be exposed to the users through a comprehensive description of the terms of use. In addition, local laws should apply to each federated node. A suggestion to facilitate business is to provide a set of predefined contracts.

Review Published Data to Make Informed Decisions on Buying Legitimate Products.

Data marketplace should be easy and friendly to use, leveraging productivity and decreasing operational costs through an enriched cost-effective functionality. A general comment that emerged by most of the participants was the need for an easy and friendly to use data marketplace, which can provide intuitive and comprehensive functionalities in the most productive way. This approach should enable mitigating the companies' operational costs in their quest of selling or buying data and services.

Need for Mechanisms that Ensure the Validity of the Datasets and Services Onboarding Process. Users' Reputation Schemes should also be supported as a Protection Measure.

It was clear by most of the interviewees that trust to the platform should be ensured by providing self-regulating mechanisms regarding on the one hand the validity and integrity of the onboarded data sets and services, and on the other hand the trustworthiness of the providers. The existence of such mechanisms will act as key enablers for the buyers, to annotate and provide feedback that pertains to the quality of the datasets and services that they have bought, as a quality metric of the data and services a producer offers.

Due to the expected large number and vast diversity of the onboarding datasets and services, flexible pricing models, billing mechanisms and brokerage services should be provided. The integrity of the transactions between producers and consumers should be safeguarded through smart contracts, audit mechanisms and transaction logs, which must constitute an inherent part of the system.

A common sense that was evident from all participants is their need to use TRUSTS as a one-stop-shop service, through which they can find, bid for and buy available data sets and services. To that end they considered the existence of a billing system as well as brokerage services as granted. Another aspect that the interviewees considered to be supported by TRUSTS is the implementation of flexible pricing models suitable to being adapted according to the characteristics of the provided datasets and services. Finally, it was mentioned that it would be useful for the enterprises and companies to be able to create corporate accounts for their employees so that only one subscription/enrolment will be required.

Effective and secure user management should be employed.

Besides the profiling of users, datasets, and services, one fundamental aspect that emerged from the interviews was the need for user management. In more details, within the TRUSTS environment, the users need to feel protected, especially because they intend to make monetary transactions for valuable assets. To that end, strong authentication and authorization mechanisms should be provided, either to isolated users but also to enterprises and companies that must give access to more than one of their employees. Furthermore, it was mentioned that each user should be aware of new data products / shared data catalogues / data services that fit their needs in a timely manner, as well as be able to announce to the marketplace their needs for data sets and services.

Inherent protection of private datasets should be provided.

Many of the interviewees need to gain access to data that might often originate from the processing of personal (including sensitive) data. Thus, the protection of such data sets through anonymization mechanisms (that will be applied on the data sets during their onboarding process and before they are published via the TRUSTS platform), is more than necessary according to the participants' opinion. Furthermore, some of the interviewees stated that it would be very useful if de-anonymization risk assessment could be provided as a protection measure for the anonymized data that the TRUSTS users' aim to publish. Finally, participants also welcomed the possibility to rely on data sets intersection, through cryptographic techniques that allow two or more parties to combine data in an encrypted manner to be able to compute their intersection (all relevant protection approaches can be applied e.g., Private Set Intersection (PSI)/Multi-Party Computation (MPC), masking common parameters to datasets that are used for correlation, etc.).Work package WP4 was working extensively with these topics. Please finde more details on theses aspects there.

6.3 Conceptualizing Intellectual Property Rights (IPR) Management for Services and Software Components for Future TRUST Platform Implementation

The topic of managing and protecting intellectual property rights (IPR) within an organization like the future TRUSTS OpCo can be complex and challenging. One potential solution is to implement a decentralized autonomous organization (DAO) model, such as a TRUSTS-DAO, to handle the management of services, software licenses, and cost and revenue sharing. Additionally, utilizing digital tokens, such as dataNFTs, can aid in securely and transparently protecting members' IPR. This chapter will explore the potential benefits and drawbacks of implementing a dataNFT-based cost and revenue model. It will also delve into the various structural, organizational, legal, and technical elements that must be considered when building a strong foundation for a TRUSTS-DAO. Furthermore, it will examine the importance of utilizing a 'Zero-Knowledge' approach in securing IPR and the steps required for setting up a TRUSTS OpCo.

Overview of the chapter 6.3:

6.3.1	*Developing a Consensus on the Intellectual Property Rights of Services and Software Components among TRUSTS Consortium Partners*
6.3.2	*Implementing a TRUST-DAO model for managing services, software licenses and cost sharing in the TRUSTS OpCo*
6.3.3	*Implementing dataNFT in a TRUSTS-DAO model for secure and transparent protection of members' IPR*
6.3.4	*Utilizing dataNFTs for managing software license usage and ownership through digital tokens*
6.3.5	*Analysis of the Pros and Cons of Implementing a dataNFT-based Cost and Revenue Model*
6.3.6	*Building a Strong Foundation: Navigating the Structural, Organizational, Legal, and Technical Elements of a TRUSTS-DAO*
6.3.7	*Supporting the Securing of Intellectual Property Rights with a 'Zero-Knowledge' Approach*
6.3.8	*Setting up the TRUSTS OpCo*

6.3.1 Developing a Consensus on the Intellectual Property Rights of Services and Software Components among TRUSTS Consortium Partners

One of the goals of the TRUSTS project is to establish a TRUSTS operating company (OpCo) or an alternative operating entity, to manage the technical, legal, and administrative aspects of the TRUSTS platform. This report focuses on the technical and some of the legal aspects, such as protecting the intellectual property rights of the TRUSTS partners and users of the TRUSTS platform, the existing concepts and steps that have been taken for implementation, and what will still be necessary in the future.

Since the TRUSTS project ended, it is essential for the future development of a TRUSTS OpCo to clarify the rights of use for the services and software components developed during the project. This is because the use of the developed software has a direct impact on the business model and the economic feasibility of using the software components in the future TRUSTS OpCo. It is therefore essential to answer this crucial question to establish the TRUSTS OpCo: under what conditions are the consortium partners of the TRUSTS project willing to bring in their services and software components into the future TRUSTS platform?

The type of services and licenses used and the level of user fees will have a direct impact on the profitability of the future TRUSTS OpCo. If the licenses or prices for using the components are too high, it could reduce

the margins that can be achieved from data transactions with market participants. On the other hand, if prices are too low, the owners of the software components and their developers may not find it profitable to operate or develop the components. Both these scenarios would be detrimental to the sustainable operation of the future TRUSTS platform and OpCo.

To transfer the TRUSTS platform developed during the EU Horizon 2020 project into sustainable operation by the TRUSTS OpCo, it is necessary to clarify the rights of using services and software components as early as possible and establish a contract among the TRUSTS consortium partners that enables the future TRUSTS OpCo to operate the platform in an economically viable manner. The interests of all parties involved must be considered and a well-balanced solution must be found.

In research projects, a mixture of different types of rights of use can always be found. Some rights remain with the consortium partners who developed the software beforehand and now contribute it to the project and develop it further through funding. In this case, the rights to the software usually remain with the contributing organization. On the other hand, funding institutions take the view that assets developed with publicly funded money and their rights of use belong to the public.

This chapter presents a proposal for a methodology for balancing the interests of the TRUSTS OpCo (operation on low costs) and the contributing TRUST consortium partners (receiving a high revenue from usage of their components) through contractual agreements within the consortium.

The main challenges to this endeavour are the following:

- TRUSTS partners contributing services and software components seek to earn the highest possible revenue in exchange for the rights to use the software.
- The TRUST OpCo starts under difficult conditions in a barely established data exchange market and must keep the operational costs of the software components used for the TRUSTS platform as low as possible in real-life operations.

Solution approach:
Introduction of a DAO-based dynamic remuneration system for the software components contributed by TRUSTS partners.

Proposal for implementation:

Decentralized autonomous organizations (DAOs) are a new form of digital organization that have gained popularity in recent years. They are based on blockchain technology and operate as decentralized, self-governing entities that are owned and controlled by their members. One of the key advantages of DAOs is their hands-off handling of the software with low management efforts. This makes them an attractive option to companies looking to streamline their operations and reduce costs.

One potential use case for DAOs is in the field of data and intellectual property rights (IPR) agreements. In this scenario, a DAO can be set up as a legal entity to manage and govern data and IPR agreements in a lean, cost-efficient, and open manner. This is made possible using Web3 technologies, which allow for greater transparency and collaboration in the management of data and IPR agreements.

Despite being in the early stages of development, there are already solutions available for setting up and managing DAOs. For example, platforms like Ocean (oceanprotocol.com) and DataUnion (dataunions.org) provide tools for creating and managing dataNFTs (non-fungible tokens), while DAO toolkits like Aragon (aragon.org) provide the necessary infrastructure for setting up and managing decentralized organizations. This means that companies do not need to reinvent the wheel but can instead adapt existing solutions to their specific needs.

An important principle in the field of data and IPR agreements is sovereignty. This refers to the idea that individuals and organizations should have control over their own data and intellectual property. DataNFTs can help with this by allowing for the creation of unique digital assets that can be owned and controlled by their creators. One aspect of revenue sharing in the field of data and IPR agreements that can be challenging is determining the value of data or intellectual property. This is often difficult because the value of data or

IPR is mostly determined by its future applications, which can be uncertain. For example, the DataUnion value share approach addresses this issue by allowing partners to participate in future success, while also providing flexibility for partners to enter or exit the partnership.

The following subsection describes the concept of utilizing dataNFT-based cost and revenue models, which utilize non-fungible tokens to automate the allocation of costs and revenues related to running TRUSTS as a data platform. This chapter examines the advantages of using dataNFT-based models, including how they can create a more efficient and fair system for managing the costs and revenues associated with data platforms. Additionally, it explores the challenges and limitations of implementing this model, and provides recommendations for organizational, legal, and technical considerations.

6.3.2 Implementing a TRUST-DAO Model for Managing Services, Software Licenses and Cost Sharing in the TRUSTS Operating Company (OpCo)

Implementing a dataNFT-based Services and License Cost Sharing System within a TRUSTS-DAO Framework in TRUSTS

DataNFT, short for "data non-fungible tokens," are a type of digital asset that represents ownership of a unique piece of data or information. They are typically stored on a blockchain and can be bought, sold, or traded like other digital assets. In this subsection, we will explore how dataNFTs can be used for managing software license usage and ownership, as well as for sharing development, services, and software costs among partners in a start-up company (such as the TRUSTS OpCo). DataNFTs can be used for managing software license usage and ownership by creating unique digital tokens that represent ownership of a specific software license. Each token would be unique and linked to the specific license that it represents. The OpCo can then use smart contracts on the blockchain to track and verify the ownership of the license and ensure that the software is only used by authorized users or that all members of the TRUSTS-DAO contribute accordingly to the contractual agreements.

The approach outlined in this subsection is that the pricing mechanisms for the future TRUSTS OpCo are designed to assume that the TRUSTS consortium operates as a virtual, decentralized organization, where members contribute services, development efforts, license rights and software components that are used collectively and billed individually. This virtual autonomous organization can be compared to that of a Decentralized Autonomous Organization (DAO). In this model, the entirety of the TRUSTS partners who provide services and software components for the operation of the TRUST platform are treated as a virtual decentralized organization (TRUSTS-DAO).

DAOs are designed to be decentralized, meaning that no single person or entity has control over the organization. Instead, the organization is run by its members, who use a token-based system to vote on proposals and allocate funds. One of the key benefits of using tokens for cost sharing in a TRUSTS-DAO is transparency. Because all transactions are recorded on the blockchain, members can easily see how funds are being allocated and used. This transparency is important to build trust among members and maintain accountability within the organization. Decentralization is another important benefit of using tokens for cost sharing in a TRUSTS-DAO. No organization is controlled by any single entity, which allows for a more democratic decision-making process. Members can vote on proposals and allocate funds based on the consensus of the group, rather than relying on the decisions of a single leader or group of leaders. Security is also a key benefit of using tokens for cost sharing in a TRUSTS-DAO. Since tokens are stored on a blockchain network, they are protected against hacking and other forms of tampering. This provides an added layer of security for the organization and its members.

The flexibility of a DAO-approach is another important benefit of using tokens for cost sharing in a TRUSTS-DAO. Since organisations are not controlled by any single entity, they can easily adapt to changing circumstances and quickly respond to new challenges. For example, if a new project or initiative arises, the organization can quickly allocate funds without needing to go through a long and complicated approval process. Finally, using tokens for cost and revenue sharing in a TRUSTS-DAO can also result in lower transaction costs. Transactions on a blockchain network are usually cheaper than those on traditional networks, as blockchain

networks are decentralized and there is no need for intermediaries such as banks or payment processors. Using tokens for cost and revenue sharing in a TRUSTS-DAO enables a more transparent, decentralized, secure, flexible, and cost-effective way for the organization to operate. The token-based system allows for a clear and transparent way for members to vote on proposals and allocate costs, revenues, and funds, and the decentralized nature of the organization allows for a more democratic decision-making process.

Implementing a TRUSTS-DAO Governed by DataNFT for TRUSTS Consortium Members

Using a "TRUSTS-Decentralized Autonomous Token" (or "TRUSTS-DAO Coin" for cost sharing in a TRUSTS-DAO can bring specific benefits to members that go beyond just allocating and sharing the costs of running the organization. One of the main benefits – if for example these dataNFTs are used also for charging transferred user data - Is that members can use these tokens to gain access to exclusive benefits such as discounts, rewards, or access to special projects (like further development or participation in future growth projects). For example, Partner A, who develops and maintains the TRUSTS Core Services, might receive 10% of the total tokens available. Partner B, who develops and maintains the TRUST recommender system, might receive 5% of the total tokens in circulation.

Another benefit of using tokens for cost sharing is that members may see an appreciation in the value of the tokens they hold. This can be a financial benefit for members and can incentivize them to participate in the organization's activities. As the demand for the token increases, the value of the token may also increase, which can provide a financial return to members. This means that in practice, in the beginning of the life cycle of TRUSTS, the revenue for the TRUSTS OpCo generated by the software components from the consortium starts low and increases with the popularity of the TRUSTS platform and the amount of data exchanged. Therefore, token liquidity is an important benefit of using tokens by the TRUSTS OpCo. If public tokens are used for this mechanism, tokens can also be easily traded on various cryptocurrency exchange platforms, which allows members to easily liquidate their tokens if they choose to. This can be a benefit for members who may need to sell their tokens for financial reasons. This feature can increase the adoption of the token by potential members and investors, as they may see the token as a liquid investment.

The TRUSTS OpCo can also set up a mechanism for partners to earn additional tokens based on their performance. For example, if a partner develops and maintains their software components or services in a timely manner, they can receive a bonus token. Partners may then trade or sell their tokens on a secondary market, giving them more liquidity options. Additionally, partners can also use their tokens to purchase goods and services from other partners in the group. Additionally, the TRUSTS OpCo can also set up a mechanism to add or remove tokens based on the performance: for example, if the TRUSTS OpCo revenue goes up the total token available will increase; and vice-versa if the total revenue decreases.

Voting rights vs. profits rights

TRUSTS-DAO creates also voting rights in the future TRUSTS OpCo. Members can use their tokens to vote on proposals, which gives them a say in how the organization is run or further developed. This can boost a sense of ownership and can incentivize members to participate in the organization's activities (for example maintenance of the TRUSTS platform, enhancing existing software components). By providing members with the ability to vote on proposals, use of resources, or incentivizing them for their contributions to the operation of the TRUSTS OpCo, the organization can become fairer and more balanced. This increased transparency in resource usage can lead to more effective decision-making, as all stakeholders have a say in the direction and operation of the organization.

One common concern about this governance model is how to maintain this fair and transparent voting process when members holding more tokens have more influence on decisions. This proportionality between tokens and decision-making power may make sense in theory, but there is a risk of overreliance on the value of a single organization within the DAO. The issue arises when one or two organizations, for reasons that may not be entirely fair, become excessively influential. This could skew the decision-making process and undermine the democratic principles of the DAO. To mitigate this risk, it is crucial to have transparent and objective mechanisms in place to ensure that all members have an equal opportunity to participate in some decision-making, regardless of the number of tokens they hold.

One potential solution to this disadvantage could be the introduction of a dual governance model for voting rights and profit rights. The profit rights could be tied to the tokens, whereas the other aspect of the tokens or a separate token type would decide on voting rights. However, such a model would be even more complex than the current model presented. It would be like a corporation having two types of shares: voting shares and non-voting preferred shares. The voting shares would be used for decision-making in the voting governance, and the total number of shares would be used for decision-making in the profit governance. Therefore, if the TRUSTS dataNFT is designed with a “voting share” and a “profit share”, a dual governance model could be implemented, making the token model fairer and addressing the concerns mentioned above.

Token economics is a crucial aspect of a dataNFT-based model for software licensing as it helps to incentivize the participation and contribution to the ecosystem. This can include things such as token buyback and burn mechanisms, staking mechanisms, and other economic incentives that can be implemented to encourage participation and contribution. A dataNFT-based model for TRUSTS OpCo requires a combination of technical and business expertise.

A token-based reputation system is another benefit of using tokens for cost sharing in a TRUSTS-DAO. TRUSTS-DA tokens can be used to create a reputation system for members. Members who hold more tokens or have a higher token balance can be seen as more influential or more valuable to the organization. This can incentivize members to participate in the organization's activities and to contribute to the organization in meaningful ways. By creating a reputation system based on tokens, the organization can reward members who contribute to the organization and make it more effective.

6.3.3 Discussion about Advantages and Disadvantages of Utilizing dataNFTs and Potential Mitigation Measures

The concept of dataNFT as a data token for managing software license usage and/or ownership is a new way to use blockchain technology to track and verify the ownership and usage of software licenses. The future TRUSTS OpCo may use dataNFT that represent ownership of a specific software license. DataNFT can be useful for TRUSTS OpCo to manage the usage licenses from TRUSTS members, and for members to prove ownership and usage of their licenses / IPR. The following table provides a concise overview of the main benefits of using DataNFTs in a TRUSTS-DAO setting:

Token-based incentives	The TRUSTS OpCo can use dataNFT tokens as a form of incentives for partners to contribute their software components and services. For example, the company can offer bonus tokens to partners who develop and maintain their software components and services in a timely manner, or to partners who provide additional features or functionality.
Token-based revenue sharing	TRUSTS OpCo can use dataNTF tokens as a form of revenue sharing for partners. For example, the company can set up a smart contract on the blockchain that automatically distributes tokens to partners based on their contributions to the company. This can help to ensure that partners are fairly compensated for their work.
Token-based decision making	TRUSTS OpCo can use dataNFT tokens to give partners more control over the company's decision-making process. For example, the company can set up a voting system that allows partners to vote on important decisions using their tokens. This can help to ensure that partners are more invested in the company's success and that their contributions are taken into account.
Token-based liquidity	TRUSTS OpCo can use dataNFT tokens to provide partners with more liquidity options. For example, partners can trade their tokens on a secondary market, which can give them more flexibility when it comes to managing their contributions to the company. Additionally, partners can also use their tokens to purchase goods and services from other partners in the company.

Summary of the advantages

- Transparency and immutability: The use of blockchain technology ensures that all transactions are transparent and cannot be altered or tampered with, providing a verifiable record of all licenses and their ownership.
- Decentralization: A DAO-based model for software licensing is decentralized, meaning that it is not controlled by a single entity. This makes it resistant to censorship and interference from third parties.
- Automation: Smart contracts automate the process of purchasing and distributing licenses, making it more efficient, legally predictable, and reducing the need for intermediaries.
- Security: The use of blockchain technology and smart contracts provide a high level of security, making it difficult for licenses to be counterfeited or fraudulently obtained.
- Ownership and Transferability: The token-based system allows for verifiable ownership and transferability of licenses, enabling users to transfer their license to others or resell it.
- Governance: The DAO is governed by its members, who can vote on important decisions related to the management and operation of the system, thereby giving more control and power to the community.
- Cost-effective: The automation and decentralization reduce the need for intermediaries and other associated costs, making the licensing process more cost-effective for both software developers and users.
- Flexibility: The smart contract's code can be updated and improved over time, which allows to adapt to changing circumstances and market conditions, making it more flexible.

A dataNFT-based model for the TRUSTS OpCo would create a decentralized system for managing and distributing costs / revenues. To begin with, a dataNFT-based cost/revenue sharing model and their terms of reference need to be defined. This could include the type and functionality of available software, the cost of operating each software component, and any restrictions on how the software can be used. The dataNFT then need to be deployed, making it publicly available for anyone to interact with.

Possible measures for mitigation of the above-mentioned disadvantages of using data NFT are:

- **Complexity:** The technology behind a DAO-based model for software licensing can be complex, making it difficult for setting up, managing and for some parties to understand and interact with the system. To mitigate the complexity of a DAO-based model for software licensing, companies can provide user-friendly interfaces, clear documentation, and training programs to help users understand and interact with the system. In cases of a dual governance model, it may be even more difficult to comprehend the system. Dual governance models can also be simplified and made more transparent to ease comprehension. The advantages of dual governance seem to outweigh the disadvantages of increased complexity.
- **Lack of regulation:** As the system is decentralized and operates outside of traditional legal frameworks, it may be difficult to enforce legal remedies in the case of disputes or breaches of contract. On one hand, token-based systems must operate within the legal framework of the jurisdictions they belong to. For example, if the ownership structure of a company is tracked through token ownership, this would be partly in violation of existing laws, as shareholders are typically required to be identifiable. Only stock corporations have anonymous shareholders, but they must still be non-anonymous for tax purposes. Therefore, the concept of a DAO is not easily covered by existing regulations.
  On the other hand, it is not established that smart contracts operate outside the legal system. Depending on the jurisdiction, blockchain-based transactions may still need to be conducted in compliance with the law. If this is the case, smart contracts that combine the will of multiple parties for transferring assets and data can be considered legally enforceable contracts. This also appears to be the prevailing view among EU legal scholars. To address the lack of regulation, the involved organizations can work with legal experts to ensure compliance with relevant local laws and regulations. Additionally, they can establish clear policies and procedures for dispute resolution and contract enforcement. Smart contracts can also be designed to include clauses that allow for legal remedies in case of disputes or breaches of contract.
- **Volatility:** The value of the cryptocurrency used to purchase licenses may be subject to significant fluctuations, which could make the cost of licenses unpredictable for users. To mitigate the volatility of cryptocurrency, stablecoins or other forms of digital currency could be used that are pegged to the value of

traditional currencies. Additionally, hedging strategies or other financial instruments could be used to protect against cryptocurrency fluctuations.

- **Smart contract bugs:** Smart contracts are self-executing code, hence a bug or a vulnerability can compromise the functioning of the system or even lead to financial losses. To mitigate the risks of smart contract bugs, thorough testing, and auditing of the used smart contracts before deployment could be conducted. Bug bounty programs could also be established to encourage the identification and reporting of bugs by third parties.
- **Limited adoption:** The adoption of blockchain technology and DAOs is still in the early stages, which means that the ecosystem of tools and services supporting them is still limited. This might hinder the wide adoption of the system. It is undeniable that blockchain technology and smart contracts are gaining widespread adoption in various industries. From finance and supply chain management to healthcare and real estate, the potential use cases for these technologies are vast and diverse. Furthermore, as more and more companies and organizations begin to see the value in utilizing blockchain and smart contracts, it is likely that we will continue to see an increase in adoption in the coming years. This narrative of starting small (in terms of revenue) but capitalizing on a promising trend in the long term is a common one in the technology industry and certainly applies to the growth and development of blockchain and smart contract use cases. As more and more businesses and organizations begin to understand the benefits of blockchain and smart contract technology, such as increased transparency, security, and efficiency, it is likely that we will continue to see a rapid increase in adoption across various sectors. Additionally, the growing interest in decentralized finance (DeFi) and non-fungible tokens (NFTs) has further fuelled the growth of blockchain and smart contract technology. The potential for these technologies to disrupt traditional systems and create new business models is enormous, making it a promising trend that is worth capitalizing on in the long term. The fact that big and small companies are investing in this technology is a clear sign that the industry is growing and that the interest in blockchain and smart contract technology is here to stay. To address limited adoption, partnerships with other organizations and entities could be developed to increase awareness and promote the use of their platform and / or DAO-model. Also, investments in the development of new tools and services could be made to support the ecosystem.
- **Scalability:** The current blockchain technology infrastructure is not yet able to handle large number of transactions at the same time. This could be a limitation for the scalability of the system. To mitigate scalability issues, new technologies such as sharding and off-chain scaling solutions could be developed / further researched (Sharding is a technique used to horizontally partition a database table, so that the data is split into smaller, more manageable chunks known as shards. Each shard can be stored on a separate server, allowing for more efficient and scalable data storage and retrieval. It is often used in distributed systems, such as blockchain networks, to improve the performance and scalability of the network. Off-chain scaling solutions, on the other hand, refers to a method of increasing the capacity of a blockchain network by moving some of the transactions and data off the main blockchain and onto separate, parallel systems. This can help to reduce the load on the main blockchain and improve its overall performance.)
- **Energy consumption:** The process of creating and maintaining of a blockchain network can be energy-intensive with some methods / technology used. This could be mitigated by choosing a blockchain technology which uses the new, energy-saving technology.
- **Technical expertise:** Setting up and maintaining a DAO-based system for software licensing requires a certain level of technical expertise, which could be a barrier for some software developers. To address the need for technical expertise, training and support for developers could be developed and provided, or service contracts with specialized companies that provide technical expertise in blockchain, and smart contract development could be established.

6.3.4 Building a Strong Foundation: Navigating the Structural, Organizational, Legal, and Technical Elements of a TRUSTS-DAO

This subsection is focused on the process of establishing a TRUSTS-DAO using dataNFTs in order to establish a sustainable agreement among the members of the TRUSTS consortium. The procedure outlines the steps necessary to identify and choose software components, define licensing and legal conditions, and create a framework agreement that regulates the use of the software by the TRUSTS OpCo and consortium members. Additionally, the subsection covers the functional and technical considerations for implementing a pricing or licensing model based on a decentralized autonomous organization, including the design of smart contract functionality, the use of token systems for license verification and management, and the development of user-friendly interfaces and access controls. The goal is to ensure that the TRUSTS-DAO is established and run in a sustainable manner and that the rights of all parties involved are protected.

Structuring the Organizational Framework of a TRUSTS-DAO

The TRUSTS consortium, to establish a sustainable agreement, adopts the procedure proposed for the establishment of a TRUSTS-DAO using dataNFT. This procedure model ensures that all members are on the same page with regards to the process of establishing the TRUSTS-DAO and its functioning and to ensure it is efficient and effective. To establish a sustainable TRUSTS-DAO, it is important to identify all the software components that will be used for the future TRUSTS Core System. During the TRUSTS project, a TRUSTS platform was developed as a first step in this regard. It is necessary to continue by compiling a list of software components (open source/proprietary software) that will be used. This will help identify any potential issues with the compatibility of software components and ensure that the TRUSTS platform uses software components that are reliable and secure.

After determining the software components that will be utilized for TRUSTS Core Services and Additional Services, it is essential to define the license and legal conditions under which the TRUSTS platform will be established and utilize the data NFT-based revenue and cost-sharing model. A distinction will be made as to which components are necessary for the basic operation of the platform ("must-have"), which could be included as a useful addition ("good-to-have") and which components are rather optional ("nice-to-have").

WP	Functional Context	Name of TRUSTS module / set of software components	Description
WP3	Smart contracts (T3.2)	Smart contract executor	Tool providing and executes smart contracts
WP3	Semantic layer (T3.4)	Vocabulary Management System	A UI where users can manage vocabularies that are to be use through the project
WP3	Semantic layer (T3.4)	Metadata Broker	Central metadata repository of the platform. Is compliant to the IDS communication protocol
WP3	Semantic layer (T3.4)	Metadata Storage System	The triplestore (database) where the metadata is actually stored in RDF format.
WP3	Semantic layer (T3.4)	Platform Interface	The base component of the user interface that each node in the platform will have, allows for onboarding searching and consuming assets.
WP3	Semantic layer (T3.4)	IDS Extension for CKAN	An extension that is required to make the CKAN platform interact with IDS components.

WP	Functional Context	Name of TRUSTS module / set of software components	Description
WP3	Semantic layer (T3.4)	Vocabulary Extension for CKAN	An extension that is required to have the CKAN platform software to use the vocabularies in asset onboarding
WP3	Semantic layer (T3.4)	TRUSTS Client	
WP3	Brokerage (T3.6)	Recommender system	Providing services to recommend connections between datasets, services and users
WP3	Transfer learning methodology		
WP4	De-anonymisation / anonymisation toolkit (T4.3)		
WP4	Metadata schema for data assets		
WP4	Protocol for metadata exchange		
WP4	Protocol for Private Set Intersection	PSI library PSIttacus	Java library that enables two parties to find identical data in their data sets without sharing the full sets with each other

Table 1213: Functional context of software components used in TRUSTS

WP	Functional Context	Name of TRUSTS module	Description	Software Components	Place of use	used by Partner	Licence type
WP3	Smart contracts (T3.2)	Smart contract executor	Tool providing and executes smart contracts	Hyperledger Fabric	Corporate Node	FHG	Apache License 2.0
WP3	Semantic layer (T3.4)	Vocabulary Management System	A UI where users can manage vocabularies that are to be use through the project	PoolParty	Central Node	SWC	Proprietary Licence
WP3	Semantic layer (T3.4)	Metadata Broker	Central metadata repository of the platform. Is compliant to the IDS communication protocol	Metadata Broker Core	Central Node	SWC	Apache V2
WP3	Semantic layer (T3.4)	Metadata Storage System	The triplestore (database) where the metadata is actually stored in RDF format.	Apache Jena Fuseki	Central Node	SWC	Apache V2
WP3	Semantic layer (T3.4)	Platform Interface	The base component of the user interface that each node in the platform will have, allows for onboarding searching and consuming assets.	CKAN	Corporate Node	SWC	GNU Affero General Public License
WP3	Semantic layer (T3.4)	IDS Extension for CKAN	An extension that is required to make the CKAN platform interact with IDS components.		Corporate Node	SWC	GNU Affero General Public License
WP3	Semantic layer (T3.4)	Vocabulary Extension for CKAN	An extension that is required to have the CKAN platform software to use the vocabularies in asset onboarding		Corporate Node	SWC	GNU Affero General Public License
WP3	Semantic layer (T3.4)	TRUSTS Client			Corporate Node	SWC	
WP3	Brokerage (T3.6)	Recommender system	Providing services to recommend connections between datasets, services and users	Know-Center ScaR recommender framework	Corporate Node	KC	Proprietary Licence
WP3	Transfer learning methodology						

WP	Functional Context	Name of TRUSTS module	Description	Software Components	Place of use	used by Partner	Licence type
WP4	De-anonymisation / anonymisation toolkit (T4.3)					RSA	The MIT License
WP4	Metadata schema for data assets					RSA	
WP4	Protocol for metadata exchange					RSA	
WP4	Protocol for Private Set Intersection	PSI library PSIttacus	Java library that enables two parties to find identical data in their data sets without sharing the full sets with each other PSI protocol if based on our solution for Mobile Private Contact Discovery, which itself uses the following resources: - The OT code is based on the public domain library libOTe by Peter Rindal. - Elliptic Curve operations are implemented using MIRACL. - Some of the binary circuits are based on ones from ABY. - The garbled circuit interface is inspired by FlexSC. - The used cuckoo filter implementation is cuckoofilter. - The implementation of LowMC is based on Picnic.		Corporate Node	KC, TUG, FORTH	Proprietary Licence
WP4	Compute-intense neural networks over several nodes (T4.4)					EMC	
WP3	Interoperability component					RSA	The MIT License

Table 1314: Functional context, used software components, place of use, responsible consortia partner and type of licence used in TRUSTS

After identifying and describing the license types used, a specification of the possible future license use will be drawn up - especially for proprietary licenses (such as pay-per-use, open-access, research, business, etc.). This will help ensure that the TRUSTS OpCo is using software that is licensed appropriately and that the licenses used do not conflict with the intended business model. A framework agreement is necessary to regulate the software components used by the TRUSTS OpCo and the consortium members (and possibly other providers). This will help ensure that the software used by the TRUSTS OpCo is used appropriately and that the rights of the software developers and other rights holders are protected. The contributors need to agree on the terms and conditions of the use of the software components. The Terms and Conditions will need to regulate the duration of the use, the payment structure, the rights of the rights holders, and the obligations of the TRUSTS OpCo. By having these agreements in place, the TRUSTS OpCo can ensure that it is able to use the software components in an appropriate manner and that the rights holders are protected.

The TRUSTS partners need to sign a binding agreement that regulates the use of the software components by the TRUSTS OpCo. The contractual aspects will be part of the TRUSTS-DAO dataNFT, as described above. This dataNFT-stored legal agreement will be a key document that will govern the functioning of the TRUSTS platform using the dataNFT method. It will be the foundation of the trust and the legal framework of the TRUSTS-DAO. The agreement will also state the terms of use and the rights and obligations of the members of the TRUSTS-DAO, which will help ensure that the TRUSTS OpCo is established and run in a sustainable manner.

Implementing a TRUSTS-DAO: Functional and Technical Considerations

In addition to the actual steps for implementing a pricing or licensing model based on a decentralized autonomous organization, there are various functional necessities that must be considered in order to implement this model.

The functionality of a smart contract must be clarified. This must be designed in such a way that the acquisition and distribution of licenses and the creation and management of license tokens can be handled. Functions for verifying the authenticity of licenses, tracking ownership or enforcing the terms of the license agreement must also be added. Then, the functionality of the token must be considered. The token used for the licensing system must be designed in such a way that it is unique, verifiable, and also transferable. It should be possible to store it within the blockchain, thus also ensuring permanent proof of ownership. As a digital certificate, a token confirms the identity of the respective user and must therefore not have any security gaps. The verifiability of the token can be achieved, for example, by using a digital signature or encryption technologies. The token often contains information such as the name of the user, the validity period or even a digital signature created by a trusted authority. The opposite system (recipient of the token) verifies this information. The token can be transmitted via secure network connections such as HTTPS.

The next step is to consider the user interface. The system must have a user-friendly interface enabling the user to interact with the smart contract and acquire licenses. Examples include web-based interfaces or mobile applications. A user-friendly interface is characterized by intuitive operation or quick and easy access to the required functions. In most cases, these are clearly structured, clearly laid out and show easy-to-use buttons with help functions. The existing examples (such as Ocean, DataUnion) provide good practice in that regard. In parallel, access controls play a major role. These should provide a way to control access to the software based on the license token. It is conceivable that this could be integrated into the software itself or by means of a separate access control system.

In the area of automation, the aim is to automate the system as much as possible. This would ensure an efficient design of the process. Examples of this are the automatic verification of the authenticity of licenses, the distribution of licenses or even the distribution of the tokens themselves. Other positive aspects include increased time savings, increased accuracy or increased productivity, and reduced costs. Efficient automation performs recurring tasks quickly and efficiently, reduces human error, performs multiple tasks simultaneously and with consistent quality, allows processes to be adjusted quickly, and supports consistent monitoring of the system. However, the ability to analyse data stands out the most, as it allows a large amount of data to be analysed and interpreted as quickly as possible.

To be available to many users and to be able to handle many transactions, the system has to be scalable. Scalability allows for parallel growth to many users while adapting to emerging challenges. Scalable systems allow operators to avoid replacing a system altogether, but easily allow for extensions or the addition of more components. In turn, of course, rapid deconstruction is also possible. For security issues, the system should have robust security measures in place to protect against hacking or other forms of threat. Examples include the implementation of extensive encryption or security protocols to protect user data or transactions.

For the timely detection of anomalies and the timely initiation of countermeasures, the establishment of a monitoring system is essential. From a constant overview of the system's performance to the detection of threats or even the control of compliance guidelines, this point must be permanently anchored within the software. Corresponding capacities must also be provided around associated reporting or analyses.

By collecting, processing, and preparing data assets, it can be merged into simple reports or charts. Tools for analysis can be used in various ways, depending on the requirements of the company. Starting with reporting, real-time monitoring or even notifications. A business intelligence tool could be integrated into a data exchange platform as an additional function for business users to create insights from the exchanged data. This can be done by connecting the data exchange platform to the business intelligence tool through an API (Application Programming Interface) or with specialized connectors or by integrating these functionalities in future software versions. This will allow the business intelligence tool to access and analyse the data that is

being exchanged on the platform. Additionally, the business intelligence tool can be configured to automatically pull data from the data exchange platform at specific intervals, ensuring that the insights generated are always up to date.

Once the data is connected, business users can create reports, charts, and other visualizations to gain insights into the data. The business intelligence tool can also include features such as data modelling, data mining, and statistical analysis to help users discover patterns and trends in the data. The business intelligence tool can be integrated with other tools and platforms such as data visualization software and machine learning platforms to provide even more advanced analytics. When it comes to integrating the system, it is important to note that the ability to seamlessly exchange data between systems and applications is crucial. Not only does it increase the usability of the system for the users and participating organizations, but it also makes it more attractive to other software providers or partners. This is an important requirement to consider when implementing a system like this, as it ensures that the system can perform its intended functions and provide a seamless user experience.

A constant exchange of data between systems and applications not only increases the participants own usability of the TRUSTS system, but also its attractiveness to other potential and future providers of software and / or (data) services. These functional necessities are crucial to ensure that the system can perform its intended functions and provide a seamless user experience.

The system should also have robust security measures in place to protect against hacking and other forms of cyber-attacks. By considering the protection against unauthorized access, the loss of data or the prevention of any damage, IT security contributes significantly to the security of the business and, consequently, the loss of profits. A well-functioning security policy strengthens customer confidence and ensures uninterrupted business operations. Establishing this could include implementing encryption and other security protocols to protect user data and transactions. The developer should have a plan in place to maintain and support the system, including monitoring for bugs and vulnerabilities, providing technical support to users, and making updates and improvements as needed. This could include implementing encryption and other security protocols to protect user data and transactions. Security is a crucial aspect of any blockchain-based system and should be given the highest priority to protect user's data and transactions. The system should be designed to handle many users and transactions and should be able to scale as the user base grows.

Implementing a TRUSTS-DAO: Business and Organizational Considerations

In addition to the functional necessities, there are several business necessities that should be considered when establishing a decentralized autonomous organization (DAO) based model for software licensing. To start with, the business model should be clearly defined and should be designed to generate revenue for the software developer. This could include charging for licenses, offering paid upgrades or support, or implementing a token-based system for revenue sharing. The issue of user experience gets a major role in this context. This is crucial to ensure that the product is easy to use and meets the needs of the target group. For example, simple navigation determines whether users quickly find the functions and menu items they are looking for. The use of simple hierarchies, intuitive buttons or menus greatly simplifies the navigation. Similarly, the use of simple and precise language allows information to be provided quickly to all users. Visual aids or even opportunities for collecting feedback and troubleshooting also speed up general problem solving.

While the issue of scalability has already been mentioned within the functional needs, it also plays a special role from an economic perspective. A scalable system allows the company to quickly respond to growing business needs, adding the necessary resources without having to deal with complex or costly updates. This directly reduces the company's costs and ensures constant efficiency of business processes. A scalable system strengthens the confidence of all customers in the existing IT infrastructure, prevents failures and immediately provides sufficient capacity in the event of a rapidly growing customer base.

TRUSTS Software Developer Community engagement is crucial, and the developers of the TRUSTS-DAO should engage with the community by providing support, gathering feedback, and working on implementing improvements. Community engagement is crucial for any successful development of sustainable software,

as it allows for feedback and suggestions from the users, which can help to improve the system and increase its adoption rate. Therefore, social aspects such as possible community involvement should also be considered. Public visibility not only leads to increased attractiveness as an employer, supplier, or partner, but can also be used as a further way of retaining potential investors. Especially regarding partners in the healthcare sector, a social and responsible image promotes brand awareness. The admins of the TRUSTS OpCo should further have a plan in place to maintain and support the system, including monitoring for bugs and vulnerabilities, providing technical support to users, and making updates and improvements as needed. Maintenance and support are crucial for any blockchain-based system, as it ensures that the system is functioning correctly and that any issues are addressed in a timely manner.

The TRUSTS Opco then should design and set the token economics in a way that aligns with the business model and incentivizes the participants – and possibly also the user of the TRUSTS platform – to participate and contribute to the ecosystem. By taking these business necessities into account, the dataNFT-based model for software licensing can be established in a way that is efficient, effective, and sustainable for TRUSTS OpCo.

Implementing a Legal Framework for the TRUSTS-DAO: A Guide to Establishing the TRUSTS Decentralized Autonomous Organization

The legal requirements for a dataNFT-based model for software licensing can vary depending on the jurisdiction in which the system is being used. However, there are a few key legal considerations that should be considered. The legal status of smart contracts and their enforceability can vary depending on the jurisdiction. It is important to understand the legal framework surrounding smart contracts in the jurisdiction where the system will be used and to ensure that the smart contracts and the licensing terms are compliant with local laws. This includes understanding any legal requirements for the formation, execution, and performance of smart contracts, such as the need for a digital signature or notary, and the rights and obligations of the parties.

Tokens used in the system may be classified as securities, commodities, or other types of financial instruments, and may be subject to securities regulations. It is important to understand how tokens will be classified in the jurisdiction where the system will be used and to ensure that they are compliant with local laws. This includes understanding the regulatory requirements for the issuance and distribution of tokens, such as registration and disclosure requirements. The licensing agreements should be compliant with the local laws and regulations. The terms of the agreement, including the rights and obligations of the parties, should be clearly defined in the smart contract and should be compliant with the local laws. This includes understanding the legal requirements for the formation, execution, and performance of a licensing agreement, such as the need for a written agreement, the rights and obligations of the parties and any legal remedies available to the parties in case of a breach of the agreement.

The system must also comply with national and EU consumer protection laws, such as requirements related to providing clear and accurate information about the software, the terms of the license, and the process for purchasing a license, which would be applicable to transactions carried out between businesses and consumers (B2C) via the TRUSTS platform. The system should then be compliant with local tax laws, including any taxes that may be due on the purchase or transfer of licenses. This includes understanding the tax implications of the purchase or transfer of licenses, such as sales tax, value added tax, and income tax. If the system is intended for use in multiple jurisdictions, it may be necessary to consider the laws and regulations of each jurisdiction separately.

To comply with anti-money laundering (AML) regulations, the system should have a process for verifying the identity of users and for detecting and reporting suspicious activity. This includes understanding the legal requirements for the Know Your Customer (KYC) and AML process, such as the need for user identification and the detection and reporting of suspicious activity and complying with these requirements. It is important to note that laws and regulations surrounding blockchain technology, smart contracts, and dataNFTs are still evolving and may vary from jurisdiction to jurisdiction.

Implementing a dataNFT-based structure for the TRUSTS-DAO: Technical considerations

After considering the functional, legal, and business aspects and necessities for building a software model based on the principle of the decentralized autonomous organization, the next step is to describe the steps for building the model itself. To establish a dataNFT-based model for software licensing, the following steps would need to be taken:

The first step is to design and create the draft for the development of the smart contract. This will be used for the licensing process and must contain the description for the purchase and distribution of the licenses as well as the creation and management of the license tokens. Firstly, the possible parties must be identified for this and recorded accordingly in the contract. The type of licensed technology, the type of use that the licensee envisages, must also be mentioned. The terms and conditions, i.e., the duration or validity of the license, the fees, and possible restrictions on the use of the model must also be specified. Rules for possible termination of the contract, including the possibility of early termination and consequences for breach of the contract by one of the parties, should also be noted.

For the subsequent use of the smart contract, it must be transferred to a blockchain network. This is conceivable by creating a new blockchain or providing a contract based on an existing blockchain. Within the blockchain network, digital records of transactions are stored. The individual transactions are strung together in blocks and the blocks are time-stamped. A reference to the previous block ensures that it is not possible to change the data.

Afterwards, the creation of the TRUSTS-DAO can be initiated. Approaches to establishing an existing DAO already exist and can of course be relied on further. The DAO would then be responsible for managing the smart contract and making decisions in connection with the system. In this interaction, it is possible to define the details, rules, and mechanisms of the DAO through the smart contract. Examples include control of members of the organization or decisions about the use of funds. Particular attention should be paid to the acceptance of new members. After smart contracts are published, they can join using transactions on the blockchain. After a successful joining, for example, voting or regular monitoring can be performed. The terms and conditions for licensing the software can then be specified. These influence, among other things, the number of available licenses, the cost of each additional license or any restrictions on the use of the software.

The number of available licenses must be constantly reconsidered and restructured. Reasons for this are resource constraints, quality controls, technical limitations or even aspects of product development. The development and maintenance of a software requires time and money, increasing with the number of users. If an infinite number of licenses are sold, the danger increases that continuous, error-free provision of the software is no longer possible. In parallel, the allocation of an infinite number of licenses increases the risk that satisfactory customer support or even attention to customer requirements can no longer be provided in sufficient form. Software solutions, for example using on-premises can only be installed on a limited number of devices, whereby the actual product development can also no longer keep pace with emerging customer needs or requirements. Once the smart contract is implemented and the DAO is created, the developer must promote the system to potential users. This could be done through various marketing and promotional activities, such as social media campaigns and community involvement. This can be combined with the actual user introduction. Here, users are given the opportunity to interact with the established smart contract and purchase the licenses. A web-based interface or mobile application can be used for this purpose.

In the context of user introduction, particular attention must be paid to providing early information to users and making all information about the technology known. The creation of documentation on the process or use, the preparation of test environments, or the provision of resources to combat potential problems in the use of smart contracts provide enormous support in this regard. Regular measurement of success rates helps to make adequate adjustments during the introduction. The final steps to be added are the construction of monitoring and maintenance modules for the software and aspects of collaboration with the community. The developer would need to monitor the system to ensure that it is functioning properly and to make any necessary updates or changes to the smart contract. Collaboration with the community means offering sufficient support needs, soliciting feedback, and participating in a steady delivery of improvements.

6.3.5 Setting up the TRUSTS Operating Company (OpCo)

Establishing a TRUSTS operating company (OpCo) is a crucial step in the successful implementation and operation of the TRUSTS platform. Careful planning, coordination, and execution are necessary to ensure that the OpCo can effectively manage and operate the platform. The OpCo must have a clear and defined exclusive role in the operation of the TRUSTS platform, including responsibilities such as managing and maintaining the platform, overseeing the development of new features and capabilities, and ensuring compliance with relevant laws and regulations.

The governance body, such as a board of directors or a governance council, would play a key role in overseeing and guiding the token-based decision-making process described in the sections above. This body would be responsible for ensuring that the decision-making process is transparent and considers the interests of all stakeholders within the TRUSTS consortium. They would work to ensure that the token-based system is implemented fairly and effectively, and that the organization is able to make informed and equitable decisions. The governance body would also play a role in making decisions related to the usage of resources and the allocation of incentives for members who contribute to the operation of the TRUSTS OpCo.

The governance body, whether it be a board of directors or a governance council, would be responsible for overseeing the overall operation and management of the TRUSTS OpCo. This includes setting strategic direction, making decisions on key initiatives and projects, and ensuring that the organization is operating in compliance with all relevant laws and regulations. One of the key tasks of the governance body would be to ensure that the token-based decision-making process is functioning effectively and in line with the principles of transparency and fairness. This would involve monitoring the use of tokens and ensuring that they are being used in a way that is fair and equitable to all stakeholders. Additionally, the governance body would be responsible for reviewing and approving any proposed changes to the token-based decision-making process, to ensure that it remains responsive to the needs of the organization and its members.

Another important duty of the governance body would be to review and approve the proposals and resource usage that is put forward by the members of the TRUSTS OpCo. This would be done to ensure that these proposals are in line with the overall strategic direction of the organization and that they are in the best interests of all stakeholders. The governance body would be responsible for ensuring that the use of resources is transparent and that any issues or concerns are addressed in a timely and effective manner. With the TRUSTS-DAO approach, this could also be decentralized and virtualized, especially for future development stages of the TRUSTS platform.

The OpCo must have a comprehensive business plan in place that outlines strategies and tactics for generating revenue, managing costs, and achieving long-term success. This plan should be regularly reviewed and updated as needed. The OpCo must also have a funding plan in place that ensures it has the necessary resources to operate and manage the TRUSTS platform. This could include securing funding from consortium members, venture capital firms, or other investors. With this step, the OpCo must interact with a wide range of partners and potential partners to broaden the base of shareholders. Applying the TRUSTS-DAO approach in a broader way could also include data producers and data consumers and other users of the TRUSTS platform in that funding process.

The operation of the TRUSTS platform requires a TRUSTS OpCo team with specialized skills, knowledge, and experience to effectively manage and operate the platform. This team should comprise individuals who possess expertise in various fields such as data science, data engineering, data security, software development, business management, and legal compliance. Additionally, robust security measures must be implemented to protect the platform and the data it stores from cyber-attacks and other security threats. These measures may include encryption, firewalls, and other security protocols. Furthermore, the OpCo must establish relationships with key stakeholders such as consortium members, regulatory bodies, and other relevant parties to ensure that the needs and interests of all stakeholders are taken into consideration. Additionally, the OpCo must establish an effective communication and engagement plan to effectively communicate and engage with TRUSTS users and TRUSTS-DAO members.

Summarizing the aforementioned aspects, it is necessary to set up a TRUSTS operating company (OpCo) to effectively manage the day-to-day operations of the platform. The following aspects should be considered when planning and establishing the TRUSTS OpCo:

Legal structure	It is crucial to choose a legal structure that is suitable for the operations of the TRUSTS platform. This could be a limited liability company, a partnership, or a corporation. It is important to consult with legal experts to ensure that the chosen structure is compliant with local laws and regulations and allows relying on the DAO-approach for operations.
Funding	The TRUSTS OpCo will need to be funded to cover expenses such as development, support, and maintenance. This funding could come from the consortium members, investors, or through the sale of tokens. It is important to have a clear funding plan in place before establishing the TRUSTS OpCo.
Governance	The TRUSTS OpCo should have a governance structure in place that allows for decision making and management of the platform. This could include a board of directors, a management team, and an advisory board. It is important to ensure that the governance structure aligns with the overall goals and objectives of the TRUSTS platform.
Compliance	The TRUSTS OpCo should have compliance measures in place to ensure that the platform is compliant with local laws and regulations. This could include compliance with data protection laws, anti-money laundering regulations, financial law, consumer protection law, competition law, and securities laws.
Operations	The TRUSTS OpCo should have a clear plan for the day-to-day operations of the platform, including marketing and promotion, user onboarding, and community engagement. It is important to ensure that the platform is user-friendly and easy to use for potential users.
Transparency	The TRUSTS OpCo should be transparent in its operations and decision-making. The usage of dataNFT as infrastructure for allocating and managing cost and revenue sharing increases the transparency of involvement and contributions.
Long-term plan	The TRUSTS OpCo should have a long-term plan in place that aligns with the overall goals and objectives of the TRUSTS platform. This could include plans for expansion, new features and services, and partnerships.

7 TRUSTS Platform Contractual Measures for IPR Protection

7.1 Introduction

In addition to the technical possibilities mentioned in the previous chapters to protect the IPR of the users of the TRUSTS platform, possibly the simplest and yet most effective possibility of protection is to conclude appropriate contracts with the users, to demand compliance with them and to punish violations. Since (raw) data are neither patentable nor protectable, nor are they protected by copyright in most cases, attention must be paid here to the special nature of data as a "thing without corporeality". Data can be owned, but one cannot acquire ownership of it. If someone steals a corporeal thing, most legal systems around the world have appropriate sanctioning mechanisms enshrined in law to recover the stolen property. Additionally, if a court order is in place, law enforcement agencies can be relied upon to recover the stolen property. This possibility does not apply to data assets, which are not regulated by a property law-type of regime, and it is much more difficult to simply enforce any legal claim.

If data assets have been stolen - for example by copying - the legal possibilities to enforce any legal claims are comparatively small. For this reason, it is necessary to resort to contractual arrangements to regulate the use of the TRUSTS platform and enable a certain degree of legal certainty. If certain actions are permitted and others are explicitly excluded, a contractual provision can, for example, be used to enforce a contractual penalty in the event of non-observance of the contract. Contracts are then up for enforcement and evaluation of compliance or non-compliance.

This aspect is easier to resolve in court than the question of who held which user rights or property rights in a data asset (which is handled differently throughout Europe). In the North American legal sphere, the threat of high contractual penalties (higher than the actual damage suffered by the plaintiff) in the event of breach of contract are a tested means of improving compliance with the contract. In the European legal sphere, these threatened contractual penalties are not enforceable to the same extent as in North America. According to the European understanding of the law, it is rather the damage incurred or lost profit that can be sued for. In the North American legal understanding, the threatened penalties can also be significantly higher than the value of the damage and therefore have a deterrent effect on any data thieves.

In this chapter we present two drafts of a "Code of Conduct for using the TRUSTS Platform" (CC) and "Terms and Conditions for using TRUSTS Services" (TC). The TC draft is deliberately without any specific penalties or deadlines because this will be the subject of further discussion in the consortium and within the future TRUSTS OpCo.

Draft	Name	Rationale
CC	Code of Conduct for using the TRUSTS Platform	General rules on the treatment and behaviour of users on the TRUSTS platform. As a rule, such a code of conduct does not contain any enforceable aspects. Nevertheless, it regulates the interaction of the users of the TRUSTS platform.
TC	Terms and Conditions for using TRUSTS Services	The TC governs the conditions under which the users of the TRUSTS platform conduct a transaction with each other. It regulates the rights and obligations of Data Providers (DP) and Data Consumers (DC) and defines the legal position of TRUSTS OpCo as a third party not directly involved in the transaction between the two.

The following chapters are first drafts of CC and TC and will need revision and enhancement in the second half of the TRUSTS project.

7.2 Draft “Code of Conduct for using the TRUSTS Platform” (CC)

A draft code of conduct for the use of the TRUSTS data exchange platform is presented below. This text is a framework for amicable cooperation. For a TRUST platform to be operated by a TRUST OpCo later on, this design of a CC must of course still be refined. At the latest by the time the TRUSTS platform goes live his is deemed necessary for the TRUSTS OpCo. Therefore this framework need to be supplemented and expanded to include sanctions and penalties.

7.2.1 Preliminary Remarks / Preamble

1. The amount of data available today, or the amount of data produced daily, has reached unprecedented levels. Data is collected in almost all areas of everyday life and work, especially in the industrial sectors. It is often claimed that data is the oil of the 21st century. Therefore, a thriving data market that develops from an ecosystem of data services is a crucial factor for employment and growth as well as for sustainable social stability and prosperity.
2. The availability of data as well as its effective and targeted use and utilisation are core enablers of success and are competitive advantages in many industrial sectors, value chains and organisational processes and thus are a decisive factor for production, in addition to labour and capital. However, already established data infrastructures are largely disconnected, which means that the usability of existing data is often low, and efficient data use is only possible with a great deal of effort and associated high costs due to the lack of interoperability. TRUSTS has set for itself the task of changing this.
3. Persons, organisations, or companies participating as data seekers or data providers in TRUSTS agree to be bound by this Code of Conduct. Only by accepting to be bound by this Code of Conduct may they gain access to TRUSTS. Data seekers and data providers exchange data on the exchange platform provided by TRUSTS or arrange such data exchanges. The operator of TRUSTS acts as the provider of the necessary infrastructure and provides services for refining, analysing, visualising, or merging data. It is the common goal of the participants to establish and promote an effective and targeted data exchange within the framework of the trading platform. Through allocation[37] and thus the exchange of the data, it is the common goal of the participating parties to improve and optimise the uses of these trading objects and thereby achieve the above-mentioned impact of a proper use of collected data - also outside the exchange platform and with effect for third parties.
4. To this end, TRUSTS participants will comply with this Code of Conduct as a voluntary commitment and will conduct themselves in conformity with the principles and rules of conduct set forth herein and the data exchange rules set forth below. In doing so, the participants are aware that TRUSTS can only achieve its goals if basic rules and forms of conduct are complied with.

7.2.2 Draft §1 General Principles

1. TRUSTS Participants are data seeker or data provider, or intermediaries (data broker or similar). They shall always act in accordance with the relevant legal provisions in all actions related to TRUSTS. They shall comply with the applicable standards of the General Data Protection Regulation (GDPR). The participants are aware of how consequential the collection and trading of personal data may be. The preservation of informational self-determination and the protection of privacy as well as the security of data processing are a core concern for TRUSTS. Transparency is one principle enshrined in the GDPR, hence if participants comply with the EU legal framework on data protection, they already commit to observing the principle of transparency.
2. This means disclosing the origin and intellectual rights of the exchange platform data when requested by TRUSTS. It is further agreed that any economic exploitation of data must be refrained from if it may

[37] „Allocation" here means the assignment of limited resources to potential users.

violate the fundamental rights of the data subjects. It must be ensured that the data was obtained from a credible source under legally sound conditions, including without violating the rights of third parties.

3. The users of TRUSTS services believe in the sustainable success of bidding and selling practices based on the principles of integrity, fairness, and partnership. In doing so, the participants fulfil their contractual obligations towards each other with the greatest possible care and professionalism.
4. Transparency about the origin and traceability of the collection process of the exchanged data and the operation of the Participants and TRUSTS OpCo is essential to the signatories of this Agreement. They recognise that the benefits of collected data can only be maximised if the process by which the data is collected is also traceable. As already laid out in the GDPR, it must be ensured, especially in data exchanging, that procedures for processing personal data are documented in a comprehensible manner. They should be documented in such a way that they can be retraced within a reasonable period. Those participants who act as customers on the exchange platform openly communicate their data requirements to enable the data providers to collect data in a targeted manner and ensure compliance with the purpose limitation and data minimisation principles.[38]

7.2.3 Draft §2 General Rules of Conduct - Respect / Discrimination

1. Participants shall act loyally, fairly, and responsibly towards each other and towards the TRUSTS OpCo. Honesty and integrity are further maxims guiding the participants' actions. The participants undertake to treat each other with kindness and patience. They are aware that their work is used by other people, organisations, and companies and that they themselves depend on the high-quality work of others. Every decision made by the participants affects the functioning of the exchange platform and indirectly also the entire sphere of influence of all participants.
2. The participants undertake to communicate with each other in a respectful manner. Differences of opinion are no excuse for unpleasant manners and misbehaviour. Conflicts of interest shall be prevented where possible with any endeavour and, if materialised, resolved on a factual level, if necessary, with the involvement of an impartial arbitration body, which may be the TRUSTS OpCo itself in the event of a conflict between participants. Participants recognise that respectful interaction promotes productivity and the achievement of their goals.
3. Harassment and other exclusionary behaviour by a participant or the partners of the TRUSTS project is not acceptable. This also applies to threats or disparaging language directed against other persons / organisations / companies - also in the form of discriminatory jokes - which includes racist and sexist expressions. The participants strongly condemn this kind of behaviour. Again, the signatories recognise that intra-company conflicts of this nature damage the reputation of TRUSTS as well, making it difficult to achieve its goals.
4. Every participant in TRUSTS has the right to be treated fairly, courteously and with respect. No one shall be discriminated against, favoured, harassed, or excluded on the Data Ecosystem and affiliated TRUSTS because of their ethnic origin, gender, religion or belief, disability or impairment of health, age, appearance, sexual identity, or other personal characteristics. The signatories respect the dignity and privacy of the natural and legal persons involved. Every participant has the right to be protected against discrimination and harassment.
5. The protection of the environment and the conservation of natural resources are of great importance to the participants. TRUSTS impacts the natural environment through CO2 emissions, water consumption and energy use. Participants will nevertheless continuously strive to reduce their impact on the environment by reducing their energy consumption as much as possible and by using raw materials responsibly.

[38] It is self-explanatory that a "Code of Conduct" is precisely not an obligation, but a declaration of intent. It is recommended to regulate the real necessary parts with the Terms & Conditions.

Finally, TRUSTS is also intended to serve environmental protection in its core purpose, in that the allocation of data is not only intended to maximise data use and thus economic growth, but also to contribute to research on environmental protection.

7.2.4 Draft §3 Conflicts of Interest

1. TRUSTS respects the organisational and entrepreneurial autonomy of its participants also regarding their business activities outside TRUSTS. On the other hand, TRUSTS expects all participants - as already formulated above - to behave fairly and loyally towards it and each other. Personal interests of the participants should influence their business judgement in connection with their activities on TRUSTS as little as possible. The participants therefore undertake to refrain from activities that could lead to a conflict of interests. If participants perceive a risk of a conflict of interest in any of their activities, they shall disclose this to TRUSTS OpCo and make good faith efforts to resolve issues amicably. The place of arbitration shall be within Europe and / or ideally under the jurisdiction of European Court of Arbitrations itself. The rules of arbitration shall be established according to applicable EU law.
2. Participants shall avoid dealing with third parties that may jeopardise the former's compliance with the principles of this Code of Conduct, the reputation of TRUSTS or the ability to serve a broad customer base, including those who use data generated and transferred in the data marketplace as end users. Employees who enter and maintain business relationships must pay appropriate attention to this.
3. Participants shall also ensure that participating companies take reasonable precautions and apply all the necessary measures to ensure that the Code of Conduct is also complied with by the employees acting in each case.[39]

7.2.5 Draft §4 Data Protection and Confidentiality

1. The confidential handling of data and information received by the Participants during business relations in connection with data exchange via TRUSTS is essential to the signatories. Accordingly, data and information shall be treated with the greatest possible care and confidentiality. The Participants, as responsible entities, shall ensure that the requirements of data protection, including data security, are observed.
2. Employees of the participants who are entrusted with the collection, processing or use of personal data shall be made aware of the particular importance of the strictest compliance with the GDPR and the overall EU data protection legal framework and shall be obliged to comply with it. They are informed by the company employing them that violations of data protection law may be prosecuted as an administrative offence or misdemeanour or under criminal law and may give rise to claims for damages. Possible sanctions under labour law must also be pointed out. The obligation to maintain data secrecy also applies beyond the employment relationship.
3. Participants shall collect, collate, process, use and store personal data only in accordance with legal requirements. They shall consider that the collection, storage, processing, and other use of personal data may be carried out only in accordance with EU data protection law, in particular the GDPR. All components of information processing must be secured in such a way that the confidentiality, integrity, availability, verifiability, and resilience of the information worthy of protection is guaranteed, and unauthorised internal and external use is prevented.
4. Participants shall recognise that the security of other data collected, gathered, processed, used, or stored shall also be ensured, against interference by third parties. Participants shall therefore comply with security standards so as not to jeopardise a core market objective of transferring data to where its benefits are maximised through data loss to third parties.

[39] The aim is to prevent a conflict of interest within a participant's company from spilling over to TRUSTS.

5. Finally, participants are strongly encouraged to assess their role regarding individual data processing operations (incl. data anonymisation), determine who is/are the controller(s), draw up appropriate arrangements between joint controllers if necessary, and arrangements with data processors they rely on.

7.2.6 Draft §6 Violations and Sanctions

Violations of this Code of Conduct may have legal consequences. TRUSTS OpCo may act against violations by individual participants by issuing warnings and terminations. Unless otherwise specified, a reasonable and customary period of notice must be given. TRUSTS OpCo also reserves the right to file criminal charges.

7.3 Draft „Terms and Conditions for using TRUSTS Services“ (TC)

7.3.1 Creation of this Draft Terms and Conditions (T&C)

In this chapter, a "General Contractual Terms and Conditions for using the TRUSTS Data Exchange Platform" (in short: "TRUSTS T&C" or "TC") is drafted and presented. This draft makes a proposal of potential T&C accompanying the TRUSTS platform when it enters operations.

This draft T&C is an attempt to summarise the results developed in the project and to provide a legal framework for further work on and with TRUSTS. This T&C was conceived and written with a view to later practical application in the real operation of the TRUSTS data market. It is self-evident that certain contract-relevant decisions on organisation and structuring can only be made ad-hoc after the entry into operations and were therefore left open in part during this research project. This means that corresponding clauses/formulations may have to be changed or adapted at a later stage.

Bearing in mind that at the time of this report it has not yet been finally clarified what legal form the future TRUSTS Operating Company (short: “TRUSTS OpCo”) will have, it was assumed for the formulation of this text that a legal entity will be established.

However, the draft text is formulated in such a way that the various legal forms of the operating company are equally possible. The draft TRUSTS T&C only regulates the relationship between the participants of the data exchange platform. It does not regulate the legal form of the operating company.

7.3.2 Draft §1) Definitions

(1) The term "TRUSTS Platform" (or TRUSTS for short) refers to the entirety of the systems, functions, and tools of the TRUSTS data exchange platform (“Trusted Secure Data Sharing Space” as funded project within the EU Horizon 2020 Programme. The platform services will be delivered only in trial operation, prototype, “beta” during the runtime of the project).

(2) “Data” or “Data Assets” are exchanged on the TRUSTS platform. Data Assets are any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording as files, raw data, data streams or other manifestation.

(3) „Exchanging Data“ means the act of exchanging data or metadata. If the data is shared based on contracts, it is “data sharing”. For data sharing, fees (subscriptions) may be charged for the provision of the services. "Data trading” means a data exchange, when data assets are treated like economic goods (offered, “bought”) and paid according to data-related billing models (x GB of data for price y).

(4) A participant in the TRUSTS platform (in short: "Participant") is a natural or legal person or organisation that is involved in any way as a provider (DP: data provider or "Seller") or consumer (DC: data consumer or "Buyer") or in any other function in exchanging, processing, enriching, analysing and computing data assets via the TRUSTS platform.

(5) A participant in the TRUSTS platform must go through an admission process ("Listing"). The purpose of this Listing process is to clarify the specific suitability of the participant for the use of the TRUSTS platform

(KYC – Know your client). While data seekers go through a simplified listing process, data providers must go through a more in-depth listing process depending on the type, amount, sensitivity, and nature of the data assets provided. After going through the onboarding process, a participant can provide data on the TRUSTS platform.

(6) TRUSTS distinguishes the following functional roles: Data Provider, Data Demander and (Data Market) Operator, where a Participant can be both: a Data Provider and a Data Demander. The functional roles differ as follows:
    (a) Data Provider (DP): a natural or legal person or organisation that wishes to offer data on the TRUSTS platform for exchanging with others. The TRUSTS OpCo may demand remuneration in return.
    (b) Data Consumer (DC): a natural or legal person who requests to receive data assets via TRUSTS platform and intends to use these data assets for his own. DCs obtain data (data assets) via the TRUSTS platform and use them within the scope of their rights of use for analysis or for further data processing.
    (c) Data Market Operator (TRUSTS OpCo): a legal entity which is the technical and administrative operator of the TRUSTS Platform. As the operating company, TRUSTS OpCo is responsible for the administrative and technical operation of the TRUSTS data exchange platform. For assuming the operator responsibility and for the running costs of the operation, the data market operator may charge fees and / or use other forms of cost allocation - for example through effort-based cost allocations or other forms of allocation.

7.3.3 Draft §2) Scope of the Terms & Conditions

(1) These Terms and Conditions govern the participation in the exchanging of data on the TRUSTS platform as well as the rights and obligations of the participating players in relation to TRUSTS OpCo.
(2) These Terms and Conditions shall apply to the business relationship between TRUSTS OpCo and all (trading) Participants, in particular the Data Providers (DP) and the Data Consumers (DC).
(3) These Terms and Conditions shall govern the resulting business relationship between TRUSTS OpCo and the Participants in a generally conclusive manner. Any deviating agreements between the parties must be in writing.
(4) These agreements shall enter into force without prejudice to the provisions of § 3 para. 2 or after the listing process regulated in § 6 has been completed.

7.3.4 Draft §3) The Operator: the TRUSTS Operating Company (TRUSTS OpCo)

I) Basics and Self-Conception

(1) TRUSTS OpCo shall promote and facilitate the operations necessary to the exchange of data.
(2) TRUSTS OpCo provides a technical infrastructure through which participants can exchange data. One part of the data ecosystem is the TRUSTS platform. Selected Data Providers (DP) and Data Consumers (DC) are admitted as participants to this platform.
(3) In its role as operator of the TRUSTS platform, the TRUSTS OpCo itself does not act as a market participant, but as an operator of the platform itself. The data exchange participants conclude the exchange contracts among themselves. If not explicitly stipulated in relevant European laws, TRUSTS OpCo does not become a part of a data asset exchange contract but provides the data asset exchange infrastructure as an intermediary. In other cases, TRUSTS OpCo may be designated as data intermediation services under the Data Governance Act, if certain criteria are satisfied.

(4) The TRUSTS OpCo shall, however, be entitled to conclude contracts with DCs as commission agent for a DP or as representative of a DP.
(5) The TRUSTS OpCo shall provide the platform infrastructure necessary to enable interoperabel data exchange. Furthermore, the TRUSTS OpCo shall support the DPs in the settlement of contracts related to the exchange of data by offering a settlement system, providing data management services and consulting services (see services of the OpCo in § 3 No. II).
(6) To be able to carry out data- or volume-related settlements, the TRUSTS OpCo shall establish a monitoring system to accompany the data exchange on the platform. The results of the monitoring are the basis for the service settlements vis-à-vis the market participants. The monitoring system is to support the quantitative and qualitative settlement procedures and contribute to transparent, fair, and usage-based load sharing and settlement.[40]

II) Services of TRUSTS OpCo

(1) Provision of the data exchange infrastructure: TRUSTS OpCo shall ensure the functionality of the platform. TRUSTS OpCo shall ensure that the functionality of the exchange platform is restored as quickly as possible by taking preventive and follow-up measures in the event of force majeure, riots, acts of war or natural disasters or other events for which TRUSTS OpCo is not responsible (e.g., unavoidable power failures, strikes, lockouts, orders by public authorities).
(2) Billing service: The data monitoring system of TRUSTS OpCo enables the usage-based billing of the services. TRUSTS OpCo provides users with a easy-to-use usage-based billing service that participants can use. The DP and DC, as providers and consumers of data assets, have a great interest in a comprehensible usage-based billing. If the participants make use of the billing service, the following shall apply:
    a. To be able to use the settlement service, the participants register with a user account at TRUSTS (specified as DP/DC). By assigning the data transactions to a user account, the exchange activities are recorded and thus made billable. In connection with the user accounts, the participants provide TRUSTS OpCo with contact and invoice data, VAT numbers and other necessary data upon request. In addition, upon request, participants shall provide other information such as customer service contacts, general profile information on the organisations, and other information required by law or requested by TRUSTS OpCo for the provision of the service, etc.[41]
    b. By using the settlement services, TRUSTS OpCo is authorised to retain, receive, or disburse funds in accordance with payment instructions (subject to the terms of this Agreement). In this capacity, the TRUSTS OpCo is neither a Data Consumer (DC) nor a Data Provider (DP) in respect of the data assets exchanged and will not be a party to any contracts between the DP and DC. The DP is the responsible party for provision of data assets. TRUSTS OpCo will also not act as trustee or fiduciary. It does not accept deposits or issue loans.
    c. If the DP uses the settlement service, TRUSTS OpCo will process payments and refunds of transactions submitted through the service, subject to the terms of this agreement. The DP is responsible

[40] A monitoring system is also necessary for free data exchange so that the entire trading system receives legal and technical information about the operation. It is pointed out here that it still needs to be examined whether and if so to what extent personal data should be analysed or logged here. It is suggested that a transparent and secure monitoring solution be implemented for this purpose.

[41] At this point, for a future version of the T&C, consider removing the following: Provision of information requested by the DMT; profile information on organizations. Suggested clause, if applicable: "In addition, market participants shall make available on other information such as customer service contacts."

for providing to the TRUSTS OpCo all necessary legal information for the data exchanged. This is done so that TRUSTS OpCo, as the operator of TRUSTS, is always immune from liability and can also warn against and sanction any infringements of copyright or other rights by participants (such as exchanging unlicensed data). Data providers (DPs) are obliged to be especially transparent regarding the legality of the data provided. They are obliged to provide all necessary information correctly and completely.

d. TRUSTS OpCo undertakes to settle data exchange transactions without delay. If the settlement date of a data asset transaction is not the same as the due date of the related debt, TRUSTS OpCo shall determine, in accordance with applicable law, the date on which the payments of the transactions must be settled or from when a due date occurs.[42]
e. Furthermore, the TRUSTS OpCo shall, if possible, provide the participants concerned with information on the reasons for the rejection to enable them to rectify any factual errors that led to the rejection. Transactions that have been duly initiated or authorised will be settled without delay / as soon as possible / within period ‘x’.
f. To ensure the smooth and uninterrupted operation of TRUSTS, the OpCo is dependent on sufficient cash flow. TRUSTS OpCo may therefore require that either a minimum balance is maintained in the User Account or that a separate reserve account (a "reserve") is established for services used to secure the fulfilment of payment obligations under this agreement. Further, TRUSTS OpCo may restrict transactions to or from a provider account in such amounts and for such periods as it reasonably deems necessary for its protection or the protection of other Users if: (1) it is exposed to financial risk; (2) the participant has breached one or more terms of this agreement; (3) there is a dispute in connection with the provider account or a related transaction; or (4) it is necessary to do so to ensure the security of the trading platform's systems.
g. TRUSTS OpCo or an affiliate thereof will provide participants using the settlement service with summaries of their account activity. Except as required by law, the user account holder is solely responsible for (a) establishing and maintaining current records of all transactions and (b) reconciling all payment activity to and from the account. TRUSTS OpCo is under no obligation to store, retain, report, or otherwise provide copies of or access to any records, documents or other information relating to the user account or any transactions.
h. In processing payments, TRUSTS OpCo may use the services of one or more third parties to provide the service and process transactions.
i. Participants agree to pay the applicable fees from time to time. The fees shall be in accordance with the TRUSTS Fee Schedule and shall include, at a minimum, the cost of the transactions and any other applicable charges. TRUSTS OpCo reserves the right to change the fees at any time. In the event of a change in fees, participants may terminate their use of the settlement service. The procedure is governed by § 3 para. 2 lit. J.
j. To the extent permitted by law, TRUSTS OpCo may set off any debt owed by a participant to it, fee debts, against any reserve or proceeds owed or debit a participant's bank account or other payment

[42] Note: depending on the chosen business model of the TRUSTS or on the amount and complexity of the data exchange transactions, the settlement date and the maturity of the debt may not coincide. The OpCo should strive to keep this delta as small as possible. On securities exchanges, however, this clearing process sometimes takes hours or even days. The entire clearing process is still under discussion in the TRUSTS project. However, as a precautionary measure, this corresponding section should be provided at this point. More precise regulations can only be made when the business model is further advanced and in particular the clearing process can be more closely defined.

instruments with it. All set-off items will be calculated at the time of settlement of a transaction by TRUSTS OpCo and deducted from the funds transferred or collected. If the participant owes TRUSTS OpCo an amount higher than any credit balance on the user account, TRUSTS OpCo may debit the participant's bank account after payment has not been made in response to an invoice from TRUSTS OpCo within a period of one week. In addition to the amount collected, the participant shall be held liable and shall pay to TRUSTS OpCo, on account of TRUSTS OpCo, its costs in connection with the collection of the amount, including any attorneys' fees, court costs, collection agency fees and accrued interest.

(3) The participant may terminate the use of the billing service and/or this agreement at any time. Termination shall result in the closure of the user account. Upon closure of the account, all unsettled data exchange transactions will be cancelled. Any remaining balance may be redeemed less any amounts owed to TRUSTS OpCo.

III) Limitation of Liability

(1) TRUSTS OpCo shall be liable for damages culpably caused by a breach of its material contractual obligations under these terms and conditions. However, in the case of slight negligence, the liability of TRUSTS OpCo is limited to the amount of the foreseeable damage typical for the contract. This shall not affect the mandatory statutory liability, in particular in the event of culpable injury to life, limb, and health (personal injury).

(2) TRUSTS OpCo shall not be liable for damages that occur because of force majeure, riots, acts of war or natural disasters or because of other events for which it is not responsible (e.g., strikes, lockouts, orders by sovereign authorities) or that are attributable to technical problems that are not culpably caused.

(3) Furthermore, TRUSTS OpCo shall not be liable for damages incurred by the participants in their contractual relationships with each other.

7.3.5 Draft §4) Data Exchange System and Currency

(1) TRUSTS OpCo shall determine the currency for services and settlements. It may determine that data assets are settled in multiple currencies.

(2) Unless otherwise specified, the service and settlement currency shall be the EUR.

(3) If a service or settlement currency other than the EUR is also permitted, the conversion of EUR into foreign currencies shall be based on the euro foreign exchange reference rate of the European Central Bank, unless otherwise provided. The Participants reserve the right to deviate from this rule in their contractual relationships with each other.

(4) If digital forms of payment / cyber money are also permitted as currency, TRUSTS OpCo shall determine the form of settlement or the link to generally applicable reference rates.

7.3.6 Draft §5) General Duties to Cooperate

(1) Notwithstanding any special services and performance obligations under these Terms and Conditions, the participants are obliged to cooperate to a reasonable extent in the orderly conduct of data exchange on the exchange platform and the business relationship between the Participants.

(2) This obligation includes the immediate disclosure of all information / specifics about TRUSTS OpCo of which they become aware that are necessary for the proper conduct of the business relationship in accordance with these Terms and Conditions and / or the proper trading and / or settlement of the data assets included in the TRUSTS platform.

(3) Furthermore, the participants shall ensure the timeliness, accuracy, specificity, and consistency of such communications.

7.3.7 Draft §6) Participation in Data Exchange / Listing Process

(1) All participants undertake to comply with the "TRUSTS Code of Conduct".
(2) All natural and legal persons and organisations that have been authorised by TRUSTS OpCo to participate and have been granted access to the TRUSTS platform are entitled to participate in data exchange on the platform. Access to the infrastructure shall be granted in accordance with the applicable provisions and the decisions made on this basis by TRUSTS OpCo.
(3) As a rule, all participants shall be subject to a suitability test (due diligence) prior to data exchanging. This due diligence shall include a review of the participant regarding the Participant's trustworthiness and credibility. Participants shall provide TRUSTS OpCo with the information relevant for the due diligence. The participants guarantee that the information provided is complete, correct, and free of contradictions. TRUSTS OpCo is entitled to make enquiries, both directly and via third parties, which it deems necessary to verify the information provided by the applicant, including consulting commercial databases or creditworthiness information. Here, the cost and benefit of a credit report must be weighed up in each individual case. From a certain turnover in data exchange onwards, a credit report must be carried out.[43]
(4) In addition to clarifying legal and administrative issues, the suitability test prior to data exchange is also particularly concerned with proving that a participant can appropriately and securely handle the data to be exchanged and is committed to doing so. It must be ensured that all aspects relevant to data protection are comprehensively considered and that the data to be exchanged are secure and uncompromised from third parties during exchange, transport and storage or further processing.
(5) In addition to organisational credibility, data providers must also prove that they are in legal possession of the data to be exchanged and that they are also allowed to exchange it (this includes clarification of licensing issues before exchange begins).
(6) After sufficient verification of the participants, the TRUSTS OpCo shall decide on the granting of permission to exchange data on the TRUSTS platform.
(7) TRUSTS OpCo may refuse to grant permission for data exchange on the TRUSTS platform if there are justified circumstances concerning the person or organisation of the participant which give reason to suspect that the principles of data exchange or the law are not being observed or if it is to be expected that this could lead to damage to the reputation of TRUSTS.
(8) TRUSTS OpCo may also refuse or withdraw permission to exchange data via the TRUSTS platform if participants exchange in data assets that are pornographic, glorify violence, are defamatory or otherwise contrary to common decency. Exchanging or providing links to such offers may also result in exclusion from data exchange via TRUSTS. In the event of justified suspicion, the participant must prove in detail in each individual case that no damage has been caused to TRUSTS.[44]

[43] For larger providers, there will also be a listing procedure that is based on the listings of securities exchanges.

[44] This paragraph enables OpCo, for example, to keep providers of link collections away from the data exchange platform. It cannot be ruled out that legal or illegal link collections become interesting for such providers as tradable data, and they prefer to use TRUSTS rather than their own platform. OpCo must have knowledge of what is being exchanged on TRUSTS to be able to curb abuse.

(9) Participants are obliged to notify TRUSTS OpCo immediately after becoming aware of the occurrence of damaging behaviour or the cessation of the above requirements (§ 5). This applies if insolvency proceedings have been opened against the participant.

7.3.8 Draft §7) Data Exchange, Data Transmission and Archiving

(1) If a data exchange is concluded via the TRUSTS platform, the data exchange participants undertake to fulfil the obligations incumbent upon them under the respective contract in accordance with the T&R and CoC.
(2) The data provider (DP) undertakes to transfer the data assets to the data consumer (DC) for use and / or for utilisation in accordance with the agreed transfer of use.
(3) After the exchange has been concluded and after the data assets have been transmitted or made available, the DP undertakes to notify TRUSTS OpCo of the transmission or of the making available without delay. For this purpose, only information on the exchange itself is transmitted, but not the data itself (this is only exchanged between the DP and the DC).
(4) To be able to ensure the overall quality operation of the TRUSTS platform, the TRUSTS monitoring system will learn from the metadata the most important key information about each data exchange.
(5) The data exchange Participants undertake to comply with the general and statutory compliance rules and the Code of Conduct.
(6) The Participants agree:
    a. that the use of the exchange platform does not violate applicable legal provisions and any contractual provisions;
    b. that the rights of third parties (e.g., copyrights, patent, and trademark rights) are not infringed in the case of all data assets offered and exchanged and that the applicable criminal laws of the jurisdiction, where TRUSTS OpCo is registered are complied with
    c. that they will fully apply the requirements related to data protection and data security; and
    d. that participants are obligated to notify TRUSTS OpCo of any difficulties in the performance of contracts for the purchase, use or transfer of data. In doing so, the Participants shall describe the difficulties as precisely as reasonably possible and shall ensure the completeness and accuracy of the information.
(7) Participants in data exchange are obliged to promptly inform TRUSTS OpCo before, during and after the entire duration of the exchange of all circumstances relevant to the orderly services or settlement of TRUSTS business, provided that the participant has knowledge of such circumstances or can reasonably obtain knowledge of them through generally accessible sources of information.
(8) The DP warrants that it holds the necessary rights to the data to be exchanged (sole, one-time, permanent, etc.).
(9) The DC undertakes to perform the obligations arising from the data exchange in accordance with the contract. This includes, among other things, that upon receipt of the purchased data or upon provision of the data for use by the DP as contractual partner, the DC is obliged to pay the TRUSTS OpCo the agreed purchase price or the agreed use fee in due time.

7.3.9 Draft §8) Fees for the Use of the Exchange Platform TRUSTS

(1) TRUSTS OpCo shall provide the Participants of the TRUSTS platform with the infrastructure necessary for data exchange and the participants shall pay TRUSTS OpCo a fee in return for the provision of the data exchange infrastructure.
(2) The amount of the fees or charges shall be determined and set by TRUSTS OpCo. They shall be listed in a publicly accessible separate schedule of charges. Changes in the cost structures of the operation shall

have a direct impact on the apportionable fees. TRUSTS OpCo reserves the right to change the amount of the respective fee. TRUSTS OpCo shall notify any changes to the schedule of fees in writing in good time.

(3) Fees for the licensing or provisioning of data assets, as they typically arise between the data exchange partners DP and DC are determined in the contractual agreements between DP and DC.

(4) TRUSTS OpCo may provide for the following non-exhaustive list of fee categories in the fee schedule:

   a. Fees for the provision of the data exchange infrastructure ("service provision");
   b. Fees for the provisioning and exchanging of data assets ("pay-per-use"); and
   c. Fees for other services provided by TRUSTS OpCo such as: Billing services, consulting services, assumption of data management, data stewardship or other types of data processing / auditing.

7.3.10 Draft §9) Sanctions and Termination

(1) In the event of a culpable breach of contractual obligations under these Terms and Conditions, TRUSTS OpCo is entitled to issue a warning to the participant. TRUSTS OpCo reserves the right to issue a warning for a breach of other obligations under these Terms and Conditions.

(2) TRUSTS OpCo is free to impose contractual penalties. These penalties need to be provided for in the contract between the participants and TRUSTS OpCo - i.e., different from penalties potentially provided.

(3) TRUSTS OpCo may terminate the entire business relationship or individual business relationships under these Terms and Conditions with a participant for good cause. Good cause shall be deemed to exist if TRUSTS OpCo cannot reasonably be expected to continue the business relationship, even considering the legitimate concerns of the participant. An important reason exists if:

   a. the participant violates essential contractual obligations arising from these Terms and Conditions after a fruitless warning; or
   b. if it is established that there are circumstances in the person or organisation of the participant which impede the proper running of TRUSTS or jeopardise its public reputation; or
   c. circumstances subsequently arise in the person or organisation of the participant which prevent that person or organisation from continuing to fulfil the requirements of § 6.

(4) A Participant in the TRUSTS data exchange platform may terminate the contractual relationship under these Terms and Conditions at any time. Existing or still to be performed obligations shall be fulfilled or settled after the date of termination of the contractual relationship.

7.3.11 Draft §10) Dispute Resolution Procedure

(1) In the event of a dispute of any kind between Participants, a dispute resolution procedure involving TRUSTS OpCo may be initiated by one of the Participants. The objective is to resolve and settle issues amicably and, if necessary, rely on using arbitration. If not specified elsewhere the law of Belgium and the Court of Brussels shall be competent for all issues not settled amicably or via International Arbitration.

(2) TRUSTS OpCo will not act as a party's representative in resolving disputes where the matter has been referred to it. However, TRUSTS OpCo will attempt to resolve disputes by facilitating good faith communication between the parties.

(3) The filing of a complaint regarding any parties involved in the data exchange may be made at any time by the Participants.

(4) Upon receipt of a complaint, TRUSTS OpCo shall contact the participant about whom a complaint has been received and shall subsequently cooperate in bringing about a resolution. Participants who have

become the subject of a complaint procedure are obliged to submit comments to TRUSTS OpCo immediately upon receipt of a letter. This is intended to expedite the resolution of the dispute. If TRUSTS OpCo contacts the complainant for further information, the complainant must respond within three business days, or the complaint may be terminated. Dispute resolution outside of this complaint procedure is reserved to the parties, without prejudice, to their notification obligations to TRUSTS OpCo.

7.3.12 Draft §11) Miscellaneous

(1) All business relations under these Terms and Conditions shall be governed by the law of the jurisdiction, where the TRUSTS OpCo is established if not otherwise regulated by EU law.
(2) The exclusive place of jurisdiction for all disputes in connection with these Terms and Conditions is the registered office of the operator (TRUSTS OpCo).
(3) All data processing operations are defined as within the territory of the European Union. The EU data protection legal framework is fully applicable to personal data processing operations carried out in relation to the TRUSTS platform.
(4) TRUSTS OpCo reserves the right to decide on changes to the Terms and Conditions. Changes to these Terms and Conditions will be presented to the participants in writing or electronically no later than [x weeks] before they take effect. They shall be deemed to have been approved if no participant notifies TRUSTS OpCo in writing or electronically of any objection before the date on which they take effect. TRUSTS OpCo will make specific reference to this approval effect in its offer.
(5) In the event of non-recognition or revocation of the data exchanging permit pursuant to § 6, TRUSTS OpCo may terminate the business relationship with the Participant with six weeks' notice.
(6) Termination for good cause shall remain unaffected.
(7) The amended Terms and Conditions shall be sent to the participants immediately after their resolution for their information and perusal. If they are not objected to within x weeks, they shall be deemed accepted.
(8) Should individual provisions of these terms and conditions be invalid or unenforceable or become invalid or unenforceable after the conclusion of the contract, the validity of the remaining terms and conditions shall remain unaffected. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision whose effect comes as close as possible to the objective pursued by the contracting parties with the invalid or unenforceable provision. The above provisions shall apply mutatis mutandis if the Terms and Conditions prove to be incomplete.

8 Concluding Thoughts and Recommendations

8.1 Summary and Conclusions on IPR on Datamarkets

IPR have become an increasingly important aspect of the development and growth of data exchange platforms. The protection of IPR in these platforms is essential. And that is not easy, as direct protection of data assets as IPR is only possible for patented or copyrighted data assets. Other types of data assets cannot be directly protected, but only indirectly through protective measures and processes. Industrial data assets are not protectable by law, but only by protection mechanisms - such as password and encryption and other things TRUSTS worked on.

And that is precisely why it is not straightforward, as direct protection of data assets as IPR can only be achieved for patented or copyrighted data assets. Other forms of data assets can only be indirectly protected through protective measures and processes, such as system architecture, access control, encryption, and other security measures. The TRUSTS project has been dedicated to addressing these challenges and finding solutions to ensure the security and protection of these valuable data assets.

And of course, data providers want to protect the ownership and control of their data, while data consumers want to access and use data for their intended purposes. IPR protection in datamarkets has several challenges, including data security and privacy, data exchange agreements, and the management of IPR within the data exchange platforms.

In the context of data exchange platforms, IPR refers to the legal rights and protections that individuals and organizations have over their data, including ownership, control, and access to data. The protection of IPR is essential to ensure that data providers can maintain control over their data and to prevent unauthorized use or misuse of data. In this deliverable, we provided a comprehensive overview of IPR in data markets and outline the key findings and recommendations for further development of IPR in this context. This report summarizes the findings of the TRUSTS research project on IPR in data exchange platforms. The provided recommendations for the further development of IPR mechanisms is differentiated in midterm and long-term recommendations.

This deliverable issued mainly two types of mechanisms for IP protection: technical measures and contractual measures that need to be considered on a later stage of establishing the TRUSTS OpCo. Technical measures include securing IP both physically and digitally, data anonymization, and ensemble learning. The International Data Space Association (IDSA) approach is also offering several mechanisms to support the IPR protection, including the IDS metadata broker and the IDS Clearing House. In terms of contractual measures, the deliverable is offering a Code of Conduct for using the TRUSTS Platform and Terms and Conditions for using TRUSTS Services. The document concludes with recommendations towards the conceptualization of TRUSTS aiming at efficient and affordable IPR protection mechanisms.

The concept of mechanisms for protecting IPR in data exchange platforms is based on the idea of creating a supportive and secure environment that protects the rights of data providers. This involves the creation of four key pillars of protection: focus on data and analytics, focus on supply chain integrity, focus on coordination and integration, and focus on transparency and awareness. The focus on data and analytics is aimed at ensuring that data providers can control the use and access of their data. This involves the creation of secure data exchange mechanisms that can manage and monitoring the use of data. The IDSA-approach used within the TRUST project was exactly targeting this topic. The focus on supply chain integrity is aimed at ensuring that the data exchange process is transparent and secure. This involves the creation of secure data exchange protocols and the establishment of trusted partners within the data exchange ecosystem.

The focus on coordination and integration was aimed at ensuring that data providers can seamlessly integrate their data into the data exchange platform. This involves the creation of data exchange standards and protocols that are compatible with existing data management systems. The focus on transparency and awareness is aimed at ensuring that data providers are aware of the terms and conditions of data exchange and can

monitor the use of their data. This involves the creation of transparent and accessible data exchange contracts and the establishment of data protection and data privacy policies.

In this context, a concept was worked out which significance and necessity support on data governance and data stewardship for users. The TRUSTS platform on the other side was designed in a way to help data providers manage their data and ensure that their rights are protected by the beforementioned measures.

Furthermore, it was pointed out how important onboarding services and the initial support of users in the use of data exchange platforms are. TRUSTS concepted support services for data providers, including the onboarding of data providers and the preparation and integration of data. TRUSTS also elaborated concepts for supporting the management and protection of IPR. The platform included technical measures for protecting IPR in data sharing, including the IDS metadata broker and the IDS clearing house. The IDS metadata broker is a matching mechanism and gatekeeper between data providers and data consumers.

The threat modelling for TRUSTS involved the identification of potential threats to the protection of IPR in TRUSTS data exchange platform. The process of threat analysis includes the identification of general and extended threat types, the determination of possible impacts, and the deployment of countermeasures. The general threat types include unauthorized access to data, data theft, and data misuse. The extended threat types include cyber-attacks, data breaches, and data manipulation. The impact analysis is based on the potential consequences of these threats, including financial losses, reputational damage, and loss of control over data. To counter these threats, TRUSTS deployed a range of technical and administrative measures, including data encryption, access control mechanisms, and regular security audits.

Technical measures, such as encryption and secure data storage, can help protect IPR in data exchange platforms. The IDS metadata broker and IDS connector can act as a matching mechanism and gatekeeper between data providers and data consumers, ensuring that data exchange agreements are transparent and equitable. The IDS clearing house can monitor transactions and indicate fair use, ensuring that data providers and data consumers are protected in their data exchange activities.

The management of IPR within a datamarket requires a consensus among stakeholders on the IPR of services and software components. A TRUST-DAO model was conceptualized to manage services, software licenses, and cost and revenue sharing in the datamarket. The use of dataNFTs and a strong foundation of structural, organizational, legal, and technical elements are also important considerations in the management of IPR within a datamarket.

In conclusion, the protection of IPR in datamarkets is essential to ensure that data exchange platforms are secure, transparent, and equitable for both data providers and data consumers. The development of technical measures, such as encryption and secure data storage, the implementation of monitoring and reporting mechanisms, and the creation of a consensus among stakeholders on the IPR of services and software components are key factors in the further development of IPR in datamarkets.

8.2 Recommendations: Strategizing Future IPR Protection in Data Markets

As the use of data assets continues to grow, it is essential that data exchange platforms provide a secure and monetizable environment for the exchange of these assets. The successful survival of data platforms depends on this. The following recommendations for strategizing future intellectual property rights protection in data markets will hopefully help, to achieve this. By examining current trends and the needs of data providers, consumers, and exchange platforms, the report outlined key considerations and ends with proposing suggestions for ensuring the longevity of data markets and the effective protection of IPR in data exchange:

Firstly, the development of standard data exchange protocols is crucial for seamless data integration while preserving IPR protection. Secondly, implementing monitoring and reporting mechanisms, such as the ones developed in the TRUSTS project, will allow data providers to monitor and report any unauthorized access to their data. Thirdly, strengthening technical measures for data protection, like encryption and secure storage, will ensure the protection of IPR in data exchange platforms. Fourthly, the enhancement of security protocols for data exchange, including encryption techniques, will prevent unauthorized access and protect against data theft and manipulation. Fifthly, establishing a data exchange governance framework covering data privacy, protection, and ownership is necessary for secure and profitable data exchange. Sixthly, regulation of data exchange contracts will ensure transparency and fairness for both data providers and consumers. Seventhly, collaboration between data providers, consumers, and exchange platforms is essential for the success and sustainability of data platforms. This can be achieved through industry forums, working groups, and support initiatives such as the Data Space Support Centre. Eighthly, improving user awareness and education on IPR protection will ensure data providers understand the importance of protecting their data and IPR. Ninthly, integrating IPR protection into data management systems, especially for SMEs, will allow for easy management of IPR and control over data access. Tenthly, investment in research and development for innovative solutions for IPR protection in data exchange platforms will ensure the long-term security and effectiveness of these platforms. Eleventhly, adopting international standards for IPR protection in data markets will ensure a uniform approach and interoperability between data exchange platforms globally. Twelfthly, promoting the harmonization of legal frameworks for IPR protection in data markets across countries and regions will provide a stable environment for secure data exchange and protect the rights of all parties involved.

Maximizing Impact - 12 Recommendations from the TRUSTS Project:

1. Further development of standard data exchange protocols: The continuous development and enhancing of standard data exchange protocols will ensure seamless integration and exchange of data between data providers and data consumers, while maintaining the protection of IPR. The approach developed in the TRUSTS project in WP7 should be pursued further. Overall, standardisation approaches are an important basis for interoperability and thus usability for users.
2. Implementing monitoring and reporting mechanisms: This involves the deployment of tools and systems that enable data providers to monitor the use of their data and to report any unauthorized access or misuse. The TRUSTS project has developed and tested valuable monitoring and reporting functions. IDSA will continue to work on such mechanisms. It would be good to make the different approaches more interoperable overall. Initiatives such as Gaia-X show the need for such activities. These and similar initiatives are extremely important and should be prioritised.
3. Strengthening technical measures for data protection: Technical measures such as encryption and secure data storage can be further strengthened to ensure the protection of data and IPR in data exchange platforms. The approach in the TRUSTS project was to show how it is already possible to build a secure system using various technologies. In the future, there will be even more sophisticated approaches, which will hopefully reduce the development effort even further.
4. Development of robust security protocols for data exchange: This involves further enhancement and easier implementation of encryption techniques and other security measures to prevent unauthorized access to data, data theft, and data manipulation. Such security approaches are already common today and will certainly become even more widespread in the future. Nevertheless, security tests show that a very large number of IT users (corporate and private) do not take the issue of IT security seriously

enough. Therefore, break-ins and data theft occur time and again. More robust security protocols can at least reduce the threat from this side.

5. Establishing a data exchange governance framework: This involves the creation of a set of policies and procedures for data exchange that covers data privacy, data protection, and data ownership. IDSA is working on such a governance framework. The TRUSTS project was able to show how security could be increased through an appropriate IT architecture plus a governance framework. This framework must be further consolidated in the future.
6. Regulating data exchange contracts: The regulation of data exchange contracts can ensure that data exchange agreements are transparent and equitable for both data providers and data consumers. Here it would be good if the European legislator could create more regulatory frameworks that the users of data exchange platforms could apply. It would be very good if data assets, like objects, were subject to property rights, because then existing property rights would also apply to data assets. However, it currently seems far off or unrealistic that this will happen.
7. Collaboration between stakeholders: For the long-term success and sustainability of data platforms, it's crucial to have secure and monetizable exchange of data assets. Starting with sector-specific use-cases is a key factor for success. Effective protection of Intellectual Property Rights in data exchange platforms requires collaboration between data providers, consumers, and exchange platforms in use cases and later in productive and business model-based operating companies. This can be facilitated through the establishment of industry forums and working groups, as well as support initiatives such as the "Data Space Support Centre" (DSSC).
8. Improvement of user awareness and education: Data providers should be educated and made aware of the importance of IPR protection and the measures they can take to protect their data and IPR in data exchange platforms. It seems important and necessary to increase IT security literacy. In addition to the classic technical IT security topics, this should also include IPR-related and business-related topics.
9. Integration of IPR protection into data management systems: The integration of IPR protection into existing data management systems – especially of SME - will allow data providers to easily manage their IPR and control the access and use of their data in data exchange platforms. Some different approaches to this challenge have been taken up and investigated in the TRUSTS project and integrated into the TRUSTS platform. Other approaches should be further developed. Currently, the approach with the Eclipse Data Space Components Connector (EDC Connector) of the Eclipse Foundation seems to be a very promising approach. It remains to be seen whether and if so, how certain interoperability standards for data exchange platforms will develop. It is to be expected that there will be a manageable number of standardised connectors for the common data management systems.
10. Investment in research and development: Investment in research and development to explore new and innovative solutions for the protection of IPR in data exchange platforms will ensure that these platforms remain secure and effective in the long term. During the TRUSTS project, it became apparent that the consortium participants were hesitant about further investments in the TRUST platform or about taking over the operator responsibility. On the one hand, this is certainly due to concerns about legal liability in the event of technical problems or IPR problems, but also because data exchange is still a young field of activity. The market for data exchange is still emerging and investments are not yet considered safe. Therefore, it is recommended that further funding be invested in research and development until the still young market of data exchange has matured.
11. Standardization of IPR protection across data exchange platforms: Standardization of IPR protection across different data exchange platforms will ensure consistency in the protection of IPR and provide a level playing field for data providers and data consumers. Currently, too many approaches to IPR protection exist side by side. It is urgently recommended to achieve more interoperability and standardisation. The different systems used should understand each other better. The Gaia-X initiative has already provided valuable impetus in this regard. However, this should continue to be pursued and become a mandatory programme for as many funded projects as possible. A European framework for the use of IPR-protecting components is needed. These must also be interoperable across borders. What is needed is a framework that does not stop at project or national borders. Similar to road traffic: a car

does not need a new number plate when it crosses a national border. A user of a data system (currently) still needs several "number plates" (registrations) to be able to participate in different data exchange systems. This should be changed.

12. Development of blockchain-based management and cost-sharing tools for data exchange platforms: The development of blockchain-based management and cost and revenue sharing tools for data exchange platforms (like proposed in this report) can provide a secure and decentralized environment for the exchange of data, while ensuring the protection of IPR. Especially with regard to the use of IPR within a consortium or among operating companies, blockchain or nft-based management tools can help. Overall, it should be considered whether the also still young technology of dataNFT can be used more for IPR in data exchange. This approach could perhaps cover the policy and management-relevant aspects more dynamically than previous systems can. The approach presented here should be further researched and implemented in pilot projects.

In conclusion, the protection of IPR in data exchange markets is essential to ensuring that data exchange platforms are fair, transparent, and equitable. The above-mentioned mid-term and long-term recommendations aim to provide a roadmap for the development and improvement of IPR protection in data exchange markets, through the development of standard protocols, the strengthening of technical measures, and the establishment of a data exchange governance frameworks.

References

Abbas, A. E. (2021). Designing Data Governance Mechanisms for Data Marketplace Meta-Platforms. Paper presented at the Proceedings 34th Bled eConference – Digital Support from Crisis to Progressive Change, online.

Abbas, A. E., Agahari, W., Van de Ven, M., Zuiderwijk, A., & de Reuver, M. (2021). Business Data Sharing through Data Marketplaces: A Systematic Literature Review. Paper presented at the 34th Bled eConference - Digital Support from Crisis to Progressive Change, online.

Anjaria, K. A. (2020). Computational implementation and formalism of FAIR data stewardship principles. Data Technologies and Applications.

Arzberger, P., Schroeder, P., Beaulieu, A., Bowker, G., Casey, K., Laaksonen, L., . . . Wouters, P. (2004). Promoting access to public research data for scientific, economic, and social development. Data Science Journal, 3(29), 135-152. doi:https://doi.org/10.2481/dsj.3.135

Bishop, M. (1991). "An Overview of Computer Viruses in a Research Environment." Dartmouth College, Hanover, NH, USA. Retrieved from http://www.ncstrl.org:8900/ncstrl/servlet/search?formname=detail%5C&id=oai%3Ancstrlh%3A dartmouthcs%3Ancstrl.dartmouthcs%2F%2FPCS-TR91-156

Boeckhout, M., Zielhuis, G., Bredenoord, A. (2018). The FAIR guiding principles for data stewardship: fair enough? Retrieved from https://www.nature.com/articles/s41431-018-0160-0

Clarke, T. (2013). Just do it: Nike opens access to customer data. The Sydney Morning Herald. Retrieved from https://www.smh.com.au/technology/just-do-it-nike-opens-access-to-customer-data-20130122-2d3tt.html

Curry, E. (2020). Future Research Directions for Dataspaces, Data Ecosystems, and Intelligent Systems. In Real-time Linked Dataspaces (pp. 297-304): Springer.

Dawes, S. (1996). Interagency Information Sharing: Expected Benefits, Manageable Risks. Journal of Policy Analysis and Management, 15(3), 377-394. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/(SICI)1520-6688(199622)15:3%3C377::AID-PAM3%3E3.0.CO;2-F/pdf

De Prieëlle, F., De Reuver, M., & Rezaei, J. (2020). The Role of Ecosystem Data Governance in Adoption of Data Platforms by Internet-of-Things Data Providers: Case of Dutch Horticulture Industry. IEEE Transactions on Engineering Management.

Deichmann, J., Heineke, K., Reinbacher, T., & Wee, D. (2016). "Creating a successful Internet of Things data marketplace." McKinsey & Company. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/creating-a- successful-internet-of-things-data-marketplace

Fecher, B., Friesike, S., & Hebing, M. (2015). What drives academic data sharing? PLoS ONE, 10(2), e0118053. doi:https://doi.org/10.1371/journal.pone.0118053

Federal Office for Information Security (BSI) (2017)-. "IT-Grundschutz Methodology". Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.pdf?__blob=publicationFile&v=2

Federal Office for Information Security 200-3 (BSI) (2017)-. "Risk Analysis based on IT Grundschutz". Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2

Force11. (2016). The FAIR data principles. Retrieved from https://www.force11.org/group/fairgroup/fairprinciples

Fu, X. (2005). "On traffic analysis attacks and countermeasures", Doctoral Dissertation. Texas A&M University. Retrieved from http://hdl.handle.net/1969.1/4968

GO FAIR. (no date). FAIR Principles. Retrieved from https://www.go-fair.org/fair-principles/

Gupta, N., Blair, S., & Nicholas, R. (2020). What We See, What We Don't See: Data Governance, Archaeological Spatial Databases and the Rights of Indigenous Peoples in an Age of Big Data. Journal of Field Archaeology, 45(sup1), S39-S50.

Gurin, J. (2014). Open data now. The secret to hot startups, Smart investing, savvy marketing, and fast innovation. New York: Mc Graw Hill Education.

Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2016). "Capturing value from big data – a taxonomy of data-driven business models used by start-up firms." International Journal of Operations & Production Management, 36(10), 1382–1406. https://doi.org/10.1108/IJOPM-02- 2014-0098

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. Big Data & Society, 8(1), 205395172098201. doi:10.1177/2053951720982012

IAIS, F. Enterprise Knowledge Graphs. Retrieved from https://www.iais.fraunhofer.de/en/business-areas/enterprise-information-integration/enterprise-knowledge-graphs.html

Ivanov, Y. (2018). What is an Enterprise Knowledge Graph and Why Do I Want One? Retrieved from https://enterprise-knowledge.com/what-is-an-enterprise-knowledge-graph-and-why-do-i-want-one/

Jaiman, V., & Urovi, V. (2020). A Consent Model for Blockchain-based Distributed Data Sharing Platforms. arXiv preprint arXiv:2007.04847.

Kaasenbrood, M., Zuiderwijk, A., Janssen, M., de Jong, M., & Bharosa, N. (2015). Exploring the Factors Influencing the Adoption of Open Government Data by Private Organisations. International Journal of Public Administration in the Digital Age, 2(2), 75-92. doi:10.4018/ijpada.2015040105

Kamatchi, R., & Ambekar, K. (2016). "Analyzing Impacts of Cloud Computing Threats in Attack based Classification Models." Indian Journal of Science and Technology, 9(21). https://doi.org/10.17485/ijst/2016/v9i21/95282

Khatri, V., & Brown, C. V. (2010). Designing data governance. Communications of the ACM, 53(1), 148-152.

Kim, Y., & Adler, M. (2015). Social scientists' data sharing behaviors: Investigating the roles of individual motivations, institutional pressures, and data repositories. International Journal of Information Management, 35(4), 408-418. doi:https://doi.org/10.1016/j.ijinfomgt.2015.04.007

Kitsios, F., & Kamariotou, M. (2019). Open Data Value Network and Business Models: Opportunities and Challenges. Paper presented at the 2019 IEEE 21st Conference on Business Informatics (CBI).

Koutroumpis, P., Leiponen, A., & Thomas, L. D. W. (2017). "The (Unfulfilled) Potential of Data Marketplaces." ETLA Working Papers (Vol. 2420). The Research Institute of the Finnish Economy. Retrieved from http://hdl.handle.net/10419/201268

Lee, S. U., Zhu, L., & Jeffery, R. (2017). Data governance for platform ecosystems: Critical factors and the state of practice. arXiv preprint arXiv:1705.03509.

Lee, S. U., Zhu, L., & Jeffery, R. (2018). A Contingency-Based Approach to Data Governance Design for Platform Ecosystems. Paper presented at the PACIS.

Lee, S. U., Zhu, L., & Jeffery, R. (2019). Data Governance Decisions for Platform Ecosystems. Paper presented at the Proceedings of the 52nd Hawaii International Conference on System Sciences.

Leiponen, A., & Thomas, L. D. W. (2016). "Big data commercialization." In IEEE Engineering Management Review (Vol. 44, pp. 74–90). https://doi.org/10.1109/EMR.2016.2568798

Lis, D., & Otto, B. (2020). Data Governance in Data Ecosystems–Insights from Organizations.

Magalhaes, G., Roseira, C., & Manley, L. (2014). Business models for open government data. Paper presented at the International Conference on Theory and Practice of Electronic Governance, Guimarães, Portugal.

Martens, B., De Streel, A., Graef, I., Tombal, T., & Duch-Brown, N. (2020). Business-to-Business data sharing: An economic and legal analysis. EU Science Hub.

Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2003). “Improving web application security: Threats and Countermeasures”, Satyam Computer Services, Microsoft Corporation. Retrieved from https://docs.microsoft.com/en-us/previous- versions/msp-n-p/ff649874(v%3Dpandp.10)

Muscat, I. (2019). “What Are Injection Attacks.” Acunetix. Retrieved from https://www.acunetix.com/blog/articles/injection-attacks/

Nardi, B. A., & O’Day, V. L. (1999). Information Ecologies: Using Technology with Heart. Cambridge, MA, USA: MIT Press.

National Research Council. 2000. The Digital Dilemma: Intellectual Property in the Information Age. Washington, DC: The National Academies Press. https://doi.org/10.17226/9601.

Nokkala, T., Salmela, H., & Toivonen, J. (2019). Data Governance in Digital Platforms. Paper presented at the AMCIS.

Potiguara Carvalho, A., Potiguara Carvalho, F., Dias Canedo, E., & Potiguara Carvalho, P. H. (2020). Big Data, Anonymisation and Governance to Personal Data Protection. Paper presented at the 21st Annual International Conference on Digital Government Research.

Rosenbaum, B., Reilly, H., & Widmer, M. (2017). Protecting intellectual property rights: Challenges, opportunities, and solutions. Retrieved from https://www2.deloitte.com/us/en/pages/public-sector/articles/protecting-intellectual-property-rights.html

Smith, D. A. (2017). “7 Steps of a Cyber Attack and What You Can Do to Protect Your Windows Privileged Accounts”, Beyond Trust. Retrieved from https://www.beyondtrust.com/blog/entry/7- steps-cyber-attack-can-protect-windows-privileged-accounts

Spiekermann, M., Tebernum, D., Wenzel, S., & Otto, B. (2018). “A metadata model for data goods.” In Multikonferenz Wirtschaftsinformatik (MKWI) (pp. 326–337). Retrieved from http://mkwi2018.leuphana.de/wp-content/uploads/MKWI_147.pdf

van den Broek, T., & van Veenstra, A. F. (2015). Modes of governance in inter-organizational data collaborations.

Wilkinson, M. D., Dumontier, M., IJsbrand Jan Aalbersberg, Appleton, G., Axton, M., Baak, A., . . . Mons, B. (2016). The FAIR Guiding Principles for Scientific Data Management and Stewardship. Nature, 3(160018), 1-9. doi:10.1038/sdata.2016.18

Wiseman, L., Sanderson, J., Zhang, A., & Jakku, E. (2019). Farmers and their data: An examination of farmers’ reluctance to share their data through the lens of the laws impacting smart farming. NJAS - Wageningen Journal of Life Sciences, 90-91, 100301. doi:10.1016/j.njas.2019.04.007

Zeleti, F. A., Ojo, A., & Curry, E. (2016). Exploring the economic value of open government data. Government Information Quarterly, 33(3), 535–551.

Zhang, L., Yu, S., Wu, D., & Watters, P. (2011). “A Survey on Latest Botnet Attack and Defense.” In 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 53–60). Changsha: IEEE. https://doi.org/10.1109/TrustCom.2011.11

Zlomislic, V., Fertalj, K., & Sruk, V. (2014). “Denial of service attacks: An overview.” In 2014 9th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1–6). Barcelona: IEEE. https://doi.org/10.1109/CISTI.2014.6876979

Zuiderwijk, A., & Spiers, H. (2019). Sharing and re-using open data: A case study of motivations in astrophysics. International Journal of Information Management, 49, 228-241. doi:https://doi.org/10.1016/j.ijinfomgt.2019.05.024

Zuiderwijk, A., Janssen, M., Poulis, K., & Vandekaa, G. (2015). Open data for competitive advantage: insights from open data use by companies. Paper presented at the 16th Annual International Conference on Digital Government Research, Phoenix, Arizona, U.S.A.

Zuiderwijk, A., Janssen, M., van de Kaa, G., & Poulis, K. (2016). The wicked problem of commercial value creation in open data ecosystems: Policy guidelines for governments. Information Polity, 21(3), 223-236.