TRUSTS
Trusted Secure Data Sharing Space

D7.4
Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship I

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 focuses on the possible mechanism for protecting IPR for data market users and designs a process to further enhance the protection possibilities.

June 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 871481.

TRUSTS Trusted Secure Data Sharing Space

D7.4 Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship I

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	D7.4 Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship I		
Work Package	WP7 Business Model, Exploitation & Innovation Impact Assurance		
Contractual due date	30/06/2021	**Actual submission date**	19/07/2021
Nature	Report	**Dissemination Level**	Public
Lead Beneficiary	Governance One GmbH		
Responsible Author	Andreas Huber, Bert Utermark (G1)		
Contributions from	G1, TUD, IDSA, DIO, EBOS		

© TRUSTS, 2021

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V0.1	2021-05-10	10%	Initial structure / draft	Andreas Huber, Bert Utermark (G1)
V0.2	2021-06	65%	Worked on text in all sections	Andreas Huber (G1), Anneke Zuiderwijk (TUD), Antragama Ewa Abbas (TUD), Hosea Ofe (TUD), Natalia Simon (IDSA), Gianna Avgousti (EBOS)
V0.3	2021-07-02	75	Added text in section Data Governance and Data Stewardship for users	Andreas Huber (G1), Anneke Zuiderwijk (TUD), Antragama Ewa Abbas (TUD)
V0.4	2021-07-05	80%	Draft restructuring and update	Andreas Huber (G1)
V0.5	2021-07-08	85%	Added information, comments from partners	all
V0.6	2021-07-11	95%	Completed first draft for review	Andreas Huber (G1)
V0.7	2021-07-16	98%	Peer review and quality control with TRUST partners from two organizations	Martin Kaltenböck (SWC) Yulyia Miadzvetskaya (KUL)
V0.8	2021-07-21	99%	Incorporated reviewers' comments/ finalisation of content, additional cross-reviews to other WPs	Andreas Huber (G1), Antragama Ewa Abbas (TUD)
V1.0	2021-07-23	100%	Formatting and finalizing final version for submission	Andreas Huber (G1)

© TRUSTS, 2021

Disclaimer

The content of the publication herein is the sole responsibility of the publishers, and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the TRUSTS consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the TRUSTS Consortium nor any of its members, their officers, employees, or agents shall be responsible or liable in negligence or otherwise however in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the TRUSTS Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© TRUSTS, 2020-2022. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the

work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Table of Contents

© TRUSTS, 2021

List of Figures

List of Tables

© TRUSTS, 2021

Glossary of terms and abbreviations used

Abbreviation / Term	Description
AI	Artificial Intelligence
CA	Consortium Agreement
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[1].
DS	Data Stewardship
E2E	End to End
EU	European Union
FAIR	Findable, Accessible, Interoperable and Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation
IoT	Internet of Things
IPR	Intellectual Property Rights
IPR	Intellectual Property Rights
IPRED	Directive on the enforcement of intellectual property rights
ML	Machine Learning
SME(s)	Small Medium Enterprises
TRUSTS	Trusted Secure Data Sharing Space
TRUSTS OpCo	TRUSTS Operating Company (to be set up in the future)
WP	Work Package

[1] Höchtl and Lampoltshammer, 2017

© TRUSTS, 2021

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:

1. Legal requirements to be embedded in the platform's terms of use,
2. Defined mechanisms to report suspected Intellectual Property (IP) infringement,
3. Proposed onboarding Intellectual Property Rights (IPR) protection information and education requirements for TRUSTS user groups,
4. Proposed Data Stewardship Support Services for different (potential) data provider groups to optimize eased attraction and onboarding of Small Medium Enterprises (SMEs) data providers.

This is the first version of the project’s deliverable D7.4 “Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship I'', addressing the Task 7.3 “Intellectual Property and Data Stewardship”, along with the work that has been performed under WP7.

The purpose of this deliverable is to set up the guidelines on how IPR will be managed by the TRUSTS consortium and will be continuously updated and reported at the end of the project by M36 as D7.5 “Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship II”. This deliverable issues thereby two types of mechanisms for IP protection: technical measures (see Chapter 4) and contractual measures (see Chapter 5) that may be considered later on by TRUSTS.

The following technical measures und mechanisms have been identified that may be of interest for TRUSTS (Chapter 4.2):

1. Securing the IP both physically and digitally by the use of cryptography
2. Data anonymization by removing personal or confidential data field before publication
3. Federated learning as a technique for decentralized learning where private and sensitive data never have to leave their local storage location.
4. Ensemble learning, where aggregated data sets are used.

Further, the International Data Space, on which TRUSTS is building on, is offering several mechanisms to support the IPR protection, which are:

- The IDS metadata broker, as an intermediate relevant for TRUSTS IP mapping, as well as providing access and usage control (Chapter 4.3 and 4.4).
- The IDS Clearing House as a monitoring instance for transactions and indicator for fair use (Chapter 4.5).

In terms of contractual measures, the deliverable is offering two elements relevant for IP protection:

One solution to protect IPR is the “Code of Conduct for using the TRUSTS Platform” (CC) draft, a framework for amicable cooperation, that will be eventually enriched with sanctions and penalties in the next deliverable of this task if needed (see chapter 5.2). The other tool is the draft of “Terms and Conditions for using TRUSTS Services“ (TC), summarising the results developed in the project and providing a legal framework for further work on and with TRUSTS (see chapter 5.3).

This document has already concluded several recommendations towards the conceptualization of TRUSTS aiming at efficient and affordable IPR protection mechanisms (see chapter 6).

The recommendations towards the TRUSTS platform development can be summarized as follows (sub-chapter 6.1):

- Secure and legally compliant exchange of the datasets and services is required.
- Review published data to make informed decisions on buying legitimate products.
- 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.

© TRUSTS, 2021

- Effective and secure user management should be employed.
- Inherent protection of private datasets should be provided.

From IPR's point of view, three fundamental aspects are important for the further development of the TRUSTS platform and should be considered by a future TRUSTS operator:

1. Cross-system mapping of data assets
2. Actualisation of meta data from decentralised data storages and data networks
3. Interaction of automatic digital contracts and data assets

Further, the document lays out a description of the general context and detailed information regarding the current state of IPR protection and Data Stewardship (DS) as well as issues and solutions associated with the TRUSTS project.

This deliverable's goal is to define and to document the framework setup intended to protect original data owners/providers and resellers of enriched data whilst supporting innovation and value extraction. The 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.

© TRUSTS, 2021

1 Introduction

1.1 Introduction: IPR and Data Markets?

TRUSTS supports the emergence of a European data market and economy, based on secured, safe and General Data Protection Regulation (GDPR) compliant data exchanges and aims to develop a platform supporting these exchanges.

TRUSTS will ensure 'trust' in the concept of data markets via its focus on developing a platform based on the experience of two large national projects, while allowing the integration and adoption of future platforms. The TRUSTS platform will act both independently and as a platform federator, while investigating the legal and ethical aspects that apply on the entire data valorification chain, from data providers to consumers.

Based on the TRUSTS Consortium Agreement (CA) and as stated in the project's Grant Agreement (GA), this document is aimed at providing guidelines on how IPR will be managed by the TRUSTS consortium.

Intellectual Property (IP)[2] means technical information, inventions, developments, discoveries, know-how, methods, techniques, formulae, algorithms, data, processes and other proprietary ideas (whether patentable or copyrightable). IP also includes patent applications, patents, copyrights, trademarks, mask works, trade secrets, and any other legally protectable information, including computer software. It is the rights of the background and the rights of the foreground.[3]

Additionally, this document establishes rules for the use of foreground, side ground and background knowledge and its distribution within the project as well as the rules for handling sensitive and confidential information.

Sound Innovation and IPR management is critical to enable the successful exploitation and market deployment of the wide range of TRUSTS assets. Therefore, the consortium of TRUSTS places great emphasis in managing innovation and IPR in the framework of the project, with a view to effectively paving the way for the smooth exploitation and sustainability of its results following its completion.

TRUSTS IPR management objectives embrace the need to protect project's assets to handle and manage efficiently all the outcomes that will stem during the project's life span with a view to ensure the commercial rollout of the exploitable results along with their proper dissemination.

[2] https://www.europarl.europa.eu/factsheets/en/sheet/36/intellectual-industrial-and-commercial-property
[3] See also: https://www.lawinsider.com/dictionary/background-rights or https://en.wikipedia.org/wiki/Background,_foreground,_sideground_and_postground_intellectual_property

© TRUSTS, 2021

1.2 Deliverable Overview and Report Structure

The following section provides an overview of the deliverable's structure as well as a detailed description of the plan of action in compliance with the expected outcomes of the T7.3. The document lays out a description of the general context and detailed information regarding the current state of IPR protection and DS as well as issues and solutions associated with the TRUSTS project.

The structure of this deliverable is the following:

Section1introduces this report and gives a recap on TRUSTS projects as well as a definition of Intellectual Property (IP)

Section 2 offers a summation of the current state and the regulations and policies for IPR protection

Section 3 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 suggests concepts and actual development of monitoring and surveillance mechanism for managing IPR of the TRUSTS platform

Section 5 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

Section 6 concludes the report and provides information on the planned next steps, as well as implications and recommendations for the TRUSTS platform development and operator.

Section 7 is the bibliography used.

1.3 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**
T7.3 *IPR and Data Stewardship*	In this task we target challenges around Intellectual Property Rights (IPR) and Data Stewardship (DS). Goal is to protect original data owners/providers and resellers of enriched data whilst supporting innovation and value extraction.	Chapters 2, 3	Introducing chapters to the topic
	Obviously, bare minimum legal requirements have to 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 has to 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	Chapter 4	Overview to existing and necessary technical mechanism for protecting IPR

© TRUSTS, 2021

TRUSTST Task:		Respective Document Chapter(s)	Justification
	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 work task has to 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 has them 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.	Chapter 5 Chapter 2 Chapter 3	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			
D7.4 IPR and Data Stewardship (M18 Interim Report) For D7.4 we will conduct 3 workshops with stakeholders of the Data Market Austria (data owners/providers, data users/buyers, data aggregators / resellers) on their practical challenges and perspectives regards IPR protection and Data Stewardship. A report will be drafted, outlining related (1) legal requirements to be embedded in the platform's terms of use, (2) defined mechanisms to report suspected IP infringement, (3) proposed onboarding IPR protection information and education requirements for TRUSTS user groups, (4) proposed Data Stewardship support services for different (potential) data provider groups to optimize eased attraction and onboarding of (SME) data providers. The document will be updated during the project and presented in M18 (interim report) and M36 (final report).			

Table 1: Adherence to TRUSTS GA Deliverable & Tasks Descriptions

© TRUSTS, 2021

1.4 Interdependencies of Task 7.3 with other tasks in the project

The task T7.3 has independencies with several other work packages. First and foremost is the development of a sustainable business model. WP 7.1 is dedicated to this task. Depending on the results of WP 7.1, this will have an impact on the work of WP 7.5, which deals with the business planning and commercialization issues. If it is then clear on the basis of which business model which commercialization strategy will be pursued, WP 7.3 can adapt the results worked out so far accordingly. If the business model is more "TRUSTS Data Market", then it will have different implications for IPR protection mechanisms than if the business model is "TRUSTS Federator". The second half of the TRUSTS project will therefore be about adapting to the chosen business model and how WP 7.3 can support the other WPs in their tasks and to continue defining the desired contractual and administrative measures for protecting mechanism for IPR of data seeker and data provider.

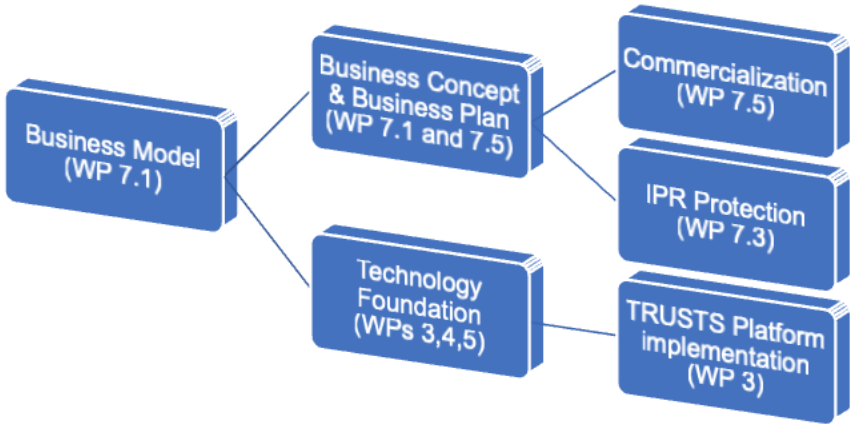

Figure 1: Interdependencies of Task 7.3 with other tasks in the project

© TRUSTS, 2021

2 Concept of mechanisms for protecting IPR

2.1 TRUSTS overall approach to IPR protection {G1}

Is Intellectual property of data assets possible?

Intellectual property rights management is an integral part of any business strategy. Knowing how to manage the IP effectively can help promote the business or product and maximise the impact of the research & innovation project. IP can be anything from a particular manufacturing process to plans for a product launch, a trade secret like a chemical formula, or a list of the countries in which the patents are registered[4].

The discussion about the protection of IPR was started more than 200 years ago, but only modern legal systems have made effective mechanisms for the protection of "intellectual property rights" possible. However, most IPRs relate to objects, works of authorship or trademarks, and thus to things that are either tangible or have undergone a particular form of (creative) creation.

A novel or an architectural design, for example, are protected by copyright due to their creation process of with the author's own creative work. This protection mechanism is well established, and publishers around the globe use this form of IPR protection as a basis for their business. Other forms of protection include the registration of trademarks or word marks to be protected for very specific jurisdictions with a limited term, or industrial design protection. Patents are another major field of IPR protection and are also well established through national and international agreements. and the IPR

Since author`s copyrights exit by default, (technical) inventions, trademarks or other things to be protected need to be actively protected: type of protection and the scope of protection must first be applied for at a patent or trademark office. After that, the owner of the intellectual property has obtained the protection right.

However, data do not fall into any of the above categories, because they are neither creative-artistic like an author's work, nor can they be protected like a trademark, nor can a patent be obtained on data. In principle, therefore, they cannot be protected by the usual IPR protection mechanisms. (Raw) data and the exchange of data is (so far) not covered by any decent protection mechanism. In essence, only the following options remain 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, storage and access
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)

[4] https://www.csoonline.com/article/2138380/intellectual-property-protection-10-tips-to-keep-ip-safe.html

© TRUSTS, 2021

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 into 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.	+++	-

© TRUSTS, 2021

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.

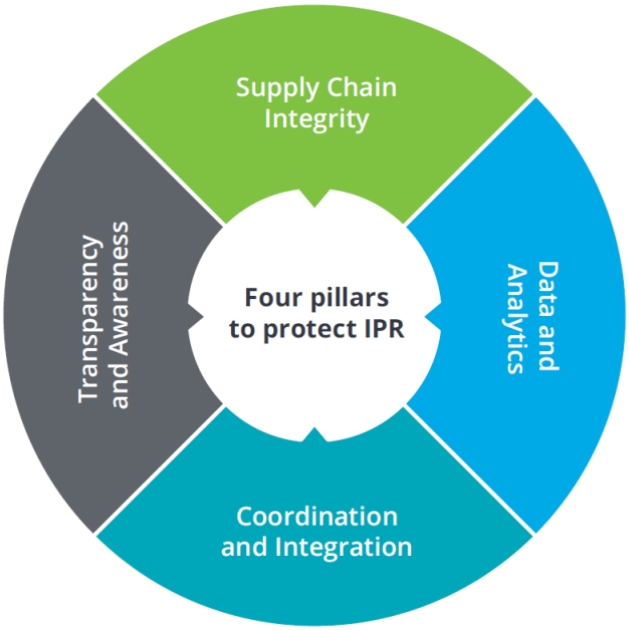

Figure 2: IPR protection pillars (Rosenbaum et al., 2017)

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 RDF, RDF-Schema, or 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

© TRUSTS, 2021

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) summarize that control over data refers to the autonomy to decide on access right 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 in 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, refer to IDS connector, enable data sovereignty by act as a security gateway where the "data provider always maintains control over the data and sets the conditions for its use." TRUSTS will use the IDS connector to ensure data sovereignty and to contribute to data protection endeavours. TRUSTS also explicitly mention 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 risks (Rosenbaum et al., 2017). Supply chain integrity can be achieved by fulfilling three strategic requirements. These are the

1. trading partner authentication,
2. the 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 contract* will contribute to fulfilling the second and third requirements. TRUSTS will ensure the supply chain visibility and provenance in data trading 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) summarize that data governance is "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 for data sharing are "regulatory instruments, licenses, formal contract-based agreements,

© TRUSTS, 2021

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: Issue & Solutions for IPR Protection

2.3.1 Regulations and policies for IPR protection

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 20205, 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. In recent decades, there has been significant progress in creating a single market for IP, yielding many benefits for the EU economy[6].

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

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

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

© TRUSTS, 2021

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[7].

Protecting IP has several benefits[8]:

1. to protect an invention, such as a new product. Directly 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 can produce more money. This is when the owner grants a licence to another company to use the IP protected subject matter for a certain period.
4. In some cases, such as for copyright and unregistered design, protecting IP is automatic and doesn't require any formalities.
5. Owning a patent or a trademark can increase the business market value and make it easier to find investors or other funding opportunities.

IP Identification means that all IP values within the project will be identified, listed, named and analysed in a systematic manner to obtain a project IP portfolio and map as figure 2 below illustrates.

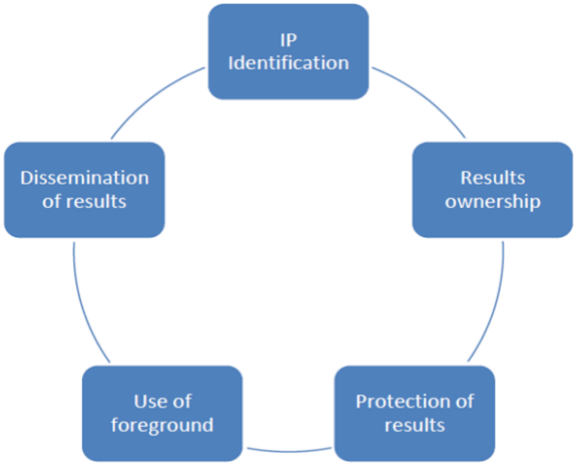

Figure 3: IPR management cycle

According to the projects GA, particularly for SMEs, regulations and (dispositive) rights regarding the use and re-use of their IP is not self-evident.

Regarding the protection of results, every partner must select the most appropriate and effective IP protection tool for every piece of foreground, in accordance with the other partners' legitimate interests and with the future planned use, if direct commercial exploitation or further research will be preferred. Partners are recommended to inform other partners about their individual protection activities plans, especially dealing with potentially joint IP.

The primary, well-known function of an IP right is to give its holder a competitive advantage in its commercial activities, by preventing unauthorised exploitation by thirds. This is especially important for SMEs, which IP rights provide with powerful weapons to compete with much larger companies[9].

It's mandatory to protect your IP because the delay of a single minute can lead to copying or stealing of your precious idea[10].

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

[8] Intellectual property rights

[9] Intellectual property: Positive aspects of IPR,

[10] How to Protect Your Intellectual Property, Updated on: Jun 22, 2021

© TRUSTS, 2021

2.3.2 Further findings from workshops with participants / contributors from Data Market Austria and DIO members

The workshops with the participants / contributors from Data Market Austria and invited DIO member focused on the two aspects:

- How and to whom can data be legally attributed?
- How can these data be used subsequently?

EU Level: Access facilitation is a major issue in the EU. Many initiatives are being taken in this regard, but so far no comprehensive regulation is being sought. The civil law classification is important - but this has not yet been regulated throughout the EU. Beyond EU level there are few binding regulations, but many open questions.

Austrian Level: Austrian property law does not provide much information. It lacks a definition of the concept of data. Furthermore, Austrian property law distinguishes between ownership and possession. According to the prevailing opinion, you can only get ownership of physical things. This means that if one says data is not a physical thing, then data ownership cannot exist. Nevertheless, data trade is possible because the allocation of concrete powers can be regulated by contract.

Learnings:

- Legal uncertainty: licence agreements are currently concluded for data trading. There are very different models here, which are individually designed. This leads to legal uncertainty.
- Affiliation of the data: not clearly clarified. There is no overarching definition or legal framework to answer the question "Who owns the data and when?
- Uniformity - at best at EU level - must be created! That means a uniform framework that regulates data trade. This should answer the questions of who owns the data and what rights are associated with it. This would reduce legal uncertainty in interstate trade and create more clarity.

Data Stewardship

The key question of this workshop was:

How can a (business) data steward help to get value out of data as a product?

Over the last few years, data has become increasingly important as a product for industry, trade and the service sector. Data can be a tradable product that can be bought and sold. In any trade, there is a contract (see IPR) and a price. In order to determine the value of data and then subsequently receive it, it must be sufficiently documented, traceably managed and archived. To this end, there are several (inter)national initiatives that deal with the value determination and data trading of data, define rules and formalise procedures. In this context, a functional role in dealing with data and data management has emerged: the "(Business) Data Steward".

A data steward has an oversight or data governance role within an organisation and is responsible for ensuring the quality and appropriateness of the organisation's data assets (including the metadata for those data assets). The overall goal of a data steward is to improve data quality.

The way data is used has a significant impact on the role of the data steward. In the beginning, data were seen as process outputs that were administered. But over time, the use and thus the value creation of data changed: from data as a process enabler to data as a product enabler to data as a product. The key question is where are the tasks grouped together that organisationally ensure that data can be used in the appropriate quality, at the right time and with the appropriately correctly assigned value creation in the respective constructs of the data economy? This is where a data steward could be helpful.

© TRUSTS, 2021

Learnings

- The data steward can fulfil many functions. It is important that the data steward is appointed with a precisely defined mandate. However, one should still keep in mind that the role of the data steward is subject to a - more or less constant - transformation, as the role of using data is changing.
- The awareness that a data steward is needed is already present in many companies. However, the data steward is not yet frequently used. Clearer guidelines are needed on what a data steward can do within an organisation.
- Legal aspects are still unclear. What legal framework is a data steward subject to?
- The digital transformation means that data stewards are faced with more and more new tasks. Thus, the spectrum of responsibilities could include the following components in the future:
    - Strategic component: companies consider appointing a chief data officer to decide where data is most appropriately and best used along the value chain - the data steward would assist here.
    - Operational component: a specialist considers how data can best be used with regard to Time2Market the data steward would support here in the area of product development (data = product)
    - Data value: financial evaluation of data value the data steward would take on the role of a product controller.

➔ Summarized, there is a need for education and knowledge exchange. There is a lack of practical examples and insights when it comes to the actual tasks of a data steward. Guidelines and legal frameworks must be created to enable companies to clearly define the tasks of a data steward and to profitably integrate him into the company organisation.[11]

Discussion

After the two inputs, the participants were divided into brainstorming sessions where they shared their experiences or the organisation's handling of intellectual property and gave suggestions on levels of protection and pragmatic solutions.

What emerged was the complexity of dealing with IPR and the desire for guidelines to make it easier. Participants agreed that these need to be uniformly regulated and communicated at EU level, as data is worked with across borders. The difficulty for organisations/institutions with regard to IPR arises from the fact that data collection is the actual effort. IPR rules and clearly defined terms are needed here: Data Sharing Agreements, Data Ownership, etc. The participants agreed that, in the long term, IPR protection can only be achieved with data certificates.

The role of a data steward was also discussed: years of industry experience, economic thinking, communication skills and interdisciplinarity (law and IT) were mentioned as prerequisites. Ideally, a data steward should be the link between law, technology and research. Certification as a guarantee of competence is desired.

First and foremost, a change in culture is needed. There is still too much uncertainty about sharing and acting with data. There is a lack of trust in the quality of data produced by oneself but also by others, as well as a lack of legal and economic framework conditions that enable secure data sharing and trading.

[11] see e g: https://searchdatamanagement.techtarget.com/definition/data-stewardship

https://www.dnb.co.uk/perspectives/master-data/6-key-responsibilities-of-data-stewards.html

https://www.techopedia.com/definition/29012/data-steward

© TRUSTS, 2021

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

Domain	Factor	Sub-factors
	Data use case	- Define data categories of platform data (e.g., user, process, and system data) - Define data use cases and link relevant actors - 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[12]. 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[13]. 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[14]:

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

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

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

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

© TRUSTS, 2021

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.

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

© TRUSTS, 2021

FAIR element	Principles related to each element of FAIR
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
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 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

© TRUSTS, 2021

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[15]. 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[16]:

- **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.

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

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

© TRUSTS, 2021

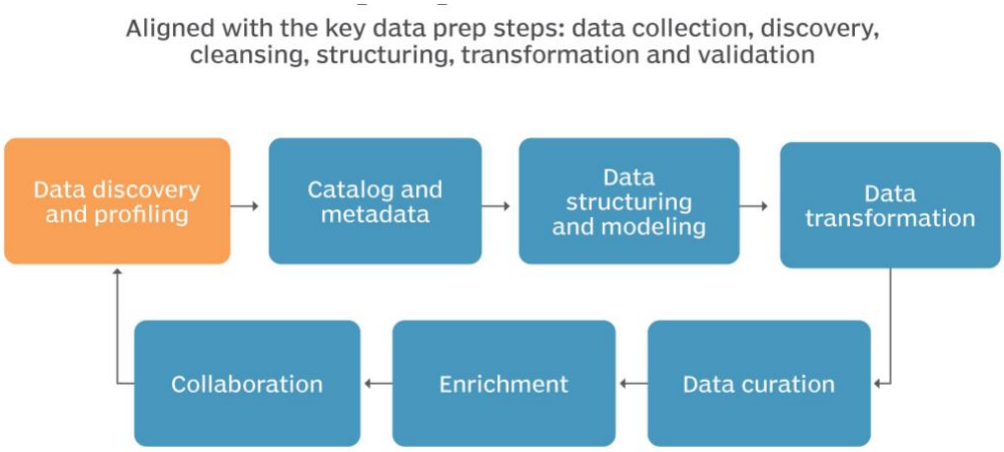

Figure 4: Data preparation capabilities and data preparation steps

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[17]. 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[18] 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

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

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.

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 trade 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"[19] 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:

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

© TRUSTS, 2021

- 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.

4 TRUSTS Monitoring & Surveillance Mechanisms for IPR Protection

4.1 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.

4.2 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

© TRUSTS, 2021

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[20].

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[21] 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.

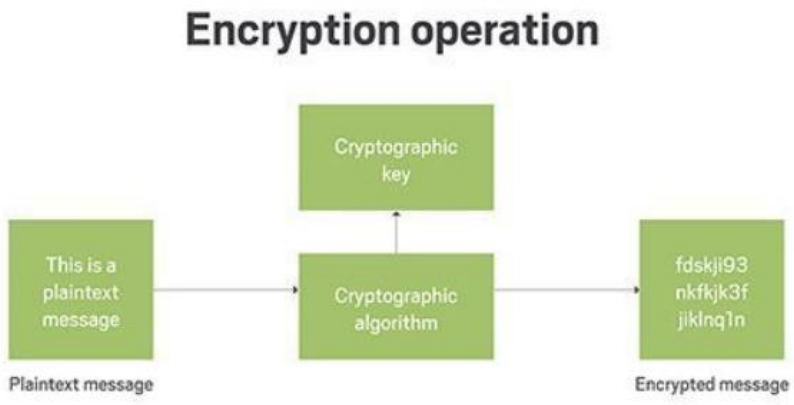

Figure 5: Encryption: How algorithms and keys are used to make a plaintext message unintelligible[22]

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,

[20] https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_EN.html
[21] https://www.csoonline.com/article/2138380/intellectual-property-protection-10-tips-to-keep-ip-safe.html
[22] Encryption By Peter Loshin, last updated in April 2020

- 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[23] of the GDPR.

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[24]:

- 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.

[23] EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)

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

© TRUSTS, 2021

4.3 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"[25]. It is considered as an optional component of a data space built according to the IDS Reference Architecture Model (IDS RAM)[26] (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[27], 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[28]. The metadata broker is not involved in the process of data exchange.

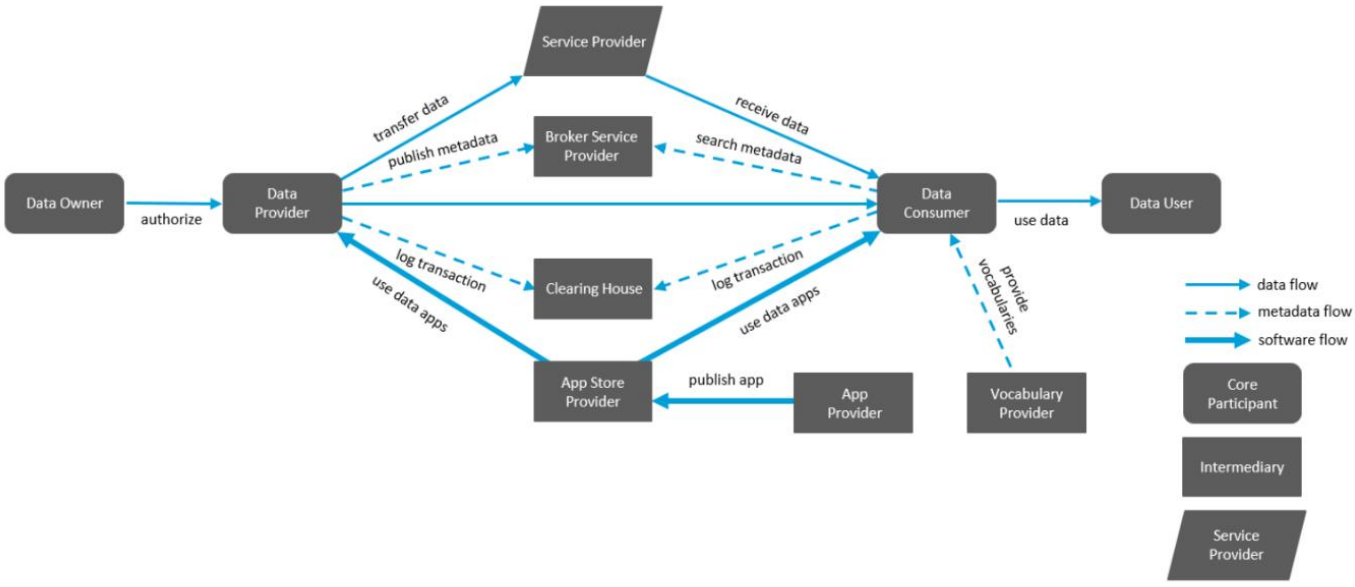

Figure 6: Roles and interactions in a data space[29]

[25] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary#broker-service-provider (accessed on June 28)
[26] https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf
[27] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary#connector
[28] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary#ids-information-model
[29] 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[30]. A more detailed overview on the metadata broker specifications is provided in the IDS Whitepaper "Specification: IDS Meta Data Broker"[31]. 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"[32], 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.

[30] https://industrialdataspace.jiveon.com/docs/DOC-2524
[31] https://internationaldataspaces.org/wp-content/uploads/IDSA-White-Paper-Specification-IDS-Meta-Data-Broker.pdf
[32] https://design-principles-for-data-spaces.org/

© TRUSTS, 2021

4.4 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[33], 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"[34], Figure 6 depicts the platform's architecture and its components.

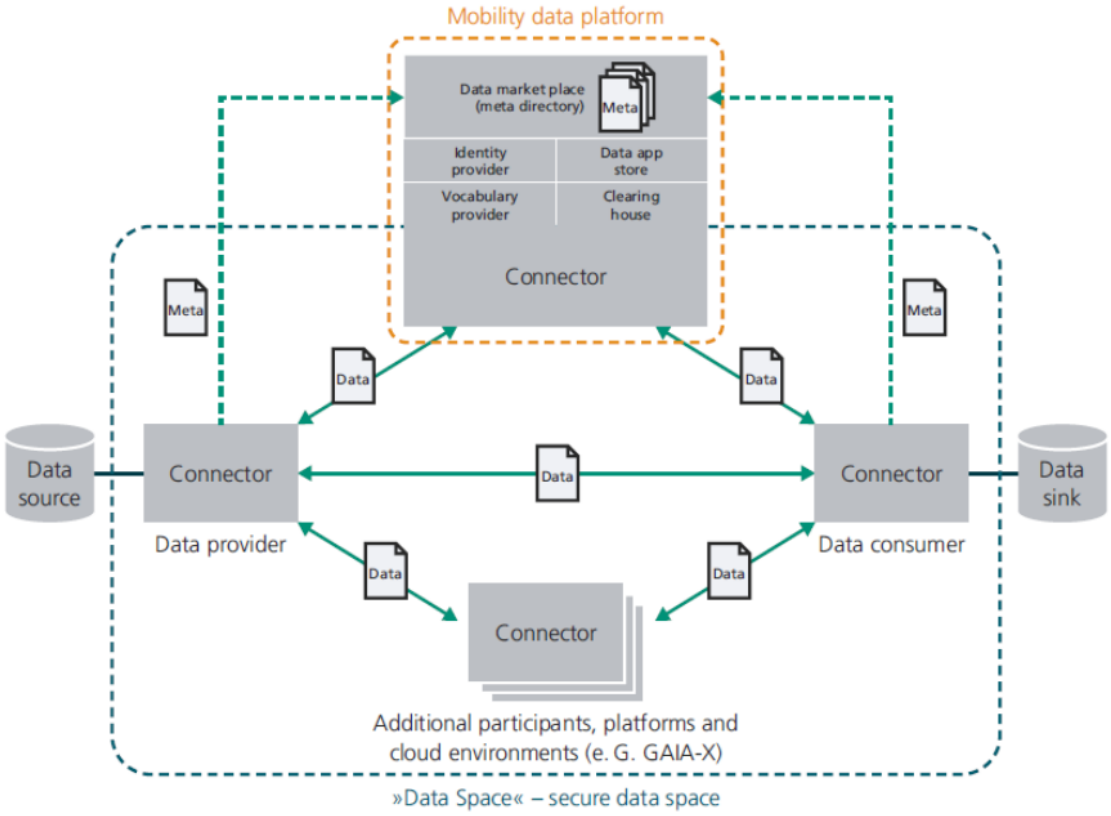

Figure 7: A data platform in the Mobility Data Space extended by IDS components

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[35].

[33] https://www.mobility-data-space.de/content/dam/ivi/mobility-data-space/documents/Mobility_Data_Space_2020_EN_neu.pdf
[34] ibid
[35] https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf

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.

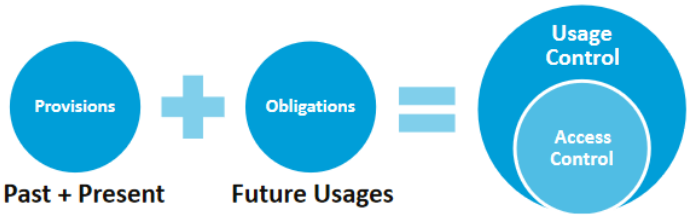

Figure 8: Data usage control – an extension of data access control36

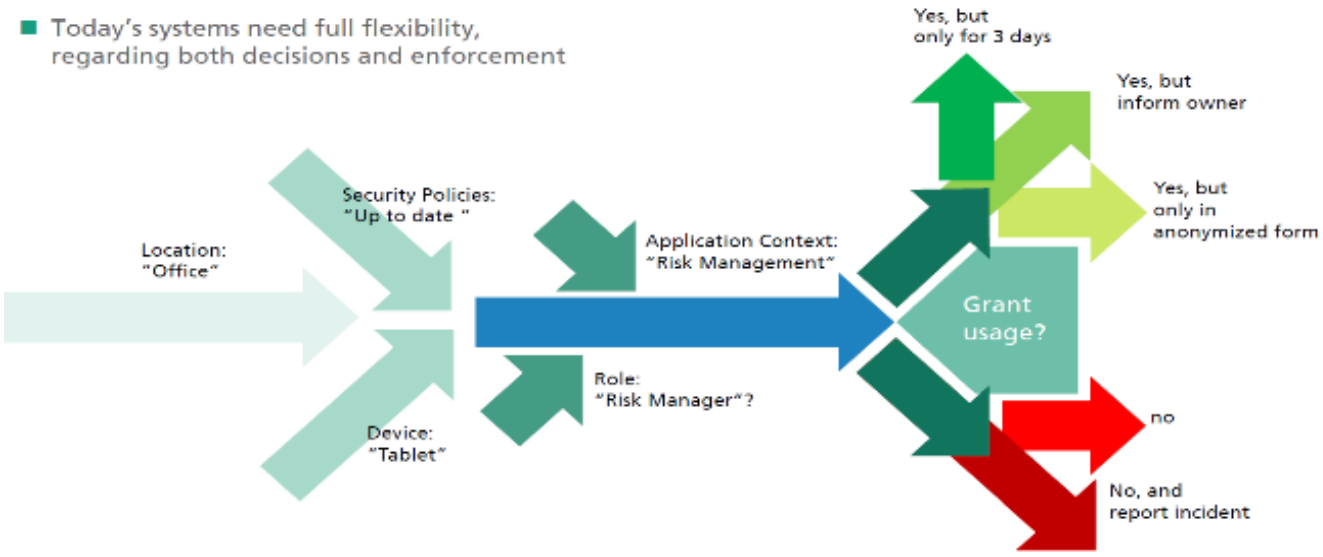

Figure 9: Example of usage control and their technical enforcement37

[36] ibid

[37] International Data Spaces Association

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 6: Security requirements that require usage control[38]

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 7: Requirements for the IDS metadata broker the usage control profile[39]

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.

[38] https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf
[39] https://internationaldataspaces.org/wp-content/uploads/IDSA-White-Paper-Specification-IDS-Meta-Data-Broker.pdf

© TRUSTS, 2021

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 8).

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.
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 8: Overview on IDS Connector Security Profiles[40]

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[41].

[40] https://internationaldataspaces.org/wp-content/uploads/IDSA-Strategy-paper-certification-scheme-V.2.pdf
[41] See „IDS Whitepaper Certification – Framework for the IDS Specification Scheme, V02" for Details.

© TRUSTS, 2021

4.5 The IDS CLEARING HOUSE as monitoring instance of transactions and indicator of fair use

In order to enable a sharing of data while keeping the control over the data, 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.[42]

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.

The following Table 9 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

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

© TRUSTS, 2021

Function name	Stage of usage	Function description
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)[43] Financial: Request financial compensation

Table 9: IDS Clearing House Functions Overview[44]

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.

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.

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

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

© TRUSTS, 2021

5 TRUSTS Platform Contractual Measures for IPR Protection

5.1 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 and 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, the law enforcement agencies can be used to recover the stolen property. This possibility does not apply to data and it is much more difficult to simply enforce any legal claim.

If data has been stolen - for example by copying - the legal possibilities to enforce any legal claims are comparatively small. For this reason, it is necessary to deal with such contractual regulations that contractually regulate the use of the TRUSTS platform and enable a certain degree of legal certainty. If certain things 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 with the contract.

This aspect is easier to resolve in court than the question of who held which user or property rights in a data asset (which is handled differently throughout Europe). In the North American legal sphere, threatened high contractual penalties in the event of breach of contract are a tried and 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 also within the future TRUSTS OpCo.

Draft	Name	Rational
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 DP and 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.

© TRUSTS, 2021

5.2 Draft "Code of Conduct for using the TRUSTS Platform" (CC)

A draft code of conduct for the use of the TRUSTS data trading platform is presented below. This text is a framework for amicable cooperation. In the future, this framework will be supplemented and expanded to include sanctions and penalties if relevant findings are obtained through the operation of TRUSTS.

5.2.1 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. The comparison is often made 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 components for success and competitive advantage in many industrial sectors, value chains and organisational processes and thus a decisive factor for production, in addition to labour and capital. However, the interconnectivity of already established data infrastructures is largely non-existent, 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 itself the task of changing this.
3. Persons, organisations or companies participating as data seeker or data provider in TRUSTS agree to be bound by this Code of Conduct. Thereafter, they may gain access to TRUSTS. They trade data on the trading platform provided by TRUSTS or arrange such data exchange. The operator of TRUSTS acts as the provider of the necessary infrastructure and also 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[45] 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 consequences of a proper use of collected data - also outside the trading 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.

5.2.2 Draft §1 General principles

1. TRUSTS Participants are data seeker or data provider or intermediates (data broker or similar) shall always act in accordance with the relevant legal provisions in all actions at TRUSTS. In particular, they shall comply with the applicable standards of the General Data Protection Regulation (GDPR). The participants are aware of how sensitive the collection and trading of personal data in particular is. 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. All TRUSTS actions must therefore not only comply with the provisions of the General Data Protection Regulation and all sector-specific regulations on data protection, but participants also declare that they are committed to the

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

principles of transparency of the data processed. This means in particular to disclose the origin and intellectual rights of the trading platform data when requested by TRUSTS. It is further agreed that any economic exploitation of data must be refrained from if it can only be achieved by violating the fundamental rights of the data subjects. It must be ensured that the data was obtained from a credible source under legally impeccable conditions and without violating the rights of third parties.

2. 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.
3. Transparency about the origin and traceability of the collection process of the traded 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 General Data Protection Regulation, it must be ensured, especially in data trading, 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 of time. Those participants who act as customers on the trading platform openly communicate their data requirements in order to enable the data providers to collect data in a targeted manner.[46]

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

1. Participants shall act loyally, fairly and responsibly towards each other and towards TRUSTS OpCo. Honesty and integrity are further maxims of 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 trading 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 bad manners, bad behaviour and bad manners among each other. Conflicts of interest shall be resolved on a factual level, if necessary with the involvement of an impartial arbitration body, which may be 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 in particular 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 signatory organisations and companies respect the dignity and privacy of the persons deployed. Every participant has the right to be protected against discrimination and harassment.

[46] 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.

© TRUSTS, 2021

5. The protection of the environment and the conservation of natural resources are of great importance to the participants. TRUSTS is a drain on 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. 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 research with traded environmental data contributes to environmental protection.

5.2.4 Draft §3 Conflicts of Interest

1. TRUSTS respects the organisational and entrepreneurial autonomy of its participants also with regard to their business activities outside TRUSTS. On the other hand, TRUSTS expects all participants - as already formulated above - to behave fairly and loyally towards it. 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 to resolve issues amicably. The place of arbitration shall be within Europe and / or under direct with the European Court of Arbitrations itself. The rules of arbitration shall be according to European regulations.
2. Participants shall avoid dealing with third parties that jeopardise 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 into and maintain business relationships must pay appropriate attention to this.
3. Participants shall also ensure that participating companies take reasonable precautions/measures to ensure that the Code of Conduct is also complied with by the employees acting in each case. [47]

5.2.5 Draft §4 Data Protection / Confidentiality

1. The confidential handling of data and information received by the Participants in the course of business relations in connection with data trading via TRUSTS is essential for the undersigned. Accordingly, these shall be treated with the greatest possible care and confidentiality. The Participants, as responsible entities, shall ensure that the requirements of data protection and 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 General Data Protection Regulation and shall be obliged to comply with it, as data trade may give them access to particularly sensitive data. They are informed by the company employing them that violations of data protection regulations 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 take into account that the collection, storage, processing and other use of personal data may be carried out in accordance with the General Data Protection Regulation. All

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

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. Finally, participants shall recognise that the security of other data collected, gathered, processed, used or stored shall also be ensured, in particular 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.

5.2.6 Draft §6 Violations and Sanctions

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

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

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

In this chapter, a "General Contractual Terms and Conditions for using the TRUSTS Data Trading Platform" (in short: "TRUSTS T&C" or "TC") is drafted and presented. This draft makes a proposal of what a T&C could look like when TRUSTS goes into 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 data market. It is self-evident that certain contract-relevant decisions on organisation and structuring must still be formulated or left open in part in a flexible manner 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 trading platform but does not regulate the legal form of the operating company.

5.3.2 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 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" are exchanged and traded on the TRUSTS platform. Data are digitally coded characters or character strings that can be processed directly with the aid of automation.

(3) Transaction objects in TRUSTS are data in the form of digitally coded characters or character strings that can be processed directly with the aid of automation; this includes, in particular, static data, dynamically

provided and/or transmitted data (irrespective of the type of provision - e.g., via API or also via streaming) or computer programs.

(4) A participant in the TRUSTS data trading 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, "Buyer") or in any other function in data trading via the TRUSTS data trading platform.

(5) A participant in the TRUSTS data trading 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 data platform. 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 offered. After going through the intake process, a participant can offer data on the data platform.

(6) TRUSTS distinguishes the following functional roles: Data Provider, Data Demander and 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. The TRUSTS OpCo may demand remuneration in return.

   (b) Data Consumer (DC): a natural or legal person who requests data on TRUSTS and wishes to use data. DCs obtain data (data assets) via TRUSTS 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 trading 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.

5.3.3 Draft §2) Scope of the Terms & Conditions

(1) These Terms and Conditions govern the participation in the trading of data on the TRUSTS trading 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.

5.3.4 Draft §3) The operator: the TRUSTS operating company (TRUSTS OpCo)

I) Basics and Self-Conception

(1) TRUSTS OpCo shall promote and facilitate the effective trading of data.

(2) TRUSTS OpCo provides a technical infrastructure through which participants can exchange and trade data. One part of the data ecosystem is the TRUSTS data trading platform. Selected Data Providers (DP) and Data Consumers (DC) are admitted as participants to this trading platform.

(3) In its role as operator of the data platform TRUSTS, the TRUSTS OpCo itself does not act as a market participant, but only as operator of the trading platform. The data trading participants conclude the

exchange and trading contracts among themselves. In normal trading, the TRUSTS OpCo does not act as an intermediary but only operates the technical data trading platform.

(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 for an effective data exchange as a data marketplace TRUSTS. Furthermore, the TRUSTS OpCo shall support the DPs in the settlement of data contracts by offering a settlement system, providing data management services and consulting services (see services of the OpCo in § 3 No. II).

(6) In order to be able to carry out data- or volume-related settlements, the TRUSTS OpCo shall establish a monitoring system to accompany the data trading on the trading 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.[48]

II) Services of TRUSTS OpCo

(1) Provision of the data trading infrastructure: TRUSTS OpCo shall ensure the functionality of the trading platform. TRUSTS OpCo shall ensure that the functionality of the trading 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 a usage-based billing service that data market participants can optionally use. The DP and DC in particular, as providers and consumers of data, have a great interest in a comprehensible usage-based billing. If the market participants make use of the billing service, the following shall apply:

   a. In order to be able to use the settlement service, the market participants register with a user account at TRUSTS (specified as DP/DC). By assigning the data transactions to a user account, the trading activities are recorded and thus made billable. In connection with the user accounts, the market participants provide TRUSTS OpCo with contact and invoice data, VAT numbers and other necessary data upon request. In addition, upon request, market 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.[49]

   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 traded and will not be a party to any contracts between the DP and DC. The DP is the responsible

[48] A monitoring system is also necessary for free data trading 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.

[49] 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 organisations. Suggested clause, if applicable: "In addition, market participants shall make available on other information such as customer service contacts."

© TRUSTS, 2021

trader for all sales and 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 for providing all legal information for data it sells. This is done so that TRUSTS OpCo, as the operator of TRUSTS, is at all times immune from liability and can also warn and sanction any infringements of copyright or other rights by market participants (such as trading in unlicensed data). Data providers (DPs) in particular are obliged to be especially transparent with regard to the legality of the data offered. In particular, they are obliged to provide all necessary information correctly and completely.
d. TRUSTS OpCo undertakes to settle data trading transactions without delay. In the event that the settlement date of a data trade (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.[50]
e. Furthermore, the TRUSTS OpCo shall, if possible, provide the participants concerned with information on the reasons for the rejection in order 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. In order 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 in order 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 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 payable 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

[50] Note: depending on the chosen business model of the TRUSTS or on the amount and complexity of the data trading 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..

© TRUSTS, 2021

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, in particular fee debts, against any reserve or proceeds owed or debit a participant's bank account or other payment 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 in excess of 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 liable for 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 trading 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 as a result of force majeure, riots, acts of war or natural disasters or as a result of other events for which it is not responsible (e.g., strikes, lock-outs, 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 market participants in their contractual relationships with each other.

5.3.5 Draft §4) Trading System and Currency

(1) TRUSTS OpCo shall determine the trading currency and the settlement currency. It may determine that data assets are traded or settled in multiple currencies.

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

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

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

© TRUSTS, 2021

5.3.6 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 trading on the trading platform and the business relationship between the Participants.
(2) This includes, in particular, 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 market.
(3) Furthermore, the participants shall ensure the timeliness, accuracy, specificity and consistency of such communications.

5.3.7 Draft §6) Participation in Data Trading / 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 trading platform are entitled to participate in data trading on the TRUSTS data trading 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 trading. This due diligence shall include a review of the participant with regard to 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 trading onwards, a credit report must be carried out.[51]
(4) In addition to clarifying legal and administrative issues, the suitability test prior to data trading is also particularly concerned with proving that a participant can appropriately and securely handle the data to be traded or acquired and is committed to doing so. It must be ensured that all aspects relevant to data protection are comprehensively taken into account and that the data to be traded are secure and uncompromised from third parties during trading, 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 traded and that they are also allowed to trade it (clarification of licensing issues before trading begins).
(6) After sufficient verification of the market participants, the TRUSTS OpCo shall decide on the granting of permission to trade data on the TRUSTS data trading platform.
(7) TRUSTS OpCo may refuse to grant permission for data trading on the data trading platform if there are justified circumstances in the person or organisation of the data trader which give reason to suspect that the principles of data trading 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.

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

© TRUSTS, 2021

(8) TRUSTS OpCo may also refuse or withdraw permission to trade data via the data trading platform if participants trade in data assets that are pornographic, glorify violence, are defamatory or otherwise contrary to common decency. Trading or providing links to such offers may also result in exclusion from data trading 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.[52]

(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 in particular if insolvency proceedings have been opened against the participant's assets.

5.3.8 Draft §7) Data Trade, Data Transmission and Archiving

(1) If a data trade is concluded via the TRUSTS data trading platform, the data trading participants undertake to fulfil the obligations incumbent upon them under the respective contract in accordance with the agreements.

(2) The data provider (DP) undertakes to transfer the traded data assets to the data consumer (DC) for use and / or for utilisation in accordance with the agreed transfer of use and / or utilisation.

(3) After the trade 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 making available without delay. For this purpose, information on the trade itself is transmitted, but not the data itself (this is only exchanged between the DP and the DC).

(4) In order to be able to ensure the overall quality operation of the TRUSTS data trading platform, the TRUSTS monitoring system will learn the most important key data of each data trade.

(5) The data trading Participants undertake to comply with the general and statutory compliance rules and the Code of Conduct.

(6) The Participants in data trading undertake to:

   a. that the use of the trading 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 traded and that the applicable criminal laws are complied with,
   c. that the protection of the data takes into account the recognised principles of data security and that the obligations of the applicable data protection regulations are observed; 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 trading are obliged to promptly inform TRUSTS OpCo before, during and after the entire duration of the trade of all circumstances relevant to the orderly trading 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.

[52] This paragraph enables OpCo, for example, to keep providers of link collections away from the data trading 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 traded on TRUSTS in order to be able to curb abuse.

© TRUSTS, 2021

(8) The DP warrants that it holds the necessary rights to the data to be traded (sole, one-time, permanent, etc.).
(9) The DC undertakes to perform the obligations arising from the data trade 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.

5.3.9 Draft §8) Fees for the Use of the Trading Platform TRUSTS

(1) TRUSTS OpCo shall provide the Participants of the TRUSTS data trading platform with the infrastructure necessary for data trading and the participants shall pay TRUSTS OpCo a fee in return for the provision of the data trading 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 provision of data, as they typically arise between the data trading partners DP and DC, are not considered here, but are the subject of the contractual agreements between DP and DC.
(4) TRUSTS OpCo may provide in particular for the following non-exhaustive list of fee categories in the fee schedule:

    a. Fees for the provision of the data trading infrastructure ("service provision")
    b. Fees for the provision and trading of data ("pay-per-use")
    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.

5.3.10 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.
(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 taking into account the legitimate concerns of the participant. An important reason exists in particular 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 TRUST or jeopardise its public reputation, or
    c. circumstances subsequently arise in the person or organisation of the participant which no longer fulfil the requirements of § 6.
(4) A Participant in the TRUSTS data trading 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.

© TRUSTS, 2021

5.3.11 Draft §10) Dispute Resolution Procedure

(1) In the event of a dispute of any kind between TRUSTS Trading 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 use arbitration. If not specified elsewhere the law of Belgium and the Court of Brussels shall be called 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 may be made at any time.
(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.

5.3.12 Draft §11) Miscellaneous

(1) All business relations under these Terms and Conditions shall be governed exclusively by European 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) The place of place of data processing is defined as within European Union. The regulations regarding PII / GDPR for personal data processing are applicable. The data protection and security regulations of European Union are applicable.
(4) TRUSTS OpCo reserves the right to decide on changes to the Terms and Conditions. Changes to these Terms and Conditions will be offered 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 the participant does not notify TRUSTS OpCo in writing or electronically of any rejection 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 trading 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 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 in the event that the Terms and Conditions prove to be incomplete.

© TRUSTS, 2021

6 Conclusions and Next Actions (M18-36)

This document is to be considered preliminary, as it reflects the plans that the partners have at the current stage of the project. A completed and more detailed version of the business models will be released at the end of the project, together with the cost analysis and the final business strategy.

IPR protection requires a global approach across all four pillars: data and analytics, supply chain integrity, coordination and integration, and transparency and awareness. Both private and public sector stakeholders could benefit from a future state that enhances IPR protection. The ultimate goal is to enable all countries to set up a consistent and uniform approach to IPR promotion and protection, so goods flow freely across borders.

1) Governments and companies cannot work in silos and expect to see IPR protection results. The four-pillar solutions together can contribute to a secure ecosystem for global IPR.
2) Pursuing analytics solutions tailored to stakeholder needs can help each stakeholder group to detect potential corruption points and deter further corruption. EKG, or graph technology, is becoming increasingly powerful at identifying trends, detecting suspicious activity, and deterring bad actors.
3) Supply chain integrity is important from end to end; supply chain solutions, such as blockchain technologies, can assist government and commercial clients in monitoring their business partners and entities of interest for indications of risk and securely storing supply chain information.
4) Coordination and integration can provide governments with the information they need to enable a smart flow of goods across borders—promoting legitimate trade and travel while deterring illicit activity.
5) Transparency and awareness between governments and stakeholder groups can provide much-needed information on IPR and prompt partnerships for stakeholders that want to have transparent supply chains.

IPR affects everyone. Governments with strong regulations, enforcement agencies, and border management alongside IPR owners with secure supply chains can facilitate a more prosperous and protected economic trading system.

6.1 Conclusion: Implications and recommendations for 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.[53] 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.

- to work together to deter and prevent future IPR violations:
- Marketplace:
    - Analyse customer/end-users' reviews on TRUSTS product to identify issues.
    - Perform due diligence on providers to minimize IPR violations; the objective is to do business with trusted partners.

Digital platforms are uniquely positioned to create and capture value in the digital economy.

[53] 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.

© TRUSTS, 2021

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 legal and secure framework that will ensure the protection of the data that are made available in terms of privacy and infringement protection. It was a common suggestion from most of the participants that TRUSTS should respect and safeguard data access according to the international, European and national data protection laws and regulations (e.g., GDPR). Also, compliance with 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. Remarks 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 functionality in the most productive way. This approach will conclude to the mitigation of 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 datasets and services and on the other hand the validity 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 by all the participants is their need to use TRUSTS as a one-stop-shop service, through which they can find, bid for and buy available datasets 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 as to be supported by TRUSTS is the implementation of flexible pricing models able to be 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 by the interviews was the need for user management. In more details, within the TRUSTS environment, the users need to feel protected since they deem to make monetary transactions. 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 products that fit in their need, in a timely manner, as well as be able to announce to the marketplace needs for datasets and services.

© TRUSTS, 2021

Inherent protection of private datasets should be provided.

Many of the interviewees need to gain access to private data, which many times might originate from the processing of sensitive / personal data. Thus, the protection of such datasets through anonymization mechanisms that will be able to be applied on the datasets during their onboarding process and before they are published, 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 private anonymized data that the TRUSTS users' aim to publish. Finally, private datasets intersection, through cryptographic techniques that allows two parties to combine data in an encrypted manner to be able to compute their intersection (all relevant protection approaches can be applied e.g., PSI/MPC, masking common parameters to datasets that are used for correlation, etc.), is also very welcome.

6.2 Conclusion: Implications and recommendations for establishing the future TRUSTS operator

One of the goals of the TRUSTS project is the conception and establishment 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 the different WP of the TRUSTS project, the relevant aspects for setting up a TRUST platform are considered (technology, legal, business, operation, etc.). As described in chapter 2, 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)

In order to be able to protect the IPR of the users of the TRUSTS platform even better in the future, a further elaborated concept is needed on how these six aspects mentioned above can be supported even more. 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 users of the future TRUSTS platform, points 3, 4 and 5 are probably the most interesting. IP infringement incident reporting and sanctioning in particular 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 for 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

a) Cross-system mapping of data assets: For the DP customers of TRUSTS OpCo, it could be interesting in the future to have all information offered by the DP 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

© TRUSTS, 2021

creation to data release, a new approach to quality control and monitoring of data assets can be established. The IDSA is already in the process of conceptual implementation with the approach mentioned in chapter 4.

b) Actualization of meta data from Decentralised data storage and data networks: Due to the conceptual approach in the TRUSTS project that data is held decentrally at the data providers and not centrally at one location as in conventional data platforms, necessities arise with regard to synchronization mechanisms and availability. If a DP 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 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 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 a peer-to-peer synchronisation mechanism for the up-to-dateness of metadata that has yet to be developed. Here, it is particularly important to obtain ongoing information about availability, releases, contracts, etc. The IDSA is working on corresponding concepts and also interfaces for data exchange.

c) 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 the contracts with standard and default smart and an overall improvement of the policy engine could be an important task for the future TRUSTS OpCo. If more contracts can be automated, more user requirements can be met. The automated creation, distribution and reconciliation of contracts is an important function here. The TRUSTS platform has already done important preliminary work here, but for a productive system it seems necessary that these functions are further expanded. In the future, the TRUSTS data ecosystem could consist of decentrally operated software components that network with each other and form a consensual network that forms 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, 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). The Austrian research project DALICC (www.dalicc.net) has developed interesting approaches to managing contracts.

© TRUSTS, 2021

6.3 Next Action: Agreement about IPR of software used within TRUSTS consortia (M18-M36)

One goal of the TRUSTS project is the conception of a future TRUSTS OpCo (or finding an alternative operating company). For the operation of a future TRUSTS platform, both the technical, legal and administrative aspects for the operation need to be clarified. This report deals with the technical and some legal aspects, how IPR of the users of the TRUSTS platform can be protected and what concepts exist for this, what steps have already been taken for implementation and what will still be necessary in the future.

For the establishment and operation of the future TRUSTS OpCo, it will be important especially towards the end of the TRUSTS project at the latest to obtain clarity about the rights of use of the software components developed during the project. This is because the question of the use of the developed software has a direct impact on the business model and the possibilities of using the software components at all or even economically.

It is therefore essential to deal with this topic in the second half of the project: under what conditions are the consortium partners of the TRUSTS project willing to bring in their software in the future TRUSTS platform?

The type of licence to use and the level of user fees have a direct impact on the profitability of the future operating company (TRUSTS OpCo). If the licences / prices for using components are too high, this could reduce the margins that can be achieved from a data transaction with market participants for the TRUSTS OpCo. If prices are too low, the owner of the software components and its developer may not be able to operate or develop further the components economically.

Both variants would be more than disadvantageous for a sustainable operation of the future TRUSTS platform and TRUSTS OpCo.

In order to transfer the TRUSTS platform developed in the TRUSTS project into sustainable operation by the TRUSTS OpCo, it is necessary to clarify the rights of using software components in each case at an early stage and to establish a contract amongst the TRUSTS consortia partners that enables the future TRUSTS OpCo to ensure economically viable operation of the TRUSTS platform. To this end, the interests of the parties involved must be taken into account and a well-balanced (contractual) solution found.

In research projects, a mixture of different types of rights of use can always be found: some rights remain with the consortium partner who developed the software beforehand and now contributes it to the project and develops it further through the funding. In this case, the rights to the software usually remain with the contributing organisation. On the other hand, the funding institutions take the view that things developed with publicly funded money and their rights of use then also belong to the public.

This is a structural conflict of interest. This potential conflict should be addressed in the second half of the project (M18-M36) in order to find a viable solution for the later TRUSTS OpCo before the end of the TRUSTS project.

From today's perspective, two things should be regulated in the planned agreement within the TRUSTS consortium:

1) Use of the consortium partners' software IPR by the future TRUSTS OpCo.
2) Further development and support of the TRUSTS software modules by the consortium partners.

© TRUSTS, 2021

Use of the consortium partners' software IPR by the future TRUSTS OpCo.

The following is a suggestion of how the process of establishing a balanced contractual agreement within the consortium could look like. The objective is, to develop a balanced agreement for the use of the consortium partners' software IPR by TRUSTS OpCo.

Proposed steps for M18-M36:

a) **Agreement on the process:** the consortium adopts the procedure proposed here for establishing a sustainable agreement and adopts a procedure model.
b) **Identification of the software components used:** first, an overview and list of all open source and proprietary software components used will be compiled. Each consortium partner will enter the software components it uses in a common catalogue in a form yet to be chosen.
c) **Software-technical requirements profile of the TRUSTS platform ("must-have", "good-to-have", "nice-to-have"):** after determining which types of software are to be used under which licence, a software-technical requirements profile of the planned TRUSTS platform will be drawn up. A distinction should 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").
d) **Licence overview:** The next step is to look at the licences used for the software modules with regard to overlapping, complementing and/or contradicting each other. Modern software often contains numerous open source software components with different licence rights - and it is therefore important to get an overview of the licence types used. It is suggested to use the methodology and analysis tools from the Austrian research project DALICC (Data Licenses Clearance Center under the lead of University of Applied Science, St. Pölten, Austria, www.dalicc.net) and to analyse the licences found in the previous step in the way tested and established in the DALICC project.
e) **Licence specifications:** after identifying and describing the licence types used, a specification of the possible future licence use is drawn up - especially for proprietary licences (such as: pay-per-use, open-access, research, business and so on).
f) **Comparison with the intended business model:** the next step is to find out what impact the selection of one of the discussed business models will have on the intended selection of software components (are they all needed in this way or perhaps additional apps/services?)
g) **Drafting a framework agreement for software use:** in parallel to the above steps, a framework agreement is drafted that regulates the future software use by TRUSTS OpCo and the consortium members (and possibly other providers).
h) **Negotiation for software use by TRUSTS OpCo:** Negotiation and drafting of an agreement with each individual rights holder regarding the future use and maintenance of the software components used in the TRUSTS platform.
i) **Conclusion of the TRUSTS agreement on IPR use by TRUSTS OpCo: finally**, the signing of a sustainable agreement by the entire TRUSTS consortium is sought.

© TRUSTS, 2021

Further development and support of the TRUSTS software modules by the consortium partners.

Similar to the above proposed process (of agreeing on the future use of the software components necessary for operationg the TRUSTS platform) there need to be a sustainable agreement of the TRUSTS consortium on the issue of support, maintenance and further development of the software components.

a) A**greement on the process:** in the consortium, the procedure proposed here for establishing a sustainable agreement is accepted and a procedure model is adopted.
b) **Development needs of the software components used:** starting from the software components selected above, the presumed development needs will be collected and estimated. Each consortium partner will enter the planning for the further development of the software components in a common catalogue in a form still to be chosen.
c) **Software-technical development roadmap of the TRUSTS platform ("must-have", "good-to-have", "nice-to-have"):** after ascertaining which software components should be further developed when and how, a software-technical development roadmap of the planned TRUSTS platform will be drawn up. The aim is to distinguish which components must be further developed for the basic operation of the platform ("must have"), which could be useful additions ("good to have") and which developments are rather optional ("nice to have").
d) **Development overview:** A TRUSTS software development plan is then drawn up, listing the planned or sensible development steps with a horizon of perhaps 2-3 years.
e) **Support and maintenance specifications:** after the TRUSTS software development plan has been drawn up, the support and maintenance efforts are specified and elicited.
f) **Drafting of a framework agreement on support, maintenance and development:** in parallel to the above steps, a framework agreement will be drafted to govern future software development / support / maintenance by TRUSTS OpCo and the consortium members (and other providers, if applicable).
g) **Negotiation of future expenses by TRUSTS OpCo or consortium partners:** Negotiation and drafting of an agreement with each individual rights holder regarding support, maintenance and further development of the software components used in the future TRUSTS platform.
h) **Conclusion of the TRUSTS agreement for the further development of the TRUSTS components:** finally, the signing of a sustainable agreement of the entire TRUSTS consortium is aimed for.

These two processes mentioned above will be the focus of the work in the M18-M36. The successful implementation of these processes will provide TRUSTS OpCo with the necessary planning certainty for the establishment and operation of the future TRUSTS platform.

© TRUSTS, 2021

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

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.

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

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

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.

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*.

© TRUSTS, 2021

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

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).

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.

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*.

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

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

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.

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.

© TRUSTS, 2021

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.

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

© TRUSTS, 2021