D1.2 Annual Public Report I

Author: TRUSTS Consortium

Contractual Due Date: 31 December 2020

TRUSTS Trusted Secure Data Sharing Space

D1.2 Annual Public Report 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	D1.2 Annual Public Report I		
Work Package	WP1		
Contractual due date	31/12/2020	Actual submission date	21/12/2020
Nature	Report	Dissemination Level	Public
Lead Beneficiary	LUH		
Responsible Author	TRUSTS Consortium, coordinated by LUH		
Contributions from	All TRUSTS WP Leads and participants; Alexandra Garatzogianni, Patricia Jozwiak, Angelina Kraft (LUH/TIB), Ioannis Markopoulos (FNET), Benjamin Heitmann (FhG), Christoph Lange (FhG), Ilan Goldberg (EMC), Gianna Avgousti (eBOS), Charlotte Ducuing (KUL), Yuliya Miadzvetskaya (KUL), Lidia Dutkiewicz (KUL), Andreas Huber (G1), Bert Utermark (G1), Nina Popanton (DIO), Manuela Schlömmer (DIO), Petr Knoth (RSA), Ana Maria Florea (REL)		

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete[1]	Changes	Contributor(s)
v0.1	08/10/2020	20%	Initial Deliverable Structure	Patricia Jozwiak and Alexandra Garatzogianni (LUH/TIB)
v0.2	03/12/2020	80%	Content	Alexandra Garatzogianni (LUH/TIB), Patricia Jozwiak (LUH/TIB), Angelina Kraft (LUH/TIB), Ioannis Markopoulos (FNET), Benjamin Heitmann (FhG), Christoph Lange (FhG), Ilan Goldberg (EMC), Gianna Avgousti (eBOS), Charlotte Ducuing (KUL), Yuliya Miadzvetskaya (KUL), Lidia Dutkiewicz (KUL), Andreas Huber (G1), Bert Utermark (G1), Nina Popanton (DIO), Manuela Schlömmer (DIO), Petr Knoth (RSA), Ana Maria Florea (REL)
v0.3	17/12/2020	90%	First and Second Review	Andreas Trügler (KNOW), Victor Mireles-Chavez (SWC)
v1.0	21/12/2020	100%	Final Version	Patricia Jozwiak and Alexandra Garatzogianni (LUH/TIB)

[1] According to TRUSTS Quality Assurance Process:

1. to be declared

Disclaimer

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
BV	Business validations
DL	Deep Learning
DMP	Data Management Plan
DoA	Description of Action
DS	Data Stewardship
DSM	Digital Single Market DSM
E2E	End-to-End
EOSC	European Open Science Cloud
FAIR	Findable, Accessible, Interoperable, Reusable
FL	Federated Learning
FR	Functional Requirements
GA	Grant Agreement
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
IDS	International Data Space
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
MPC	Multi-Party Computation

MVP	Minimum Viable Prototype
RAM	Reference Architecture Model
SAB	Stakeholder Advisory Board
SLA	Service-Level-Agreement
TV	Technical validations
UC	Use Case
WP	Work Packages

1 Executive Summary

The objective of this **Annual Report I** is to report the project's progress and status in the first year of the TRUSTS Project. For Each Work Package (WP) and for each specific Lead there are reports on overall objectives, achieved progress in the first project year and the next steps. Chapter 3 shows the first year progress within all nine Work Packages, Chapter 4 outlines a strategic level, shown for the Leads that were defined for TRUSTS: Scientific Lead, Technical Lead, Innovation Lead, Security Lead, Legal & Ethical Lead, Communication & Community Building Lead and Business & Exploitation Lead. Chapter 5 is an update of the Data Management Plan, containing State of the Art, DSM, GDPR and FAIR Data Activities by partners and Processed and published data sets in the first year of the TRUSTS Project.

2 Introduction

The main purpose of this document is to give an overview on the project's progress in the first project year of TRUSTS, targeting the general public. This report consists of separate reports for each Work Package and for each specific Lead and an update of the Data Management Plan.

2.1 Mapping Projects' Outputs

Purpose of this section is to map TRUSTS Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to TRUSTS GA Deliverable & Tasks Descriptions

Task	Respective Document Chapter(s)	Justification
T1.1 Project Management This task deals with the necessary project management tools, mechanisms and structures for the high quality, efficient and timely administrative coordination of the project. It incorporates Administration Management activities, including procedures and guidelines for activity planning and monitoring, cost and time management, submission of periodic progress reports and cost statements, preparation of annual review reports, review presentations, and timely submission of high	Section 3 - Section 5	Section 3: Progress within Work Packages (WP) Section 4: Progress within specific Leads Section 5: Data Management Plan

quality deliverables to the Commission.		
Deliverable		
D1.2 Annual Public Report I Report on the project's progress, targeting the general public. The report will focus on the impact of the conducted work.		

2.2 Deliverable Overview and Report Structure

This Deliverable (D1.2) is a report on the project's progress in the first year of the TRUSTS Project and consists of the following Sections. Section 3 contains reports of the objectives, the achieved progress and the next steps of each of the nine TRUSTS Work Packages. In Section 4 the objectives, the achieved progress and the next steps are specified for Scientific Lead, Technical Lead, Innovation Lead, Security Lead, Legal and Ethical Lead, Communication and Community Building Lead, Business and Exploitation Lead. The project's Data Management Plan (D1.6) lists all relevant information on current and planned data management activities. It will be regularly updated to reflect the development and progress of the project in M24 and M36. Section 5 contains a first update of the Data Management Plan. Conclusions are outlined in the last Section 6.

3 Progress within Work Packages (WP)

3.1 WP 1 Project Management

3.1.1 Objectives

The Project Management Work Package serves the objective to ensure the timely, successful and impactful delivery of the project's results in compliance with EC regulations and the H2020 framework. This is achieved via the hands-on and continuous monitoring of the implementation and completion of the project's tasks, activities, milestones and deliverables, safeguarding thus their proper and timely development according to the Description of Action (DoA) and the project's work-plan, while ensuring the successful, smooth and efficient collaboration among the Consortium partners. The activities of the project management work package focus on establishing tasks, providing thus guidance and direction to achieve the goals of the H2020 TRUSTS project, ensuring continuous, proactive communication with the European Commission, establishing efficient means of communication and document exchange between partners, ensuring transparency at all levels and in terms of reporting by establishing appropriate report structures and procedures, conducting quality assurance activities and performing risk analysis tasks, coordinating the

organisation of project meetings and other possible participatory events where the project could be presented and ensuring that project objectives are realised within set time, quality and budget.

3.1.2 Progress achieved

In terms of project management, LUH, as WP Lead since the start of the project and with the unanimous agreement of all Consortium Partners has selected and used all necessary project management tools, mechanisms and structures with the objective to ensure the high quality, efficient, smooth and timely administrative coordination of the project, as outlined in the Project Management Plan (D1.1), which incorporates Administration Management activities, including procedures and guidelines for activity planning and monitoring, cost and time management, submission of periodic progress reports and cost statements, preparation of annual review reports, review presentations, and timely submission of high quality deliverables to the Commission. LUH is responsible for the day-to-day coordination of project-related activities, monthly telcos of WP1, during which the progress of each WP is reported at Consortium level, online Plenaries with the duration of two full days every six months during the COVID-19 times, as well as the administrative management of the project, ensuring that contributions are made by all Consortium partners (i.e. participation in project meetings, teleconferences, taking over responsibilities, reporting, coordination of allocated WPs and tasks) according to the GA. As outlined in the Technical and Quality Assurance and Risk Assessment Plan (D1.5), the appropriate processes and instruments have been set up and are used for the continuous quality monitoring and risk assessment of the project.

The project's Data Management Plan, DMP, (D1.6) lists the technical and organisational measures regarding the handling and storage of data, such as the research data volume, access, licensing and integration features, in accordance with the relevant legal framework and in particular the GDPR. Moreover it details data characteristics, privacy preserving security plans and authorisations and answering data security and privacy questions, such as where the data will be physically processed and what physical security protection features and privacy protocols will be implemented. The DMP will be regularly updated to reflect the development and progress of the project in terms of Data Management. Its updates are and will be incorporated in the current and upcoming versions of the Annual Public Report at the respective dedicated chapter, and upon request by the EC the DMP can also be documented and submitted as a separate deliverable.

3.1.3 Next Steps

In consideration of the ongoing internal reporting activities and status updates from all WP and task leaders, it can be deduced that the project proceeds according to schedule. LUH will continue its provision of support and guidance to all partners, ensuring that potential items are addressed proactively and that the necessary conditions ensuring the smooth and impactful delivery of the project's results, as stated in the GA, are and continue to be in place. The progress of WP1 will be further reported in the upcoming versions of the Annual Report, the DMP and upon request by the European Commission. The daily monitoring of the project by the team of the Coordinator will continue to be implemented as outlined in the Project Management Plan and the Technical and Quality Assurance and Risk Assessment Plan. Adjustments will be made when and if deemed necessary by the Consortium.

3.2 WP 2 Requirements Elicitation & Specification

3.2.1 Objectives

The overall objectives of WP2 as defined in the DoA are:

- to analyse the EU and worldwide challenges and trends and to define the requirements for the provision of a multi, concurrent and cross-domain, secure and scalable end-to-end (E2E) data marketplace service.
- to define detailed and functional industry specifications appropriate for a data marketplace linked to specific target KPIs considering and bridging the vertical user point of view (PoV) with the analytics/solution provider PoV and the data marketplace platform provider PoV.
- to produce a set of KPIs and methodologies to enable:

  (a) the technological and business validation of the E2E data marketplace service and associated control and management within and across verticals;

  (b) the definition of the test reports format, parameters, test points, and benchmarking of the results for a unified and reliable outcome.

During the first year of the project, WP2 focused on:

- Initiating the analysis of the worldwide data marketplace ecosystem in terms of status, markets, trends, success and failure stories. This work will be correlated with the business model analysis in task T7.1 to define valuable techno-economic characteristics that will lead to a successful TRUSTS platform implementation and business model.
- The analysis of a wide variety of sources (online surveys, stakeholders interviews, state of the art, legal/regulatory framework and use cases) in order to define the TRUSTS functional requirements as well as the use case high level scenarios, architectures and KPIs. The work continues in Year 1 towards defining the detailed scenarios, based on the high level ones, to drive the WP5 trials.
- The definition of the trials evaluation testing methodology and the respective business evaluation methodology. The methodology required acceptance test procedures for conducting both the technological and business validations of the UC's considering the associated service management. The objective is to validate the three UC's - business wise - and develop business plans for the UCs with the highest commercial potential.
- The definition of the initial version of the TRUSTS platform architecture. The architecture represents the conceptual foundation for the implementation of the TRUSTS platform, and therefore reaching a consensus on the architecture enables all project partners with a technical view to agree on the most important abstract decisions, before realising them in their implementation. In addition, the architecture also allows the project partners with a non-technical view to contribute with cross-cutting requirements of strategic importance, such as having future proof characteristics e.g. compliance to GAIA-X concepts.

The work in WP2 is organised in 4 tasks as illustrated in the figure below:

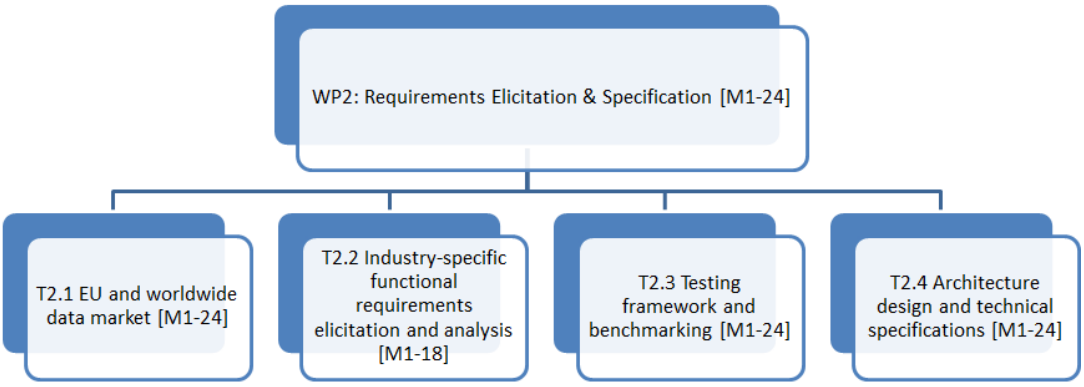

Figure 1: Tasks in Work Package 2

3.2.2 Progress achieved

In the following, year 1 progress is reported as per task:

Task 2.1: EU and worldwide data market

This task does not produce a deliverable within year 1. The first task deliverable entitled "D2.1: definition and analysis of the EU and worldwide data market trends and industrial needs for growth" is due on month 18. Nevertheless, the respective work started by defining the table of contents, the responsibilities per section, the survey for state of the art in the data marketplaces ecosystem, vertical markets, trends, success and failure stories. Evaluation of the initial input has already started. In order to increase insight validation by external experts was considered to be of importance. The initial plan was to present to the Big Data Value Forum, but since this event will be completely online, it was decided to create focus groups with external experts. A workshop is under preparation together with T7.2 on stakeholder engagement. Within the task, initial results have already been discussed with the consortium within an internal workshop on data market taxonomies and positioning of TRUSTS' results, prepared in cooperation with T7.1.

Task 2.2: Industry-specific functional requirements elicitation and analysis

The main focus of Task 2.2 was to perform a systematic survey of various sources in order to define the initial set of the TRUSTS Functional Requirements, the high level UC scenarios, the respective architectures and evaluation KPIs.

The means to collect the requirements were through:

1. key stakeholders' interviews,
2. the use of dedicated electronic surveys,

3. the analysis of selective related data marketplace activities,
4. the analysis of related legal framework,
5. the analysis of the use cases.

The context in which the requirements are analysed is the TRUSTS project objectives. The methodology to produce and use the TRUSTS data marketplace FRs is illustrated in the Figure below. In particular:

- The justification and individual requirements of all sources are analysed.
- The above-mentioned requirements drive the definition of the FRs, which will be used for the implementation of the TRUSTS platform as well as the operational processes design.
- To assist implementation, each FR is mapped to the respective project task.
- Furthermore the FRs will be used by the methodology defined in task T2.3 entitled "Testing framework and benchmarking" in order to evaluate and provide coherent feedback through the UC trials (WP5).

Figure 2: Methodology to produce and use the TRUSTS data marketplace Functional Requirements

This work is reported in the D2.2 deliverable entitled: "Industry specific requirements analysis, definition of the vertical E2E data marketplace functionality and use cases definition I" which was submitted on time on month 6. In brief, the requirements elicitation process involved:

- cooperation with the Safe-DEED HORIZON 2020 project (no 825225), in which an in depth legal analysis was made, in order to derive the respective requirements
- analysis of the state of the art of Data Market Austria and industrial information

- performance of an online survey in which 31 professionals[2] responded and
- performance of 12 interviews
- in depth analysis of all UCs in terms of required TRUSTS functionality, high level trial scenarios, success criteria and KPIs.

The outcome was the definition of a comprehensive set of 44 functional requirements touching upon all aspects of the end to end TRUSTS environment operation. The outlined Functional Requirements are technology agnostic since they do not aim to set the implementation framework but rather the required functionalities and processes of the TRUSTS data marketplace.

The work in Tasks 2.2 continued by:

- Defining detailed UC trial scenarios, in collaboration with all UC partners, based on the scenarios description template produced within the Task 2.3.
- Participates in the TRUSTS architecture definition from the Functional Requirements and UCs point of view in collaboration with the Task 2.4.

Task 2.3: Testing framework and benchmarking

The submission of D2.4 in June 2020 was accomplished, addressing the work that has been performed under this task, defining the methodologies for the Business and Technological Validations of the TRUSTS platform within and across each vertical UC. The production and assessment of the methodologies for the testing, validation and benchmarking of the results as well as for the technological and business validation of the UC's through an agile-based iterative process approach were defined. Also, the architecture of the validation toolset to be used for the test case validation was defined including both business and technological validations along with the commercial value testing and user's experience for TRUSTS data marketplace.

Three sets of business validation and two sets of technological validation have been identified, allowing the interaction between the business needs, business models and the technological enablers, over the projects' lifecycle. Business validation will be implemented throughout business validation templates, functional requirements templates and business questionnaire templates as created with close collaboration with all WP2 participants, as presented and descripted in depth in Deliverable 2.4.

The 1st Business Validation as per D2.4, was completed by October 2020, as presented as well in figure 3 below. The questionnaires from the three UCs were gathered along with the table template formed as per D2.4 about the functional requirements and it was checked if anything has changed until M10 or if all FR's were still applicable to each UC. The output of the 1st Business Validation enabled the business modelling under WP7 (T7.1), gave an input back to WP2 (T2.2, T2.4) but also to WP3 (''platform implementation''), and WP4 (T4.1, T4.2 and T4.3 "Privacy preserving and data anonymization").

[2] It should be noted that due to COVID-19 lockdown and the limited time since the project commencement a few number of responders provided feedback to the questionnaire. Nevertheless, the questionnaire responses along with the interviews provided a solid ground for the identification of the stakeholder requirements.

In collaboration with WP3 and WP4 business validation actions were performed. In particular, a questionnaire was given to align and to clarify the purpose of WP4 with the UC definitions and requirements. (Example questions of the survey: What is the approximate amount of data expected to have in each data set? Is the data public or private?). The feedback (provided by the UC owners) in this questionnaire will affect the work needs to be performed in WP4 & the platform architecture related to T2.4 as well as the platform development and integration related to T3.5. EBOS as a Task Leader, also created a template for the scenarios definition and mapping of the functional requirements to MVP functionalities, through working closely together with FNET and FORTH.

Task 2.4: Architecture design and technical specifications

The work in Task 2.4 during year 1 focused on the definition of the TRUSTS architecture and the production of the deliverable D2.6 entitled: "Architecture design and technical specifications document I". Based on the market analysis and requirements elicitation outcomes that are performed in T2.1 and D2.2, as well as the legal and ethical frameworks and requirements generated in T6.2, this task dealt with the specification of an architectural design of the TRUSTS platform. Towards defining the TRUSTS architecture the T2.4 task evaluated existing specifications such as the Reference Architecture Model (RAM) of the Industrial Data Space (published by the IDSA, co-edited with FhG) and design documents of the Data Market Austria. In addition, it defined the necessary components to constitute the TRUSTS platform.

3.2.3 Next Steps

The next steps per task are:

Task 2.1: EU and worldwide data market

The next steps in T2.1 will focus on the production of the deliverable D2.1 entitled: "Definition and analysis of the EU and worldwide data market trends and industrial needs for growth" due on month 18.

Task 2.2: Industry-specific functional requirements elicitation and analysis

Deliverable D2.2 constitutes the first version of two reports containing:

- the detailed analysis of the requirements for a vertical data marketplace targeting at least the financial and telecommunications industrial sectors, and
- the use cases definition including the target KPIs that would set the benchmarking for the actual measurements.

The key strategic outcome from the analysis of the elicited requirements from all sources is that the overall TRUSTS objectives are in line with all the key stakeholders' expectations, thus setting the bar high for defining a successful service and having significant impact on the data industry.

Task 2.2 will continuously collaborate with:

- All WP1 tasks in order to evaluate additional information with respect to the TRUSTS architecture and data marketplace initiatives and trends,

- WP7 which will produce adequate business models and receive market feedback from any related exploitation action,
- WP6 which will define the legal aspects and processes,
- WP3 and WP4 which will undertake the platform development,
- WP5 which will execute the UC trials providing valuable feedback and
- WP8 to provide information and evaluate feedback from respective events.

The aim is to systematically assess the input from all designated sources in order to update the requirements driving the development of an imminently exploitable TRUSTS platform. In addition, a systematic process has been defined in order to update and produce the final set of the functional requirements to be reported in the deliverable D2.3 enitilted "Industry specific requirements analysis, definition of the vertical E2E data marketplace functionality and use cases definition II" due on month 24.

Task 2.3: Testing framework and benchmarking

Performance of each UC will be evaluated particularly from the KPI perspective to illustrate how the TRUSTS platform capabilities can be leveraged for different applications in each UC. The results will be used to address stakeholders' perspectives. According to the results received from each UC in every agile-based iteration, the WP will provide requirements and suggestions to further improve both functional and non-functional capabilities of TRUSTS.

Validation Type	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18
	Jan-20	Feb-20	Mar-20	Apr-20	May-20	Jun-20	Jul-20	Aug-20	Sep-20	Oct-20	Nov-20	Dec-20	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21
						MS1						MS2						MS3
WP2 - T2.3																		
Business Validation (BV)							1st BV											
UC trials													Preparatory activities - planning, setup of UC's + deployment			1st phase		
Deliverables						D2.4 (eBOS)												
Validation Type	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30	M31	M32	M33	M34	M35	M36
	Jul-21	Aug-21	Sept-21	Oct-21	Nov-21	Dec-21	Jan-22	Feb-22	Mar-22	Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22
							MS4											MS5
WP2 - T2.3																		
Business Validation (BV)					2nd BV							3rd BV						
Technological Validation (TV)	1st TV						2nd TV											
UC trials				Preparatory activities - planning, setup of UC's + deployment			2nd phase											
Deliverables						D2.5 (eBOS)												

Figure 3: Time plan of TRUSTS T2.3

Early Year 2, and as the demonstration tasks of WP5 will begin, and in order to prepare for the implementation and deployment of services in the first version of the MVP, created by WP3, we will map the FR's with the MVP functionalities with the help of the template created. This will be a continuous process with every MVP version available prior its demo UC trail.

Two more Business validations (BV) and two Technical validations (TV) will take place within the time plan as defined by WP5 leader and as stated in deliverable 2.4, also shown in Figure 3. The 1st BV was finalised in Year 1 (October 2020) by the UC participants, allowing the validation of the functional requirements as listed in D2.2 and since the corresponding business information has already been provided from all three UCs. The outcome was communicated to the respective partners as well as to WP3 and WP4 to take them into consideration during platform implementation and the investigation of privacy preserving technologies.

Later on, and within the beginning of the 1st phase of the UC trials, the 1st technological validation will be performed as shown in Figure 3, allowing the validation of the architectural framework and technical specifications (T2.4) along with the work for the 'Initial Platform and integration' under the T3.5. The 2nd BV will take place right after the completion of the 1st Technological Validation, and following the iterated process between the technological and business validations, from M23 to M24 (November 2021 – December 2021) the UC participants will again re-evaluate their needs from the business perspective that might have slightly changed or enhanced in a year from their 1st input.

The final Technical and Business Validations will be performed early in year 3 for a complete environment validation from a technical, quality, performance, expendability and business point of view.

During the whole implementation of T2.3 will continue to interact with:

- WP3 which will contribute to the TRUSTS Platform implementation,
- WP4 which will provide Privacy Preserving Technologies,
- WP5 which will proceed with the execution of the UC trials in order to provide a valuable feedback,
- WP7 which will contribute to the adequate business models, to the exploitation and innovation impact assurance.

The aim is to systematically assess the input from all involved parties in order to fulfil the objective of T2.3, by validating the three UC's business wise and developing business plans with the highest commercial potential. This work will be comprehensively analysed via the deliverable D2.5 entitled "Methodologies for the technological/business validation of use case results II" which is due in M24 (December 2021).

Task 2.4: Architecture design and technical specifications

In the second year, task T2.4 will focus on iterating the architecture based on feedback from the use case partners and from the non-technical project partners. Together with the use case partners, the technical environment for testing the use case trials will be defined in multiple, iterative versions. Complementary to that, the technical impact of the requirements identified in the area of business models for data marketplaces and the legal requirements will be investigated and will be addressed if necessary through updates of the architecture. In addition, the project partners with a technical perspective will refine the architecture and document additional technical specifications based on their implementation experiences in year two. The second iteration of the architecture deliverable D2.7 is scheduled to be completed in M24 (December 2021).

3.3 WP 3 TRUSTS Platform implementation

3.3.1 Objectives

This work package implements the requirements and specifications for the TRUSTS platform. To achieve this, it is composed of supportive, innovative and integrative tasks. The overall objectives of work package 3 are defined in the description of action as follows:

- Provision of infrastructure and operations tools and methods: Establish the technical foundations to deploy and operate the TRUSTS platform.
- Smart Contracts: Ensure the technical implementation of a smart contract feature in compliance with according regulations.
- Interoperability solutions: Provide implementations of concepts to achieve data exchange across various data market platforms and with the EOSC.
- Governance & Metadata: Define semantic descriptions and data models to support data interoperability, quality, lineage and data governance.
- Integration: Compile the results into a deployable, unified TRUSTS platform solution
- Brokering services: Develop intelligent recommendation algorithms that incorporate data analysis results (with respect to, e.g., platform interactions, or service description) in order to find and suggest potential collaboration opportunities between parties.

This work package aims to address the relevant requirements identified in WP 2 by providing implementations in the form of software artefacts, metadata artefacts and documentation. In particular, the functional requirements from task T2.2 and the requirements for testing and benchmarking from T2.3 guide the work in this work package. WP 3 is also in close alignment with WP 4, where privacy preserving technologies are investigated and developed that will enable TRUSTS to provide a safe, private and trustworthy environment for use cases with high requirements in the areas of security and privacy.

The results of WP3 are used in WP5 in order to provide the foundation for the use case trials. Three different use cases based on real world scenarios and involving a realistic subset of relevant stakeholders will be used to demonstrate the potential for TRUSTS.

During the first year of the project, WP3 focused on:

- The set-up of the development environment for the platform using state-of-the-art cloud infrastructure.
- Collecting the conceptual basis and requirements for smart contracts as an enabling part for the TRUSTS platform.
- Assessing the landscape of current data marketplaces and formulating a development strategy for data interoperability of TRUSTS with other data marketplaces.
- Collecting requirements from stakeholders and organisations related to data governance and formulating a development strategy.
- Testing and setting up an initial version of a minimum viable prototype for the TRUSTS platform through reuse and integration of existing components from both Data Market Austria and International Data Spaces.

- Collecting requirements regarding recommendation scenarios, data sources and software artefacts for the purpose of service recommendations and brokerage within the TRUSTS platform.

3.3.2 Progress achieved

In the following, year 1 progress is reported as per task:

Task 3.1 Infrastructure set-up and technical operations

The aim of this task is to provide a quick start environment for the development of the TRUSTS platform components. The platform provides a set of capabilities that enable operators to develop applications with a high degree of privacy-by-design features. The cloud-based environment for the development infrastructure set-up is using Google Cloud, which is compliant with the European laws and offers robust servers with tools to ensure data security with backup, monitoring and encryption. All the resources used in the project are located in Google's EU servers.

LSTech is employing DevOps and all the state-of-the-art mechanisms to support the architecture and specifications defined in T2.4 "Architecture design and technical specifications" (D2.4 months 12 and 24). The Docker environment allows easy implementation, extensibility, portability, and security, allowing the different containers to run quickly from one computing environment to another.

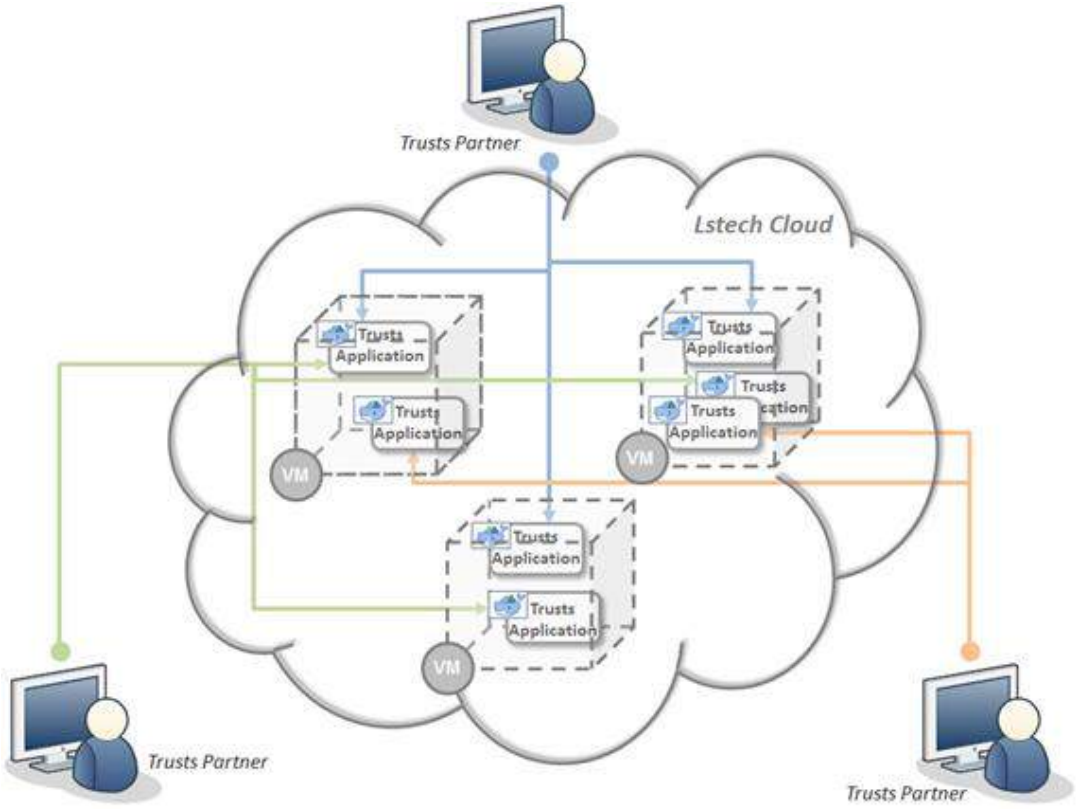

Figure 4: The development environment overview

TRUSTS technical partners have received instructions for accessing the environment and to run their application deployment on the shared Docker instances. LSTech is offering continuous assistance and technical support during the development of the infrastructure.

T3.2 Smart Contracts

Task 3.2 aims to create a conceptual description of smart contracts taking into account technical as well as legal aspects. In a first phase we have started to collect requirements of TRUSTS and Data Markets regarding smart contracts. Among all functional requirements from D2.2, the FRs 10 - 16 were considered as relevant. In addition, we have established some architecture requirements, including that we need certain policy definitions between a data consumer and data provider, on the basis of which we can define the smart contracts. Furthermore, a component to verify and log the smart contracts will be required.

We have also started to create a first pre-deliverable by the end of M12. This is mainly focused on general information about smart contracts.

T3.3 Data marketplace interoperability solutions

In T3.3, we are building interoperability solutions to connect TRUSTS with external industrial data markets. The goal is to identify interfaces and standards for exchange of data and metadata, and, if necessary, to develop own interfaces and standards. We are examining the technical capabilities of external data markets. Specifically, we are looking for machine-interoperable interfaces, currently focusing on REST APIs. It turned out that many or even most data markets do not provide machine-interoperable interfaces. Instead, they are silos where data processing and analysis reside inside the platform. Thus, we are focusing on a subset of data markets that have REST APIs readily available, i.e., Namara (app.namara.io), HERE (www.here.com), and CARTO (carto.com). The first data market, Namara, is a multi-purpose, many-to-many data market. Multi-purpose refers to the fact that it does not focus explicitly on a specific domain. It allows many-to-many relations, i.e. many suppliers can provide their data to many users. The second data market, HERE, focuses on the automotive industry. It is a single-to-many data market, i.e., the operator itself provides the data to their customers. The same is true for the third data market. CARTO, similar to HERE, is a single-domain market focusing on location intelligence in a single-to-many relationship.

We are planning to develop interoperability components for the selected set of data markets. The architecture of this component is shown in figure 5. This component will harvest data and metadata from third-party data markets using a harvesting module running on top of the IDS Trusted Connector. The harvested metadata will be stored in the TRUSTS broker, where it is accessible via the broker's search engine. Furthermore, data buyers will also be able to send requests for data, and potentially also to buy data from third-party data markets. All these requests will be forwarded to the third-party data market via the Trusted Connector, to guarantee a maximum of security. Upon completion of the interoperability component we will derive a set of guidelines and best practices, which will help data markets interested in becoming a member of the TRUSTS data market federator to build their own software components and to connect to TRUSTS via the Trusted Connector.

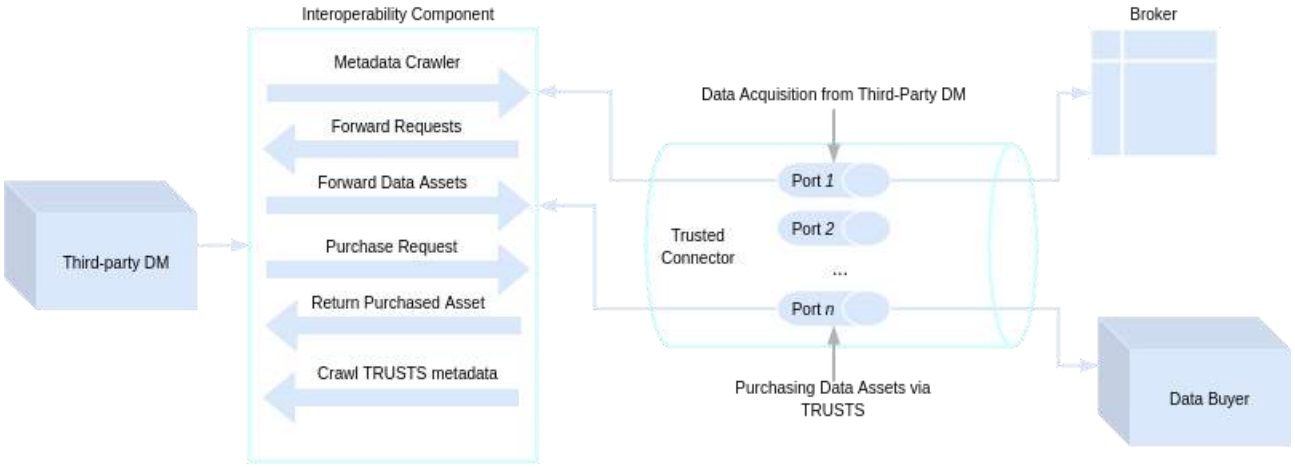

Figure 5: The system architecture of the interoperability component

T3.4 Data Governance: Metadata, Lineage and Semantic Layer

Task 3.4 aims at the definition of data governance and metadata management practices, as well as their implementation. Any development in this direction is subordinated to a good understanding of the different requirements coming from the different stakeholders and objectives in the TRUSTS project. In this respect, we have identified three major origins of requirements: i) those stemming from functional requirements specific to TRUSTS, as elicited by WP2, ii) those stemming from interoperability objectives as determined by task T3.3 and iii) those stemming from the general decisions taken in frames of the whole of WP3 regarding architecture, infrastructure and operation.

To address these requirements, the study of the following documents was undertaken:
Research Project Deliverables:

Table 2: Research Project Deliverables

Project	Deliverable	Title
TRUSTS	2.1	Industry specific requirements analysis, definition of the vertical E2E data marketplace functionality and use cases definition I
EOSC-Hub	10.3	Technical Architecture and Standards Roadmap v1
EOSC-Hub	10.4	Technical Architecture and Standards Roadmap v2 (draft)
DMA	4.4	Final Distributed Infrastructure Architecture Design
DMA	4.5	Final Version of the DMA Federated Cloud
DMA	5.4	Final Release of Foundational Data Technology Prototypes

As well as the following **technical specification documents** from related initiatives:

Table 3: Technical specification documents

Initiative	Document
GAIA-X	Technical Architecture (Release - June,2020)[3]
IDS	Reference Architecture Model 3.0[4]
IDS	International Data Spaces Information Model (Release - 2020-08-18)[5] [1]
DCAT	Data Catalog Vocabulary Version 2[6]

After the analysis of the above mentioned documents, it was decided to adopt the IDS Information Model as Core Ontology for the TRUSTS ecosystem, both for its broadness of scope, as well as for its compatibility with several technological developments brought to this project by the IDS. Any enhancements necessary to this model will be done without breaking its compatibility with well-known standards such as DCAT. Actually, the IDS Information Model has already been designed on top of DCAT and other standards.

Further review of these documents, discussions among partners and several sessions for the design of metadata workflows, led also to a first draft version of metadata management architecture, whose compatibility with the rest of the platform is yet to be evaluated. This draft architecture integrates technologies supplied by project partners, and minimizes the need for ad-hoc developments while trying to maintain compliance with the three sources of requirements mentioned above.

T3.5 Platform Development & Integration

In task T3.5, we have started with research of existing data marketplaces, in particular IDS and DMA. We also considered reuse of the CKAN data portal. We gathered criteria for selecting candidate components for the TRUSTS infrastructure. After thorough discussions among the partners participating in this task, we have decided to select a minimal set of components as a starting point of the platform, which we have labeled as “minimum viable prototype version 0 (MVP0)”. We provide a sketch of the architecture for MVP0 and its components in the following diagram.

[3] https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.pdf
[4] https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf
[5] https://w3id.org/idsa/core
[6] https://www.w3.org/TR/2020/REC-vocab-dcat-2-20200204/

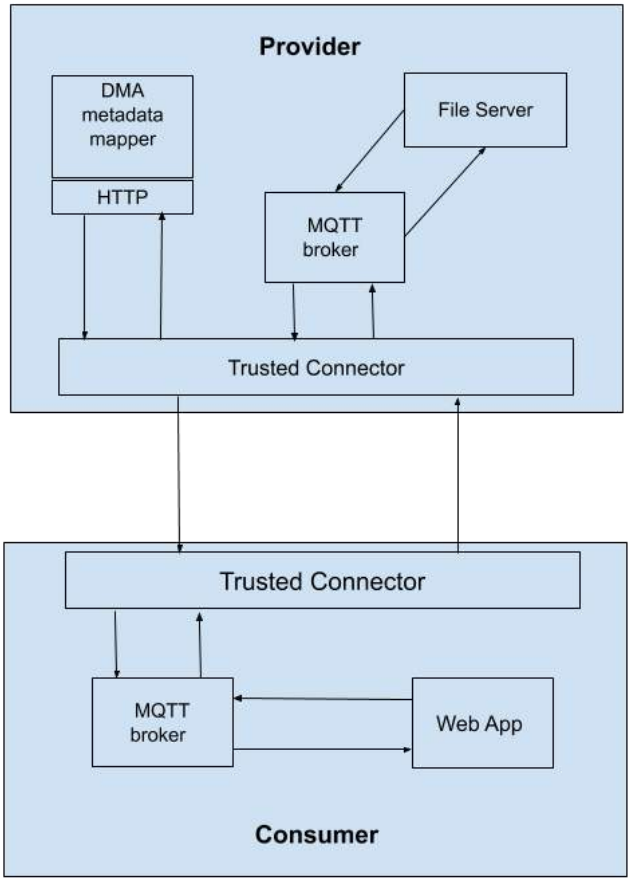

Figure 6: Architecture for MVP0 and its components

In the context of specifying MVP0, we have tested the IDS Trusted Connector for the role of a data provider and data consumer. In addition, we tested different interfaces for the communication of customized applications with and through the Trusted Connector. In particular we tested connecting via HTTP and MQTT. In addition, we have tested the routing functionality which is offered by the Trusted Connector, and which is based on the routing component of Apache Camel. On top of the IDS infrastructure, we have included the DMA Metadata Mapper Component in MVP0, in order to assess the feasibility of routing the communication of non-IDS components through the IDS Trusted Connector. As a result of implementing MVP0, we have determined that the Trusted Connector is suitable as the central communication component in the TRUSTS platform. It supports, out of box, many functional requirements such as secure point-to-point communication, uploading and downloading data between nodes. In addition it provides APIs for access control and data usage control, and it can be used to enable routing and communication between applications using different protocols and technologies.

T3.6 User and corporate profiles and brokerage

In T3.6., we aim to extract and process interaction data and metadata of (i) user and corporate profiles, (ii) services, and (iii) datasets as a basis for tripartite recommendation services in the TRUSTS portal. With tripartite recommendations, we are referring to a specific type of recommendation problem prevalent in data markets. In contrast to bipartite recommendations, in which one type of items (e.g., movies) are recommended to users, tripartite recommendations deal with two types of items (i.e., datasets and services in the data markets setting) that are not only recommended to users but also can be interlinked with each other. Based on this definition, in the first year of TRUSTS, we identified four different

recommendation scenarios: (RS1) recommendation of datasets to users/corporates, (RS2) recommendation of services to users/corporates, (RS3) recommendation of datasets to services, and (RS4) recommendation of services to datasets.

Based on these recommendations scenarios and in close collaboration with T3.4., we started to identify the metadata flow between the recommendation system and the other TRUSTS components. Here, the recommendation system will act as a node within the IDS-based infrastructure with an own IDS connector that interacts with the metadata catalogue of the IDS broker (for receiving interaction data and metadata of users/services/datasets) as well as with the TRUSTS portal (for showing recommendations and receiving feedback of recommendation clicks). Additionally, we reviewed the architectural requirements of the recommendation system within this infrastructure and decided to implement the recommendation services based on Know-Center's ScaR framework, which was already used in course of the DMA project. With this framework, we will implement three types of algorithms, i.e., (i) MostPopular, (ii) Collaborative Filtering, and (iii) Content-based Filtering, which are capable of realizing the aforementioned four recommendation use cases.

3.3.3 Next Steps

The next steps per task are:

T3.1 Infrastructure set-up and technical operations

In the second year of the project, T3.1 will continuously seek feedback from the project partners with a technical perspective on the platform, in order to improve and iterate on the provision of infrastructure. In particular, this will be based on the experiences of the tasks in WP3, WP4 and WP5. The resulting second iteration of the infrastructure will be documented in deliverable D3.2 "TRUSTS Infrastructure II" to be finished at M24.

T3.2 Smart Contracts

In the second year of TRUSTS, concrete use cases for the use of smart contracts within the TRUSTS ecosystem will be created using the architectural design of D2.6. Existing work and frameworks for smart contracts will be evaluated in order to exploit synergies within the ecosystem. Based on this and the usage policies that are applied to datasets of a data provider, first smart contracts will be designed in a machine-readable as well as a natural language. In addition, safety-critical aspects regarding smart contracts and block chains as well as the integration of smart contracts into them will be investigated. In addition to the technical aspects, the legal aspects of the design of smart contracts will also be examined.

T3.3 Data marketplace interoperability solutions

In the second year, the current early-stage interoperability prototypes of the selected data markets will be converted into more mature and robust solutions. At the moment, they exist as mere Jupyter notebooks and were used to explore the functionalities and capabilities of the APIs of the three selected data markets. They will be put on top of Trusted Connectors and interchange data with the data store of the TRUSTS broker. Furthermore, a crawler to harvest data market metadata will be implemented. Based on the specific requirements of each data market it will provide different functionality. Connected via a Trusted Connector, this data market metadata crawler will transfer the harvested data to a broker format converter, which turns the acquired metadata into the format required by the TRUSTS broker. The two mentioned components, i.e. the metadata crawler and the broker format converter, will either be extensions of already existing DMA components or, if necessary, be conceptualized, designed, and

implemented from scratch. They are either standalone components focusing on metadata of third-party data markets or merged with harvesting and metadata mapping components of T3.4. Another focus in the second year will be the conceptualization of components to map data market operations onto TRUSTS operations. In other words, we will investigate, which functionality of third-party data markets can and should be available from within TRUSTS, e.g. the acquisition and exchange of data assets, or purchasing and selling of data.

T3.4 Data Governance: Metadata, Lineage and Semantic Layer

Adequate metadata management and data lineage requires more than definition of ontologies and schemas. Thus, in the second year of the project T3.4 will advance in two directions. Firstly, the construction of controlled vocabularies for metadata management and enrichment, based on industry standards and compliant with the requirements of the project. These will serve in adequate management of data assets, as well as improve the search and recommendation functionalities. Together with the IDS information model and any enhancement deemed necessary, vocabularies will constitute the TRUSTs metadata layer, which will be concisely defined in one deliverable in Month 18 of the project, including examples and linking to working software artefacts that leverage it. Secondly, a concrete implementation of the metadata ingestion platform will be undertaken in three steps: i) prototypical ingestion of metadata into a Broker ii) pipeline for the ingestion of metadata related to services and datasets, and iii) provision of metadata endpoints for the management of other TRUSTS assets such as nodes and organizations. This implementation entails the setting up of specialized computing infrastructure, the selection of use cases, and the establishment of acceptance criteria both for individual components and for integrations.

T3.5 Platform Development & Integration

In the second year, we will be further iterating the TRUSTS platform. This will be based on interactions and feedback with the other tasks in WP 3, and on interactions and feedback with the use cases in WP5. The technical focus will be on integrating the constituent components into a homogeneous platform. As part of this, we are planning to extend our knowledge about the Trusted Connector and to express metadata and information related to the operation of the platform using the IDS information model. Another aspect will be the definition and testing of security configurations in accordance with the security requirements specified by WP 4. This also involves setting up a testing environment with instances of all components required for providing a secure data marketplace and secure services. Finally, we will also facilitate the creation of a development and testing environment for the services hosted on the platform with the help of the general infrastructure provided by T3.1.

T3.6 User and corporate profiles and brokerage

In the second year of TRUSTS, we plan to set up a first version of the recommendation system that offers three types of REST-based Web services for interacting with it: (i) services to add interaction and metadata of user/corporates, services and datasets, (ii) services to query recommendations, and (iii) services to add feedback (e.g., clicks on recommendations). Here, especially the third type of services will be an important source of data for evaluating and fine-tuning the parameters of recommendation algorithms. This first version of the recommendation system along with its API descriptions will be published in M18 in the demonstrator deliverable D3.6A “Profiles and Brokerage V1”. Apart from that we plan to conduct research in the area of privacy-preserving recommendation systems that can create personalized recommendations with a minimum amount of private user data. These research results will especially be valuable in case of sparse interaction data, i.e., in situations in which Collaborative Filtering-based algorithms do not work.

3.4 WP 4 Privacy preserving technologies

3.4.1 Objectives

Data privacy is a worldwide concern due to threats and risks that can compromise individual security, reputation, and social exposure. Aiming to mitigate privacy risks and assure civil rights on personal data, countries and territories have been ruling the activities related to data collection, transfer, storage, management, and deletion, such as the European Union's General Data Regulation Protection (GDPR). The terms of such regulations also play a crucial role in the development of artificial intelligence models that explore personal data, namely machine learning and deep learning (DL). Therefore, mechanisms for privacy preservation as differential privacy, homomorphic encryption (HE), federated learning (FL), secure components, multi-party computation (MPC), and adversarial training have been successfully proposed and applied to real-world systems.

Advanced decision-making capabilities are required for broad areas and arise from the improvements of data science along with the technical ability to draw advanced conclusions based on big data. These capabilities have been proven when it comes to public data. However, for private or personal data, there still exists the requirement to develop a technology platform that will allow the execution of advanced techniques for data analytics alongside the complete prevention of data breaches that may endanger privacy. Furthermore, regulatory constraints and the desire to preserve individuals' privacy uphold the accomplishment of this requirement, which is the main objective of this project.

This work package has the objective of integrating privacy-preserving mechanisms to TRUSTS in order to safeguard use cases in the financial domain from privacy threats. In addition, data trading and sharing activities will also be protected.

Because personal private data trading is not possible in the ordinary sense of the word, we are required to develop the ability to support data processing without compromising data privacy. Throughout the project we work in full collaboration with the UCs leaders and the WPs leaders in order to adapt the research perfectly to the system requirements and the UCs requirements.

Task 4.1 - Privacy Preserving Data Analytics

The focus of this task is investigating the design, security and efficiency of cryptographic primitives involved in building data analytic systems for private data. The result of this task will be a clear recommendation on the choice of algorithms to perform data analysis suitable for the use cases (D4.1, due in M18).

Task 4.2 - Privacy Preserving Transfer Learning and Classification

Closely related to T4.1, we started working on an abstract financial use case based on credit risk assessment, in order to design a solution combining HE with a DL architecture for secure transfer learning that can later on be included to the TRUSTS platform. Although we aim to create actual prototypes and software solutions, the main result of this task will again be a clear guideline, which algorithmic approaches for classification, making use of transfer learning, will be most promising and suitable for the context of the TRUSTS project. Transfer learning is a family of machine learning approaches characterised by the application of models for tasks that differ from the original tasks for which these models were trained. For

instance, a DL architecture trained on a large dataset for general image recognition can be adapted to classify images of specific objects on a smaller dataset. In the financial domain, small companies may not have enough data to train their models for some tasks, like credit risk assessment, that demand a wide variety of data features to profile their clients with regards to the prospect of credit offers. Financial data is inherently private since it holds features that represent the personal attributes of people (identity, location, demographic information, and bank balance).

Task 4.3 - Anonymisation and de-anonymisation

Task 4.3 has 3 specific objectives:

1. The assessment of the datasets of each use-case from a (de-)anonymisation perspective. This consists of following a 3-step procedure, where the data owners would gain knowledge of the privacy risks in their datasets, and apply the suitable anonymisation measures.
2. The development of a TRUSTS application with which data sellers would be able to run a privacy risk analysis on their datasets, anonymise their datasets, and privately and securely provide them to their buyers.
3. The development of guidelines for the data owners to become aware of the privacy risks in their datasets and anonymise them.

3.4.2 Progress achieved

When it comes to personal data, common trading practices for non-private data are prohibited, so TRUSTS should become a data market for non-private data and services market and services provider for personal private data.

We were able to map out ways (e.g. different architectures) to collaborate over personal private data and also enable running advanced analytics, developed by third party companies on personal private data, all while complying with data protection regulations, and preserving full privacy.

For example, in the architecture depicted in Figure 8 below, we describe one possible way to collaborate over private personal data using HE. Bank A and a telecom company (Telco B) want to collaborate by running analytics over their combined private data, without having to disclose the actual data content to each other. Assuming a trained machine learning model is running at the TRUSTS platform, each of the two companies could transmit their encrypted query data to the shared model that will analyse the combined data based on homomorphic encryption. In general for such a use case some kind of key sharing method needs to be implemented, so that the two different public keys can be combined for the homomorphic data computation. After the model has been evaluated on the encrypted data, the encrypted results are sent back to the original data owners.

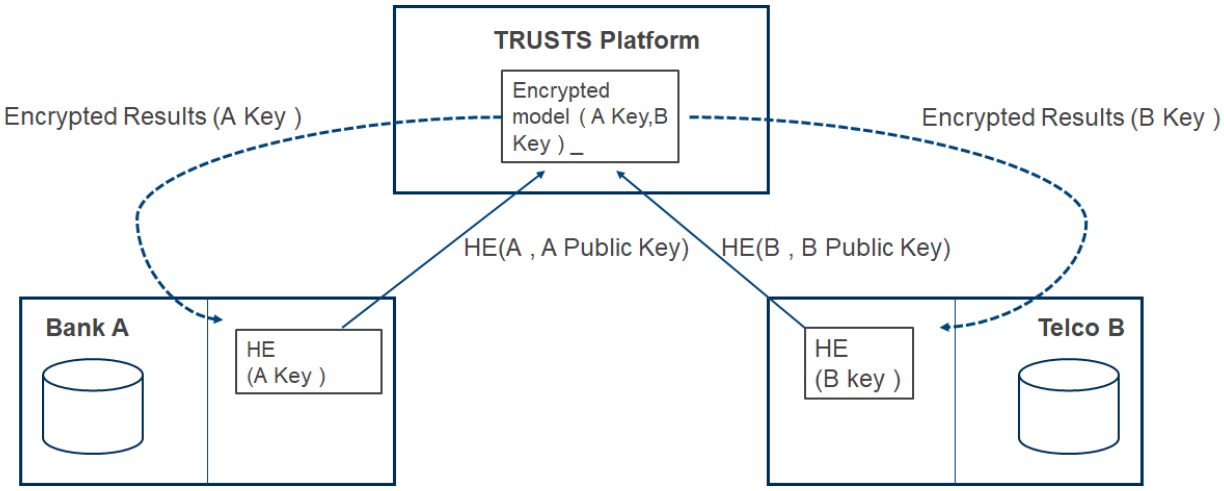

Figure 7: Example architecture allowing two parties to compute personal at the TRUSTS platform

Another option would be to use the TRUSTS platform as service provider to data owners, where MPC protocols could allow collaboration over sensitive private data. Depending on the specific scenario a startup company could for example develop new analytics and algorithms based on private data input from other parties. The final privacy-preserving implementation depends on the specifications of the respective use cases and our D4.1 "Algorithms for Privacy-Preserving Data Analytics" (M18) will contain clear recommendations for TRUSTS.

Below we describe the progress of WP4 for each Task in year 1.

Task 4.1 - Privacy Preserving Data Analytics

At the moment, we are testing several privacy-preserving approaches in close collaboration with the other tasks in WP4 and our findings and know-how are already included in these other tasks (e.g. the prototype developed in T4.2 or the architecture described in T4.3). We focus especially on the design and improvement of symmetric primitives for privacy-preserving technologies, in particular applicable to MPC and HE. In a recent publication, we also implemented a MPC protocol that shows how to use privacy-preserving technologies for large datasets as they will occur on the TRUSTS platform. Additionally, together with coworkers and motivated by Dr. Christian Rechberger and his team at TU Graz, we were also able to create a software solution based on HE that allows to exchange private and sensitive data between two parties while fully protecting the corresponding data content. Our insights from this implementation are directly incorporated in the deliverables for WP4. In order to show the performance and functionality of the respective software solution we investigated an use case related to the spread of the Coronavirus and based on health and mobile phone data: https://covid-heatmap.iaik.tugraz.at/en/. At the moment we are applying related methods and principles of this COVID-19 heatmap implementation to financial data as described in T4.2.

In order to inform and update our consortium as well as well as other interested parties about the possibilities and constraints of privacy-preserving analytics we also organized an online webinar that was advertised on the TRUSTS homepage and was well received by the participants.

Task 4.2 - Privacy Preserving Transfer Learning and Classification

Focusing on the credit risk assessment use case, we have conducted research activities that encompass the search for related works in the literature, suitable benchmark datasets, baseline models, and performance measures for the results. Benchmark datasets were collected from public data repositories for training and testing machine learning models, as Kaggle and the UCI Machine Learning Repository. Four baseline models were computed on the benchmark datasets, namely Linear Regression, Random Forest, Gradient Boosting, and Support Vector Machines with a linear kernel. Finally, besides the classification accuracy, we analysed the model results with respect to the F1 score and Cohen's Kappa coefficient. The former measures how well the model performs the classification task for every class on the dataset and computes an average of all individual class' results. The latter calculates the agreement between the ground truth results and the ones provided by the models. Therefore, technical and methodological aspects of the experiments were defined, as well as the expected contributions of the research outputs. The core method of our approach for credit risk assessment was also defined. A transfer learning prototype based on a Convolutional Neural Network architecture with a data representation yielded by an Autoencoder is already implemented and currently being tested.

Task 4.3: Anonymisation and de-anonymisation

Per objective:

1. So far, FNET from use-case 2 has provided a sample of their dataset and EBOS from use-case 1 has provided a high level description of their dataset. The appropriate privacy risk analysis modules of the application (see Objective 2) tailored to FNET's dataset have been developed.
2. Four risk analysis modules and a working UI has been developed (at the time of writing, the modules and the UI are not joined).

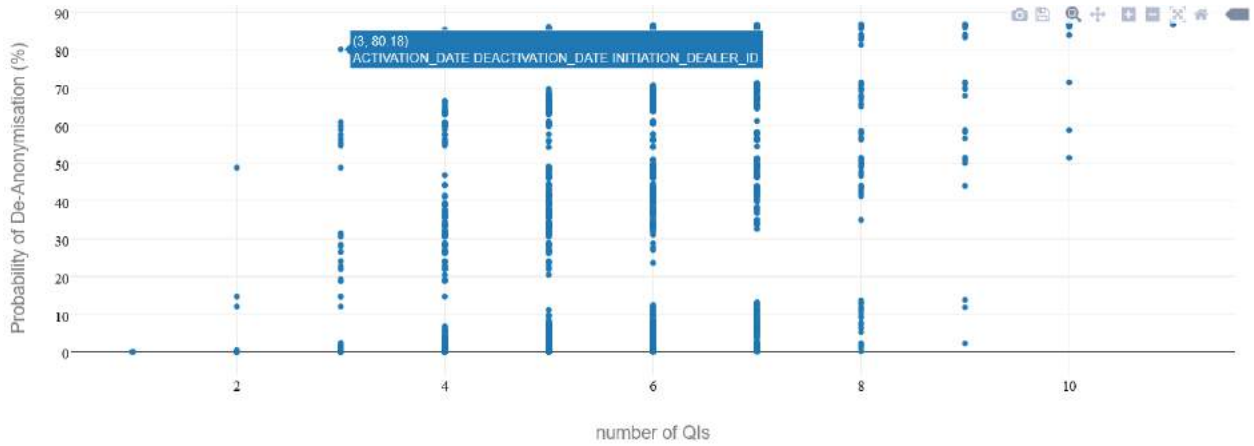

Figure 8: Risk analysis of tabular data

Probability of de-anonymization if an adversary has knowledge of any of the attributes of a dataset.

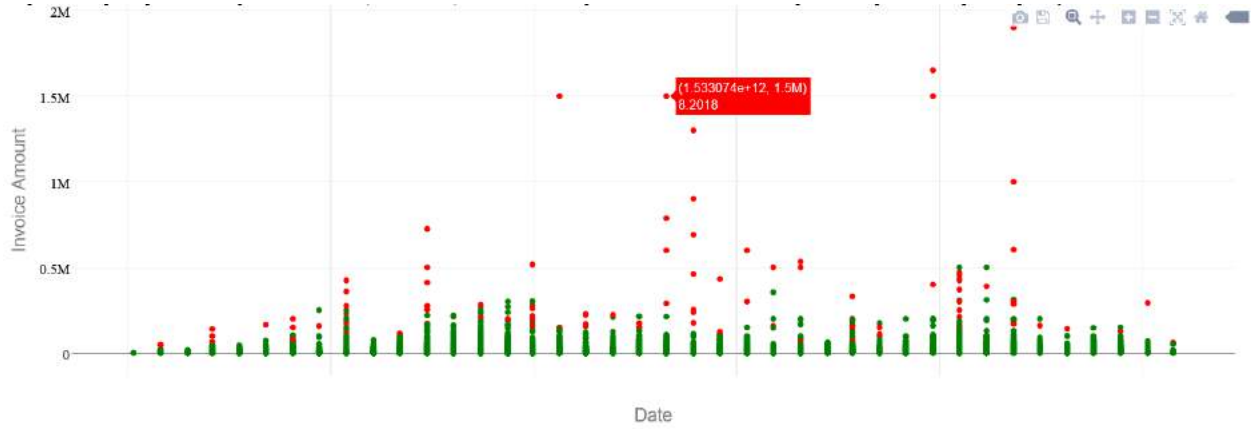

Figure 9: Invoices risk analysis

Privacy of the users' invoices given as input the amount of users, invoice amount and timeframe. Green is private; red, otherwise.

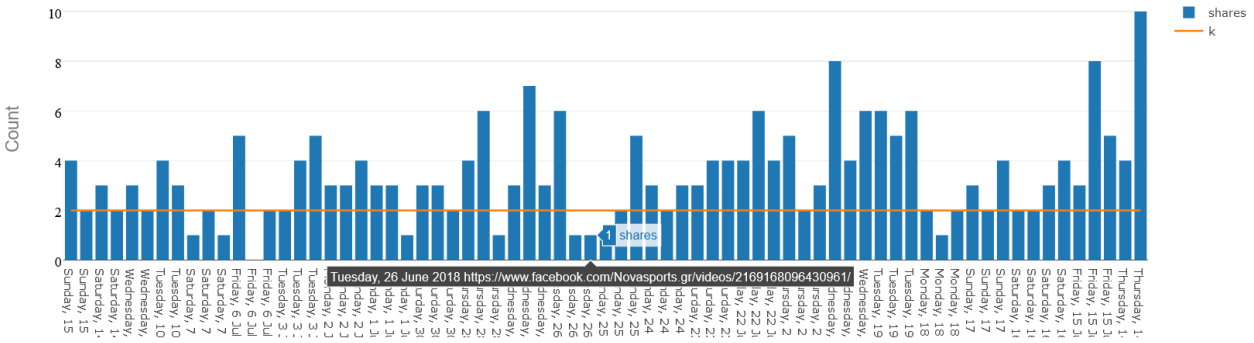

Figure 10: Aggregated data risk analysis

How well the aggregated values corresponding to users protect their sensitive attributes.

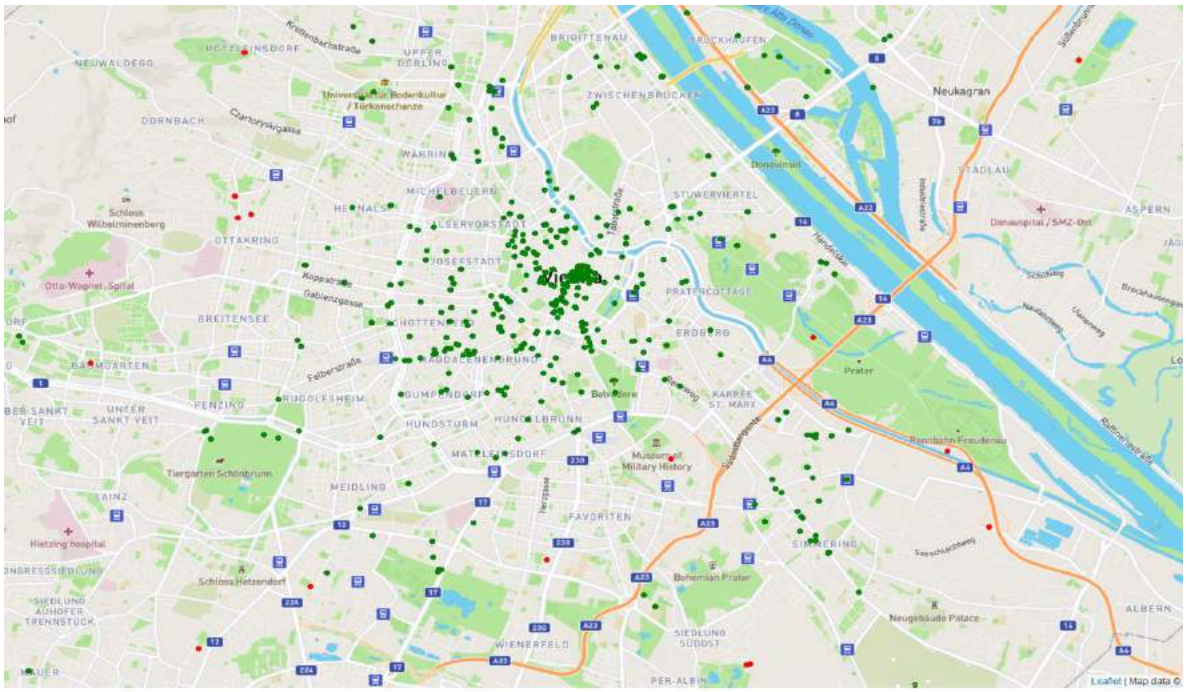

Figure 11: Risk analysis of location data: privacy of users' location within a specified radius.

Green is private; red, otherwise.

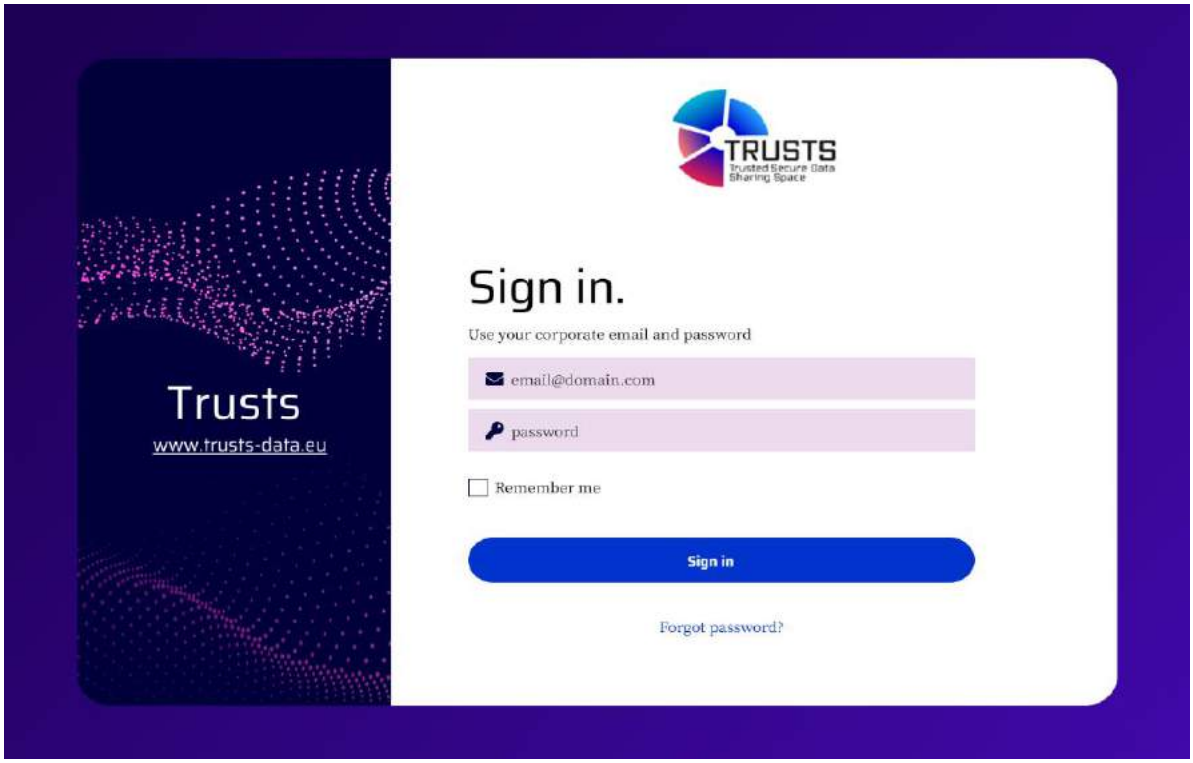

Figure 12: Sign in screen. The users log in Trusts Anonymisation Toolkit by entering their credentials

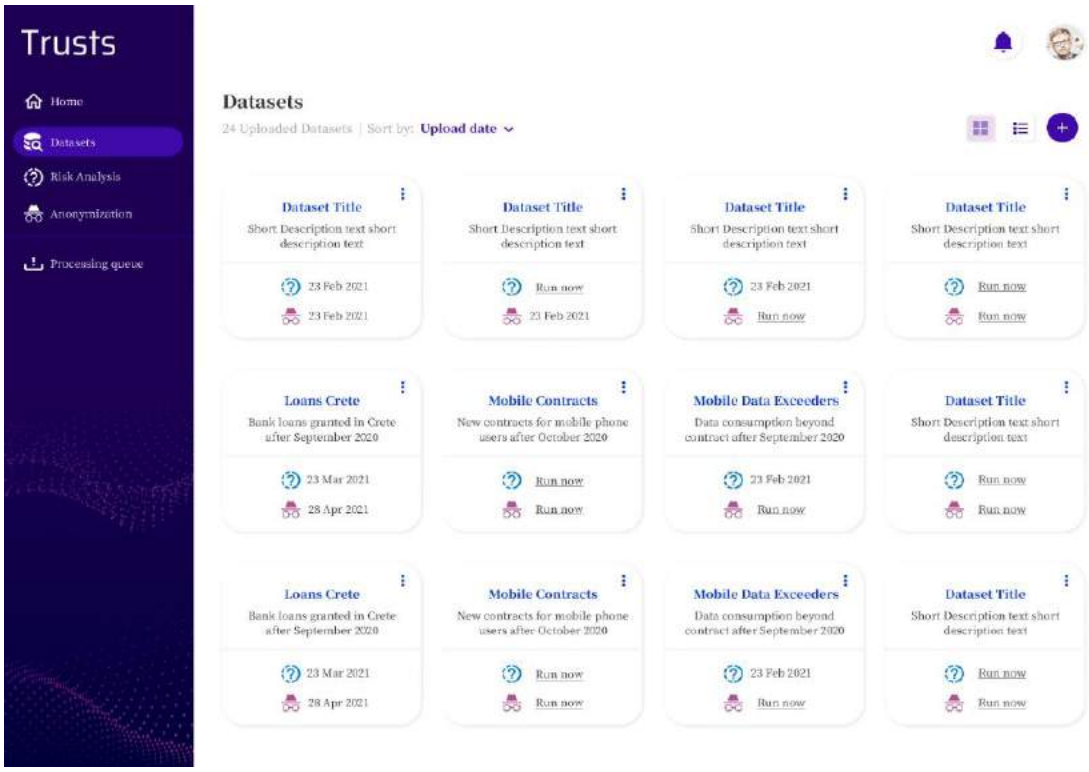

Figure 13: Datasets screen I

Users can see all of the available datasets that have been uploaded in the toolkit. For each dataset the title, a short description and last Risk Analysis or Anonymisation information is provided.

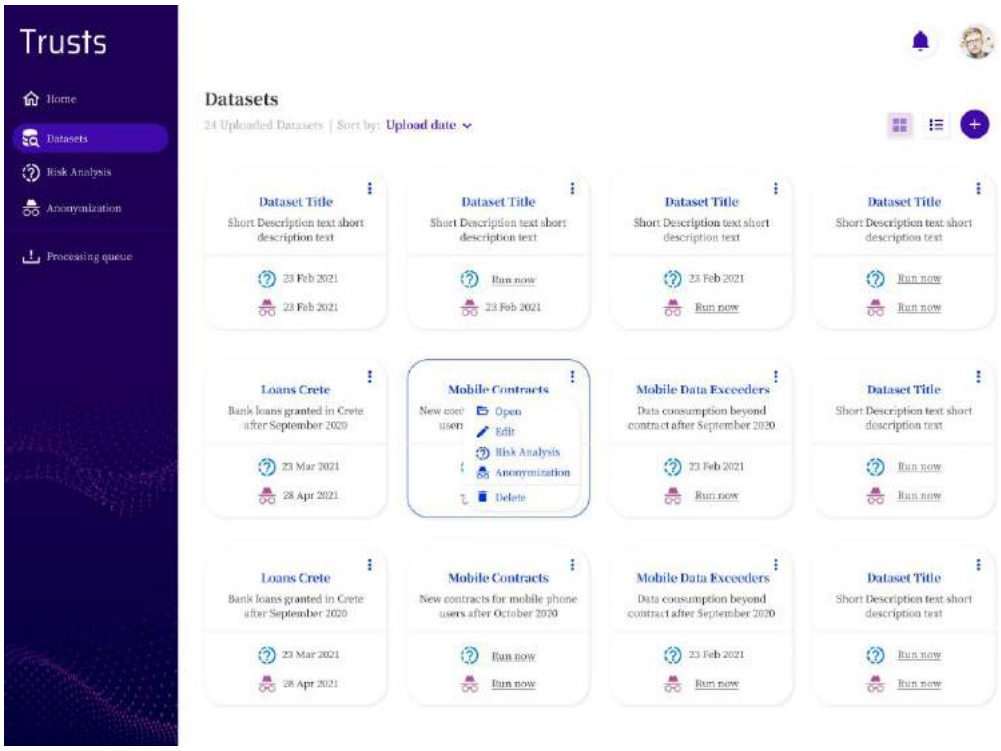

Figure 14: Datasets screen II

In this screen (Figure 14) users are able to Open, Edit or Delete any of the available datasets.

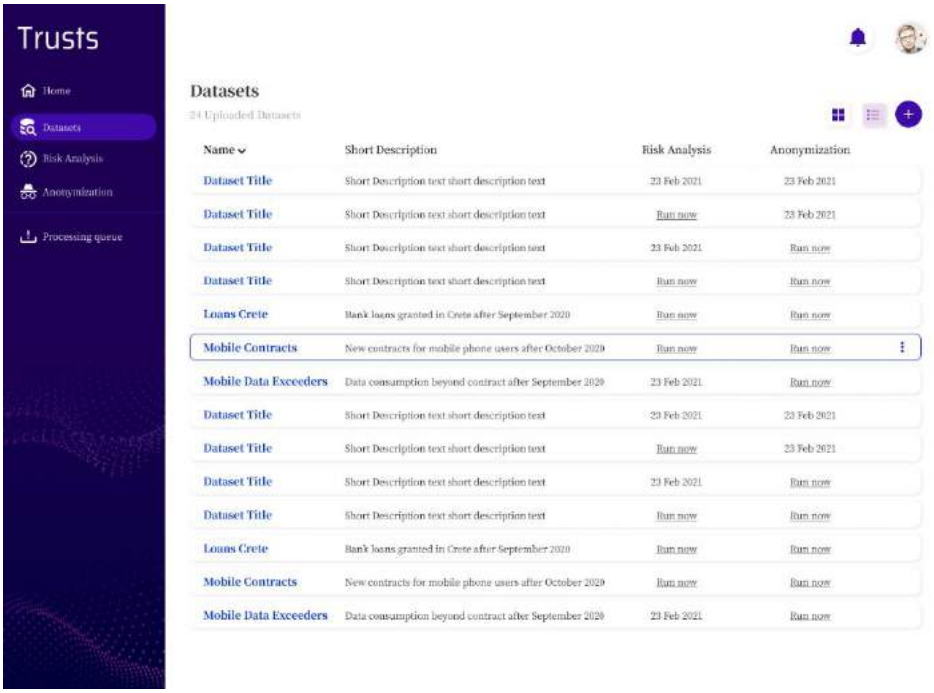

Figure 15: Datasets screen - Displaying the datasets in list view

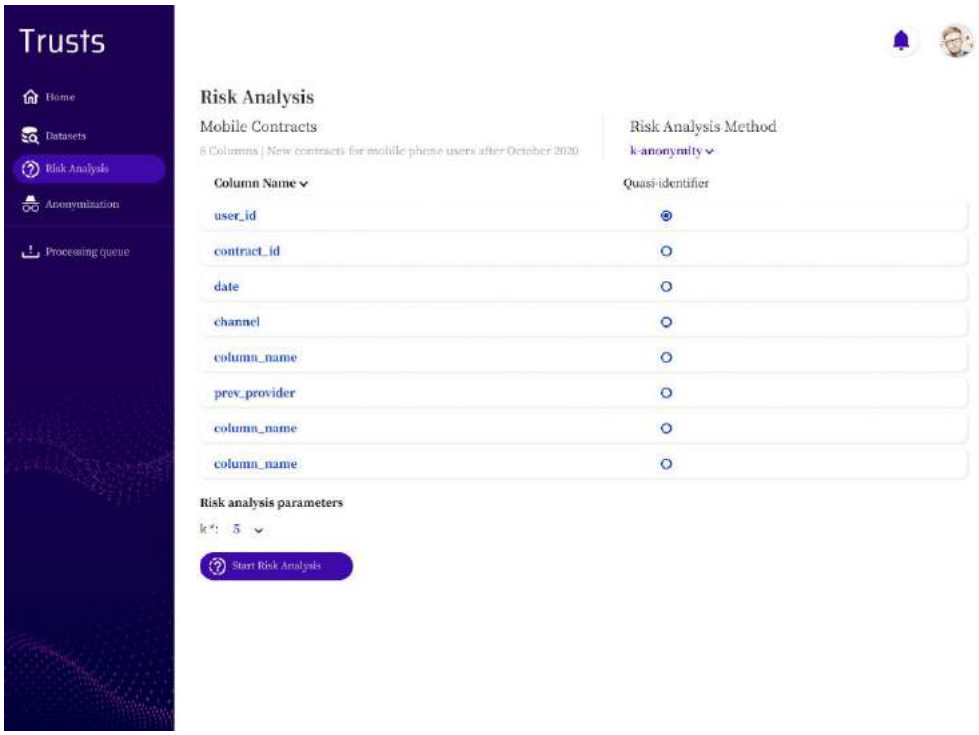

Figure 16: Risk Analysis screen

After the users select a dataset for Risk Analysis, they are requested to select an appropriate Risk Analysis method (depending on the dataset), choose the appropriate attributes and parameters that pertain to the selected method and then initiate the Risk Analysis process (Figure 16)

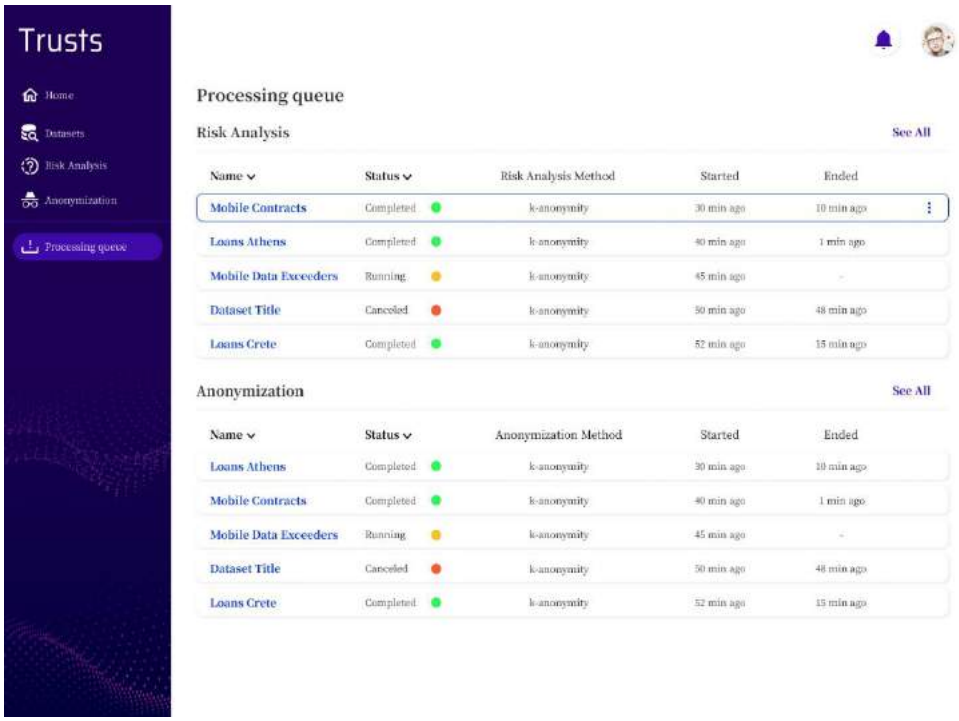

Figure 17: Processing queue screen

This screen above displays a list with the most recent risk analysis and anonymisation processes. For each process the dataset title, the process status, the (risk analysis / anonymisation) method and the started / ended time are provided.

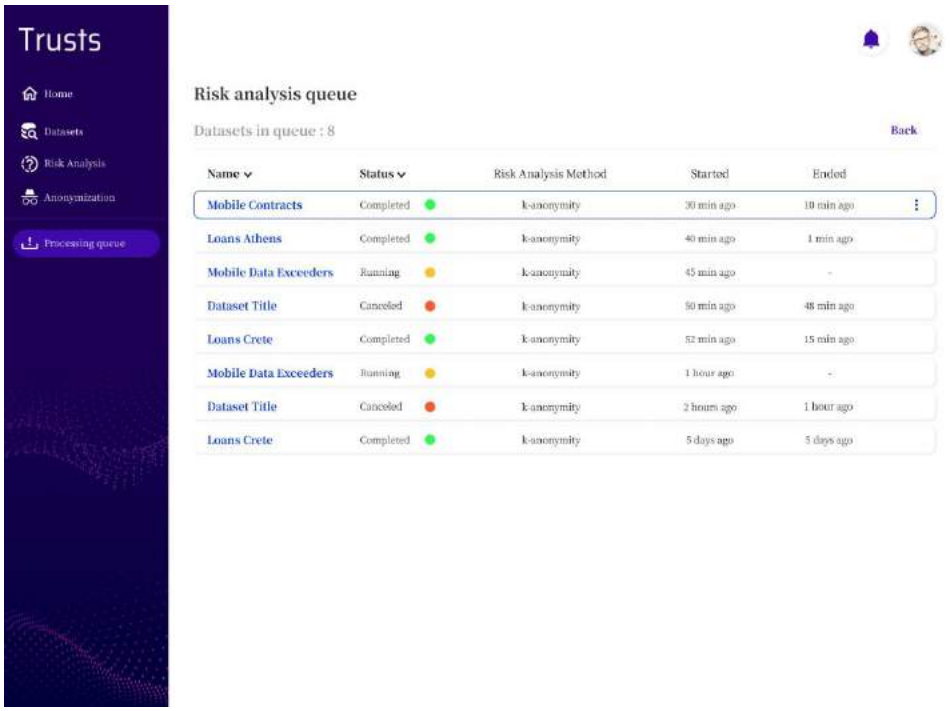

Figure 18: Risk Analysis screen II

This screen (Figure 18) provides the full list of the risk analysis processes.

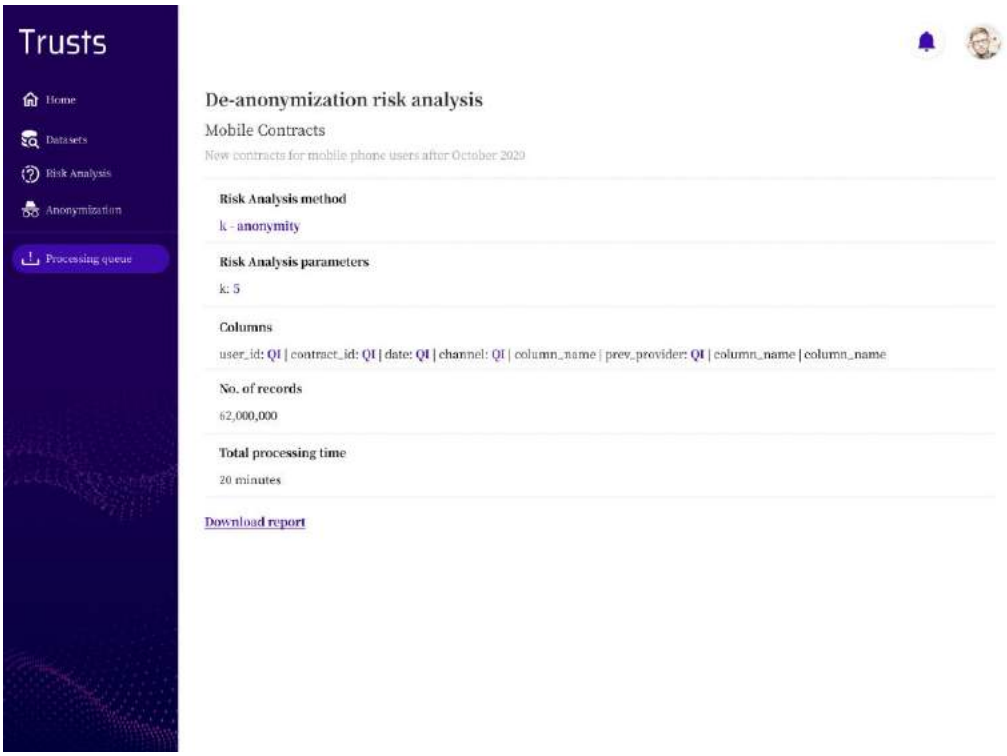

Figure 19: De-anonymization risk analysis screen

Information regarding a specific Risk Analysis process is provided including metadata of the dataset under inspection. The user can also download the De-anonymisation risk analysis report (Figure 19).

3. The development of guidelines has not yet started and will be the last milestone of task 4.3.

Additionally, the following paper was published and co-credited to the project:

Bampoulidis A., Bruni A., Markopoulos I., Lupu M. (2020) Practice and Challenges of (De-)Anonymisation for Data Sharing. In: Dalpiaz F., Zdravkovic J., Loucopoulos P. (eds) Research Challenges in Information Science. RCIS 2020. Lecture Notes in Business Information Processing, vol 385. Springer, Cham. https://doi.org/10.1007/978-3-030-50316-1_32

3.4.3 Next Steps

With respect to the achieved progress, the team will investigate, design and improve cryptographically secure protocols that enable data analysis of privacy-sensitive data. Consequently, we will focus on practical aspects of cryptographic building blocks such as, but not limited to, secure MPC and HE.

Task 4.1 - Privacy Preserving Data Analytics

We will continue to measure the performance of different cryptographic primitives and apply these methods to financial data sets and data from TRUSTS use cases. First, we will test and implement encrypted solutions for the transfer learning and classification problems of T4.2 and continue our exchange with the other members of the TRUSTS consortium to clarify the technical constraints of privacy-preserving analytics. We will also start to work on D4.1 to summarise all the insights and results of the last months.

Task 4.2 - Privacy Preserving Transfer Learning and Classification

We now have a working prototype from the machine learning perspective, the next step is to integrate the cryptographic parts to our transfer learning model. We have already approximated the corresponding activation functions with Chebychev polynomials so that a HE scheme based on floating-point numbers can be applied. We will again test the performance and accuracy of the combined model and ensure that there is no setback regarding the classification output. Additionally improvements concerning the data representation are required to ease the transfer learning process. In particular the involved datasets should have the same number of features and an enhanced domain relatedness. Subsequently, our models designed for research purposes will be made available on the TRUSTS platform so that any interested financial partner of the project can adapt them according to their needs. Further, the submission of the first research paper from the privacy-preserving transfer learning and classification task is expected to be done before the end of the twelfth project month. We will further investigate, design, and improve cryptographically secure protocols that enable data analysis of privacy-sensitive data. Consequently, we will focus on practical aspects of cryptographic building blocks such as, but not limited to, secure MPC and HE.

Task 4.3 Anonymisation and de-anonymisation

Per objective:

1. Either the complete datasets or samples and descriptions of them will be provided by the use-case partners that have not already done so. If the complete datasets are provided then the complete assessment will be done by RSA; otherwise, the tools for risk analysis and anonymisation, and guidelines will be provided to the use case partners
2. By the end of year 1, a first version will be provided having the UI developed by FORTH and at least 4 risk analysis modules developed by RSA. Development of anonymisation methods will start in year 2.
3. The development of guidelines is expected to start in year 3, after the application of Objective 2 has reached a mature stage.

3.5 WP 5 Demonstration of the TRUSTS Platform in 3 business-oriented Use Cases

WP5 officially starts in Month 13 (January 2021) and ends in M34 (October 2022). According to the GA, its focus is on demonstrating and validating the TRUSTS platform. Task 5.1 'Planning, setup and operation management' (led by eBOS), Task 5.2 'Use case demonstration execution' with 3 sub-tasks mentioned below, and Task 5.3 'Performance evaluation and lessons learned' (both led by FNET) conclude this WP.

The projected outcome of TRUSTS will be the successful implementation of a data marketplace which will be evaluated in this WP, by three specifically designed Use Cases (UCs) as described in the subtasks of Task 5.2 below, that were carefully extracted from real-life scenarios. TRUSTS solutions and business aspects will be tested through the financial sector, the telecom operators and the corporate data providers.

These UC's are:

- ST5.2.1: UC1: Smart big-data sharing and analytics for Anti-Money Laundering (AML) compliance. (eBOS)
- ST5.2.2: UC2: Agile marketing activities through correlation of anonymized banking and operators' data. (FNET)
- ST5.2.3: UC3: Buying data from a data marketplace to improve Natural Interaction. (REL)

"The Anti-Money Laundering compliance use case', UC1, is expected to demonstrate the capabilities of the TRUSTS Platform as a 'Trusted Secure Data Sharing Space' designed for AML purposes. This scenario will establish and validate how data shared via the Platform can feed into an existing AML solution boosted with big data analytics, Artificial Intelligence (AI) and Machine Learning (ML) techniques, to provide faster and more accurate detection of financial crime and money laundering. In addition, WP5 will determine how this enhanced data can be securely operated by the Platform to interested customers who need to comply with AML checks, e.g. financial institutions, internal corporate audit departments, fiduciaries and corporate service providers, tax advisors, automotive dealers, estate agents etc.

Use Case 2 "The agile marketing through data correlation use case" will demonstrate the capabilities of the TRUSTS Platform for advanced marketing activities through correlating anonymized banking and telecommunications data while maintaining core business, compliance and security processes (e,g, GDPR, etc.). The aim is to evaluate business and technological opportunities that the TRUSTS data marketplace may offer. The challenging envisioned business process of correlating external data sources in a GDPR and other respective regulations compatible manner, e.g. anonymised and aggregated CRM data of FNET and PB, has been chosen as a base evaluation scenario. Current practices e.g. absence of a unified and commonly acceptable technological and business framework able to assist such business collaboration, make it difficult to explore such business opportunities since all respective negotiations have to start each time from the beginning. Nevertheless, both FNET and PB understand that such collaboration will be beneficial for both companies and the clientele since it will lead to better products targeting real client needs. The whole economy will be benefited as well since innovative process and product production value chains will be established. Such innovative processes will be tested through UC2 trials for their user friendliness, completeness and business effectiveness.

The third and final TRUSTS UC, "The data acquisition to improve customer support services use case" is projected to generate an out-of-the-box analytics solution for the anonymisation and visualisation of Big Financial Data, specifically to boost new ways of human-computer interaction currently in their infancy, e.g. chatbots that can act as automated assistants to allow customers to converse about the management of their debt at their own pace and with a personalized experience, through the integration of Big Data.

Table 4 below is mapping the UCs with functionalities provided by TRUSTS. As a conclusion, all three specified UCs will advance through AI and ML techniques and algorithms.

Table 4: UCs and TRUSTS Functionalities

TRUSTS Functionalities	Use Case 1	Use Case 2	Use Case 3
Artificial Intelligence	√	√	√
Machine Learning algorithms	√	√	√
Anonymisation		√	√

De-anonymization protection		√	√
Smart Contracts	√		
Datasets valuation		√	√
Data correlation		√	√
Data enrichment	√		
Data quality improvement	√		
Secure Storage	√		√
Bespoke big data analytics	√	√	

3.5.1 Objectives

TRUSTS goal is to create a secure and trustworthy European Data market, for personal and industrial use, by interconnecting different user groups and providing generic functionalities for innovative applications and services. WP5's objective, as previously mentioned, is to demonstrate and validate the TRUSTS platform using three business-oriented UCs.

Initially, Task 5.1 aims to provide the necessary demonstration test-bench to the stakeholders, to show through actual field trials that the TRUSTS Platform is capable of supporting the binding KPI requirements defined in WP1. For each UC the involved partners will prepare, plan and set-up activities (UC deployment and testing), followed by an evaluation of the pilots, defining the methodology, the KPI benchmarks and the Gantt chart planning (tests, analysis and feedback loops). This task will also monitor the implementation progress (UC execution), WP5 coordination aligned with WP3 and WP4 and ensure the compliance with TRUSTS goals.

In Task 5.2, the pilot actors will perform actual testing and validation activities aiming to collect the results and validate the platform's effectiveness but also to highlight issues, gaps and difficulties confronted.

In the final task of WP5, Task 5.3, the performance of each UC will be evaluated, particularly from the KPI perspective to illustrate how the TRUSTS platform capabilities can be leveraged for different applications in each UC. Secondly, according to the results received from each UC, in every agile-based iteration, the task

will provide requirements and suggestions to further improve both functional and non-functional capabilities of TRUSTS. This task will also provide and establish systematic feedback loops to WP3 and WP4 for continuous refinement. Results will be analysed both quantitatively and quantifiably. Conclusions and recommendations will be drawn including recommendations for further trial validations. Throughout the validation testing period, knowledge and findings will be documented in deliverable D5.5/D5.6 together with evaluation reporting and impact assessment for the use cases, and extracting lessons learned for internal dissemination among the consortium, capacity building and external dissemination as appropriate.

To conclude, the project team will collect the generated results and will validate the effectiveness of the Platform within the UCs, critically highlighting any relevant interference observed, gaps in the expected results, difficulties in the adaptation of the solution, and other peculiarities of the context that might act as a constraint, so as to continuously improve the Platform.

3.5.2 Progress achieved

WP5 officially starts in M13 (January 2021), therefore advancement under this WP was not attained to date (October, 2020), but preparatory actions and planning as well as operational management in order to conduct the UC trials starting M16 (April 2021) is ongoing with the significant collaboration of WP2, WP3 and WP4.

3.5.3 Next Steps

As previously mentioned, WP5 is planned to start in M13, so the next activities and steps are related to T5.1 and the overall planning and setup of the test environment in order to prepare the ground for the UC trials execution, based on the implemented solution as provided from the technical WPs 2 and 3.

Preparatory activities, services deployment, implementation and testing plan for the pilots will be completed within the first 3 months of the WP, therefore by April 2021 will be ready to officially start the UC trials. The completion of the 1st phase of the UC trials will finish by October 2021 and then a preparatory period for the 2nd phase will occur for Year 3.

With the collaboration of WP2, the UCs will contribute to the Business and Technical validations planned to take place within the lifetime of the project, presented in the below time plan as defined by WP5 leader and as stated in deliverable 2.4. Based on this we conclude that each phase is a result of the process of previous steps, and the process should be repeatedly checked for consistency.

There are 11 deliverables within WP5, as depicted on the figure below, to be submitted throughout the project's lifetime. The first deliverable is the D5.1 'Pilot planning and operational management report' which is a periodical report, that will contain the implementation and testing plan for the pilots. The TOC and an initial draft as per TRUSTS QA process, has been prepared for the first version (D5.1) to be submitted by M14 (February 2021), prior to the UC trials begin and then, it will be updated (D5.2 and D5.3) at the end of each demonstration phase as also shown in Figure 20 below.

By the end of the 1st demonstration phase all three UC's will submit their respective deliverables (D5.4, D5.6 and D5.8) that will consist of the tests carried out during the 1st demonstration cycle under each UC. In addition, the first version of the 'Performance evaluation and lessons learned report', D5.10 will be

submitted simultaneously by the end of Year 2, M24 (December 2021). A second version of these deliverables (D5.5, D5.7 and D.9) will be updated and submitted by the end of the 2nd demonstration phase in Year 3.

Validation Type	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18
	Jan-20	Feb-20	Mar-20	Apr-20	May-20	Jun-20	Jul-20	Aug-20	Sep-20	Oct-20	Nov-20	Dec-20	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21
						MS1						MS2						MS3
WP5																MS3		
Task 5.1													*Preparatory activities - planning, setup of UC's + deployment*					
Task 5.2 UC trials																1st phase		
Task 5.3																		
Deliverables														D5.1 (eBOS)				

Validation Type	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30	M31	M32	M33	M34	M35	M36
	Jul-21	Aug-21	Sept-21	Oct-21	Nov-21	Dec-21	Jan-22	Feb-22	Mar-22	Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22
							MS4											MS5
WP5																		MS4 MS5
Task 5.1																		
Task 5.2 UC trials							2nd phase											
Task 5.3																		
Deliverables						D5.4 (eBOS) D5.6 (FNET) D5.10 (FNET) D5.8 (REL)	D5.2 (eBOS)							D5.5 (eBOS) D5.9 (REL) D5.7 (FNET)	D5.3 (eBOS)	D5.11 (FNET)		

Figure 20: Gantt Chart of TRUSTS Use Cases Trials and WP5

Figure 20 above shows a complete time plan conducted for WP5 and the effort to be accomplished throughout the project's lifetime as it also defines all of the above.

3.6 WP 6 Legal & Ethical Framework

3.6.1 Objectives

The overall objective of WP6 is to develop a robust legal and ethical framework for the TRUSTS Platform to ensure sustainability and compliance of the innovation brought by the project with all relevant regulations and ethics principles. This objective targets both the outcome of the project (i.e., the TRUSTS platform) and the individual use-cases. The work varies from general guidance of the consortium towards legal and ethical compliance, via guidance towards ethically compliant trials and testing as well as guidance in taking into account and embedding into the developed technologies of the key principles and rules, to research of aspects of the main legal frameworks, inter alia data protection, competition, consumer protection, that are specific to the development of a solution for sharing, computing and extracting the desired value out of personal and industrial data.

Based on this work, WP6 also aims to make recommendations as for whether and how the legal framework should evolve in order to rightly regulate data market ecosystems.

In order to achieve these goals, WP6 shall identify relevant overarching legal rules and ethical principles and provide guidance for their implementation in the course of the project's development. The result of this WP will be a set of requirements, which will enable the continuous monitoring of the work progresses, the final evaluation of compliance of the technological solution developed and recommendations for policy makers and stakeholders in the field.

The various tasks of WP6 should be viewed as a continued effort towards these overall objectives.

3.6.2 Progress achieved

T6.1 - Research ethics [M1-M36]

In order to ensure compliance of TRUSTS project with "ethics requirements" described in the Grant Agreements, the following process has been set up:

- A questionnaire (Annex I) was drawn and circulated amongst all TRUSTS partners (27th March 2020). It was accompanied by a Background Note providing further explanation on applicable data protection legal provisions in order to ease the filling of the questionnaire. The filling of the questionnaire was use case-specific.
- Three questionnaires were drawn, namely one questionnaire for every use case as coordinated by respective use case leaders.
- A virtual meeting was convened (15th April 2020) to have a general discussion between partners on the ethics requirements and on how to comply with them.
- A virtual meeting was convened for every use case (21st April and 24th April 2020) in order to tailor the ethics deliverables.
- Based on the information gathered through the questionnaires and the virtual meetings, a first version of the ethics deliverables was drawn and circulated amongst the partners (18th May 2020).

In this task, KUL follows up on the ethics requirements submitted to the European Commission at the end of June. Ethics deliverables shall be considered as a consistent set of measures aimed at ensuring compliance with ethics requirements within the TRUSTS project. Finally, compliance with ethics and legal requirements are considered a continued effort by the partners, to be maintained throughout the project. In this section, KUL will remind the TRUSTS partners of the main data protection and ethics related concepts from the Background note relevant for the project lifecycle.

T6.2 - Legal and ethical framework [M1-M10]

The task provides the analysis of the legal and ethical framework and challenges relevant to the platform developed in the project. The identification of legislation, principles and values regarding the sharing of personal and non-personal, including industrial, data within the context of the use cases sectors, will lead to a description of requirements which will be taken into account in the development of the envisaged technologies and integrated into the platform.

The emphasis is placed on the following topics:

1. **Privacy and data protection:** Following general guidance provided as part of WP9 on compliance with data protection law (particularly the GDPR), the focus is placed on the following aspects, deemed of specific relevance for TRUSTS:
    - **Controllership in a data market context**. The identification of controllership, within the meaning of the GDPR, in a complex data market ecosystem characterised by the working together of many players is a notoriously difficult endeavour. The Court of Justice of the European Union has been recently recently requested to clarify how controllers should be identified in such complex environments, but it remains to be seen how this case law applies to data market environments.
    - **Legal basis for processing personal data**. In order to apply the right legal regime for data usage, each dataset should be qualified according to the nature of data it involves (personal data, non-personal data, mixed data). To make personal data available, data controllers must meet one of the legal bases of Article 6 of the GDPR, and for sensitive data additionally the conditions of Article 9. Such legal basis of data processing are covered in this section.
    - **The E-Privacy Directive and forthcoming Regulation**. The ePrivacy legal framework is currently being revised. Its scope of application and main concepts will be subject to change. In addition, the analysis of the relationship between the GDPR and ePrivacy legal frameworks is analysed.
2. **Privacy-preserving techniques.** The work on privacy-preserving techniques is a continuation of the work done in WP9 with regard to pseudonymization and anonymization of personal data. Main concepts (personal data, anonymization, pseudonymisation, re-identification) and approaches with regard to privacy preserving techniques are covered in this section. **Regulation of data as an (economic) asset**: Data market ecosystems are based on the consideration of data as an economic asset. It is therefore crucial to analyse how the law approaches data as an economic asset, while it is now generally agreed that there is no - nor should there be - on ownership right on data. Markets are indeed always based on legal underpinnings. The following aspects are particularly analysed:
    - **The Free Flow of Non-Personal Data Regulation**: With this Regulation, the European Union legislator wishes to remove obstacles to the “free flow of non-personal data”, arising from both the public sector and private companies. The Regulation is viewed by the legislator as a regulatory counterpart, namely for non-personal data, to the GDPR, aimed at personal data.
    - **Data sovereignty:** With the absence of legal frameworks directly backing the commodification of data and their exchange in their own rights on data markets, industry has come up with complementary regulatory initiatives. This is the case of ‘data sovereignty’, which is expected to be tested in TRUSTS. Data sovereignty is based on the technological enforcement of data transactions. Data sovereignty is based on the law (mainly based on contract law). At the same time, it remains to be seen whether and how data sovereignty can be compliant with the law, especially when it comes to technological enforcement of contractual provisions which could overlap with legal enforcement.
    - **Towards a Data Law? Patterns for future regulation**: How to regulate data as an economic asset remains very much of a question mark. The EU is dedicated to launching legislative

initiatives in this respect. They could have an impact on data market ecosystems such as TRUSTS and should therefore be analysed.

3. **Law applicable to online platforms and intermediaries**: The setting up of a platform for the exchange of data implies the creation of a whole ecosystem in order to enable data providers and data users to exchange data. Several models can theoretically be envisaged, depending on business and technical choices made in TRUSTS. In any case, the qualification as an online platform and/or intermediary may trigger the application of specific legislative frameworks specifically dedicated to them. Especially in recent years, the EU has been more and more involved in enacting *lex specialis* legislations concerning online platforms and intermediaries.
    - **Introduction - data sharing platform as (an) intermediary(ies).** Based on the European Commission 'Staff Working Document, Guidance on Sharing Private Sector Data in the European Data Economy' this section lists different functions that a data marketplace may perform.
    - **The Platform to Business Regulation ('P2B Regulation')**: In order to restore balance between online platforms and businesses online, the EU adopted the P2B Regulation in 2019, which could apply to the TRUSTS platform. The deliverable offers an insight into the P2B Regulation, including its scope of application, the substantive provisions, procedural obligations and enforcement-related issues.
    - **Intermediary liability for data sharing platforms.** This section explains whether and to what extent online platforms and intermediaries can be held liable for the content that their users place on their infrastructure under the 'e-Commerce Directive'.

4. **Economic law applicable to data transaction:** Beyond *lex specialis* legal frameworks applying specifically to online platforms, many legal provisions are likely to apply to data transactions, such as contract law and commercial law. For lack of specific EU legislation on B2B sharing, the European Commission has also attempted to bring guidance to businesses by adopting soft law documents which could be the basis for their contractual agreements.
    - **Regulation of B2B unfair commercial practices in data-driven ecosystems**: Contrary to the regulation of B2C relationships, B2B relationships are mainly regulated at national level. Horizontal regulation of unfair commercial practices between businesses may provide very relevant regulation for, *inter alia*, data transactions so as to ensure commercial fairness. It is not possible to provide an exhaustive overview of the legislation of all Member States, but a set of national legislations are outlined.
    - **B2B sharing principles and contractual terms.** For absence of a horizontal legal framework regulating B2B transactions, the EU has been active in elaborating soft law guidelines for businesses. This section elaborates on the general guiding principles for B2B data sharing provided in the European Commission 'Guidance on sharing private sector data in the European data economy' of 2018.

5. **Competition law and access to data**. Competition law remains an important background regime. This section discusses the role of data for competition law analysis and provides a general overview of Article 101 and article 102 TFEU. Then it turns to potentially relevant data-related competition law issues, such as: the exchange of information, and in particular sensitive information, directly between competitors or indirectly through a platform; the refusal to give access to data; the relationship between competition law and personal data protection law (such as the GDPR).

6. **Financial law applicable to data transactions.** Here, an analysis was performed of the relevant financial legal framework applicable to data transitions. This section provides an overview of the relevant regulatory frameworks relating to transactions over financial data. First of all, it covers frameworks aiming at facilitating the fight against anti-money laundering and terrorist financing. Then it looks at Payment Services Directives, their scope of application and their relationship with the GDPR with the objective of informing the consortium partners of potential challenges in an anticipatory manner.

7. **Blockchain and law:** The blockchain technology is contemplated to be used in TRUSTS, including smart contracts in order to automate data transactions. It is commonplace that blockchain technology challenges the law in a number of occurrences, especially when 'public blockchains' are used. An overview of the potential legal challenges arising from the use of the blockchain technology is provided.

8. **Ethical challenges in data sharing.** This section builds on the work already performed in Deliverable 9 on the possible ethical implications of data sharing within the TRUSTS platform. It offers a high-level analysis of ethical issues in data sharing with the use of AI-driven tools such as data-driven discrimination and data bias. It provides an overview of the ethics requirements for Trustworthy AI as defined by the High-Level Expert Group (HLEG) in non-binding 'Ethics Guidelines for Trustworthy AI'.

This task results (in M10) in Deliverable D6.2 'Legal and Ethical challenges and requirements', that consists of the basis for the oversight and evaluation in T6.3 ('Oversight, validation and updates', M11-36).

T6.3 - Oversight, Validation and updates [M11-M36]

KU Leuven has provided legal and ethical guidance to partners on ad hoc basis with respect to platform related questions. The initial table of contents and possible collaborations are being contemplated.

3.6.3 Next Steps

With respect to the progress achieved concerning the legal framework applicable to TRUSTS, we will continue our legal research. This will result in an analysis of legal and ethical norms/standards meant to guide the project partners. We will also assess the integration of the legal and ethical requirements in the design of the platform, as the technical development of the project evolves.

D6.2 will be submitted at the end of October. After the submission we will start working on D6.1 devoted to Research Ethics. This deliverable will provide all information regarding the compliance of the project research activities with research ethics and, in particular, with the H2020 Programme Ethics Guidance. This deliverable will be submitted by the end of February 2021. It will then be followed by the remaining deliverables of WP6.

After the submission of D6.2, KUL will concentrate its research efforts on legal requirements relevant for setting up the platform.

3.7 WP 7 Business Model, Exploitation & Innovation Impact Assurance

3.7.1 Objectives

The objectives of the work package WP7 "Business Model, Exploitation & Impact Assurance" are to develop a feasible business model to sustain the results of the project, mobilize an ecosystem, and conduct concrete actions for commercializing the data market platform. Thus the work package sets out to conduct market research on what business models for data markets exist around the world. The main focus is on business models combining scientific and non-scientific founders since TRUSTS has the same mixed private and public owned structure. The main deliverables during the project will be on the ecosystem and its needs regarding the innovation aspects and intellectual property and data management. The work package will establish pre-conditions for successful business models and best practices.

To achieve the same, the work package is divided into the following tasks:

A. T7.1 Sustainable business models
B. T7.2 Developing and structuring the platform engagement
C. T7.3 Intellectual Property and Data Stewardship
D. T7.4 Standardisation uptake and recommendations
E. T7.5 Commercialization initiatives and action plan
F. T7.6 Innovation Impact Assurance

Task T7.1 Sustainable business models

The aim of this task is to select a viable, feasible and sustainable business model for the data marketplace platform developed in the project. Practical business models will be developed following the method of action design research which gives a structure for structuring a scientific design project in a practice-oriented situated setting. The artefact of the action design research is a set of presumably viable business models. The business model will be developed by applying tools for business model innovation as developed in TUD's award-winning platform businessmakeover.eu. The tools will be applied in workshops with project participants and, later on in the project, outside stakeholders. To inform the business model development, first, through desk research and interviews, a range of potential data marketplace business models will be explored, leading to a taxonomy of possible business model design options. In doing so, this task will closely interact and leverage outputs of task T2.1 "EU and worldwide data markets". The taxonomy will be structured using components from three approaches: (1) business model components for digital systems in general, derived from TUD's STOF ontology for multi-stakeholder business models; (2) business model components that are specific for data marketplaces (e.g., degree of curation, semantification, aggregation of data provided); (3) multi-sided platform aspects that affect value creation (e.g., shaping of boundary resources that mediate between the marketplace and its users, launch strategies and cross-subsidization models to overcome critical mass problems). Evaluation of business models will be done in three ways: (1) by conducting a summative evaluation on the implications of business model choices on critical success factors that measure the viability of the business model; (2) by informing task T7.5 on concrete actions and activities needed to realize the business model and testing the feasibility of these actions based on task T7.5 findings; (3) by applying TUD's method business model stress-testing to evaluate the sustainability of the business models in different future scenarios (e.g., different levels of citizen trust in data economy or different levels of regulatory regimes).

Agreed deliverable of task T7.1 is a "Sustainable business model for TRUSTS data marketplace" report describing the designed business model to sustain TRUSTS after the project end. A first version, due by June 2021, will focus on the taxonomy for data marketplace business models and business model options. The final report, due by December 2022, will build on the same and lay out the designed, validated and selected business model(s).

Task T7.2 Developing and structuring the platform engagement

This task aims to reach out to a large variety of stakeholders (data providers, data consumers), data ecosystems and public initiatives (related EU proposals, competence centres, professional associations and technology platforms) to ensure the development of a sustainable platform. Based on our partners' network, a mapping of the various stakeholders will be drawn, the first step towards a community engagement strategy (task T7.2). This strategy should define our activities to attract new stakeholders and connect with other European initiatives. It will be linked and prepared in close collaboration with Engagement and outreach activities in work package WP8, task T8.2.

Agreed deliverable of task T7.2 is a "Communities Engagement Strategy" report, due by June 2021, describing our strategy to widen the community around the platform and how to attract new stakeholders during the project and beyond its lifetime. It includes the presentation of a set of KPIs supporting the stakeholder's acquisition process.

Task T7.3 Intellectual Property 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. 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 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 buyers 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 ease of attraction and onboarding of (SME) data providers onto the platform, to enable value creation and extraction within TRUSTS.

Agreed deliverables of task T7.3 are 3 workshops with stakeholders of the Data Market Austria (data owners / providers, data users / buyers, data aggregators / resellers) on their practical challenges and perspectives regarding IPR protection and Data Stewardship. A "Supporting mechanisms for Intellectual

Property Rights Protection and Data Stewardship" report will be drafted in a first version, due by June 2021 and finalized in a second version, due by December 2022, 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, and
4. proposed Data Stewardship support services for different (potential) data provider groups to optimize eased attraction and onboarding of (SME) data providers.

Task T7.4 Standardisation uptake and recommendations

The lack of interoperability and the integration costs to access a data market don't allow a proper data economy to thrive yet. Those hurdles will be lowered with a standardization effort. With more interoperability, players could exchange their data in the same trusted data market as well as open source technologies will lower the barrier to access the market. This task interacts with "T3.3 Data marketplaces interoperability solutions". We'll use and implement state-of-the-art technologies and libraries provided by standardization bodies to tackle those challenges. This task will include elaboration, assessment, and identification of required future development of a variety of concepts and standards (IDSA Reference Architecture Model, FpML, etc.) aiming at developing a state-of-the-art TRUSTS ecosystem. We will provide recommendations targeting major standardization bodies, based on our research. They will be shared and presented to standardization bodies' representatives during two dedicated workshops along the project. As our main objective is to develop a sustainable data ecosystem, we'll pay special attention to the support requirements and share our experience from IDSA, which has so far supported and developed the Architecture Model for any data ecosystem.

Agreed deliverable of task T7.4 is a "Standardization activities" report, due by December 2022. This report will present our recommendations about standardisation especially in the field of our use cases. It will also include our exchanges with standardization bodies during our 2 workshops along the project.

Task T7.5 Commercialization initiatives and action plan

This task will explore and define the strategy for bringing TRUSTS to market. It will also develop a pricing model for use of the TRUSTS services and a remuneration model for partners contributing technology to the TRUSTS services, but also for organisations that have contributed resources. This task will also carry out a technology watch to identify potential competitors to TRUSTS entering the market. Finally, a business plan for the TRUSTS services, the cloud hosting and operations of the TRUSTS Professional Partners Community will be created, to ensure sustainability and financial viability after the end of the project. The form in which the TRUSTS Professional Partners Community will be instantiated beyond the end of the project will also be decided and implemented in this task.

Agreed deliverable of task T7.5 is "Business plan and Implementation plan" report, describing the strategy of the consortium to transform the platform into a sustainable ecosystem and the TRUSTS business plan (business target, services, pricing, costs, remuneration of partners, etc.). The report will be provided as an early draft version by June 2021 and as a final version by June 2022.

Task T7.6 Innovation Impact Assurance

Aspiration of this EU funded programme is to bridge from research to market, that is to move beyond (research) output to outcomes and defined impacts. Thus, research findings, concepts and prototypes shall be usable for the next level of development and adoption by pertinent (industry) players in the wider business ecosystem. To enable this, task T7.6 shall work with all work packages and tasks to both ascertain from the outset and throughout the project that the aspired Outcomes and Impacts are kept in mind and guide Output creation. Our experience from the Data Market Austria shows that this dramatically improves research transferability and hence business viability, whilst it also reduces efforts for conceptualization or technology development. Thus, continuous interactions with all work packages and tasks through regular check-ins, coordinated with project management (work package WP1) are of paramount importance. In doing so, we also complement and enrich work package WP1 by enabling a firmer content-involved challenger role of project management as compared to a more coordinated role.

Agreed deliverable of task T7.6 is continuous interactions with all work packages and tasks, acting as a cross-function to the program to ascertain and optimize innovation impact. An “Innovation Impact Assurance” report will summarize these activities, as a first version by end of June 2021 and as a final version by end of 2022.

3.7.2 Progress Achieved

To accommodate task interdependencies within work package WP7 and across work packages, and work load capacity smoothing for involved consortia partners, tasks T7.3, T7.4 and T7.5 have been scheduled for full activation by January 2021. The work package is fully on track vis-a-vis its first deliverables due by June 2021.

Fully activated tasks:

A. T7.1 Sustainable business models
B. T7.2 Developing and structuring the platform engagement
C. T7.6 Innovation Impact Assurance

Tasks pending full activation, and related main rationale:

D. T7.3 Intellectual Property and Data Stewardship: workload smoothing
E. T7.4 Standardisation uptake and recommendations: interdependency with Use Cases
F. T7.5 Commercialization initiatives and action plan: interdependency with Business Model

In the fully activated tasks, progress has been as follows:

T7.1 Sustainable business models

- Defined, elaborated and aligned on common terminology pertaining to the trinity of roles: “data market”, “data market federator”, and “data ecosystem facilitator”
- Created database of 173 data markets and data sales platforms
- Created 6 case studies on select data markets
- Conducted joint data market survey with task T3.3 on interoperability and federation
- Developed a draft business-model-based data market taxonomy
- Conducted AllHands workshop on positioning of TRUSTS (jointly with tasks T7.6)

- Contributed to quarterly TRUSTS newsletter and TRUSTS overview webinar
- Prepared an external TRUSTS webinar on business model and platform positioning

T7.2 Developing and structuring the platform engagement

- Created and rolled out a unified stakeholder database in TRUSTS
- Conducted stakeholder mapping
- Designed a draft stakeholder engagement model, building on domain-specific, standing sounding boards comprised of external stakeholders
- Educated consortia members about approach to stakeholder engagement
- Aligned with work package WP8 on the handshake between stakeholder engagement, community building and project communication

T7.6 Innovation Impact Assurance

- Ascertained linkage and increased synergies between tasks T2.1, T7.1, T7.5
- Acted as link pin to task T2.4, aligning emerging business architecture and technical architecture. Regular participation in technical conference calls and working sessions
- Conducted a range of evangelist interventions to focus and align all consortia partners to intra-ecosystem interoperability and TRUSTS architecture as both, data market and data market federator

3.7.3 Next Steps

Work package WP7 will continue to deliver along and towards its defined deliverables outlined in section "Objectives", with a particular focus on enabling a consultative process in developing and reviewing the first set of upcoming deliverables due by June 2021:

- Task T7.1: First version of the "Sustainable business model for TRUSTS data marketplace" report describing the designed business model to sustain TRUSTS after the project ends. It will focus on the taxonomy for data marketplace business models and business model options.
- Task T7.2: "Communities Engagement Strategy" report, describing our strategy to widen the community around the platform and how to attract new stakeholders during the project and beyond its lifetime. It includes the presentation of a set of KPIs supporting the stakeholders acquisition process.
- Task T7.3: Draft version of the "Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship" report, utilizing desk research and insights from a workshop with stakeholders of the data economy on their practical challenges with data stewardship and IP protection. It should be noted that the Data Market Austria is not operational, and thus we will need to substitute for its originally assumed stakeholders.
- Task T7.5: Early draft version of the "Business plan and Implementation plan" report, describing the strategy of the consortium to transform the platform into a sustainable ecosystem and the TRUSTS business plan (business target, services, pricing, costs, remuneration of partners, etc.).
- Task T7.6: First version of the "Innovation Impact Assurance" report will summarize continuous interactions with all work packages and tasks, acting as a cross-function to the program to ascertain and optimize innovation impact

The work package is currently conducting the detailed planning and preparations to enter 2021 with the following foci:

- Activation of remaining work tasks T7.3, T7.4 and T7.5
- Activation of / recruiting for sounding boards with external stakeholder
- Continuation of external communication and ramp-up of engaging outreach activities
- Delivery of a workshop with external stakeholders, jointly with task T2.1, on validation of research on data markets and data market federators, future scenarios pertaining to the data ecosystem and applicability / effectiveness of the drafted taxonomy
- Delivery of a workshop with stakeholders on challenges with data stewardship and IP protection
- Research, drafting, consultation and revision, and finalization of all elements required for the work task reports due by June 2021
- Detailing of business-model related additional requirements towards the technical platform

3.8 WP 8 Dissemination, Communication & Community Building

3.8.1 Objectives

This work package includes dissemination, communication, and community building tasks. The overall objectives, according to the GA, are to ensure efficient internal and external communication, if it does not fall under the tasks of WP1. For this purpose, the Plan for the Exploitation and Dissemination of Results (PEDR) is regularly updated.

Stakeholders are a vital part of the project and are therefore involved in communication and dissemination activities right from the beginning of the project. In addition, an external independent Stakeholder Advisory Board (SAB) is established together with WP1. To address and keep stakeholders and the wider public informed, appealing online content about the project goals and results is created on a national, European, and international level. Another objective is to ensure open access to (non-confidential) research results and to make sure that these results can be securely accessed and preserved beyond the duration of the project. WP8 advises the project partners on open access, open source, open science, and the corresponding Horizon 2020 requirements.

To make the most out of the results, bring them closer to the stakeholders and promote (science) related skills a training and capacity building programme is created (D8.6 and D8.7).

At the end of each project year, WP8 collects and documents the dissemination activities of all partners and reports on them in the annual dissemination report (D8.3).

3.8.2 Progress achieved

This part is an excerpt of the Annual Dissemination Report I (D8.3), which was elaborated and published by WP8 in a detailed manner. The Annual Dissemination Report can be found on the TRUSTS website.[7]

D8.1 Dissemination and Communication Strategy, design guide, materials, and communication channels

Within this deliverable the communication plan and strategy was set up and is regularly updated. It gives an overview of the communication and dissemination activities planned during the project and represents a guideline for the TRUSTS partners. These activities involve both digital and print media and their impact is regularly measured through standard analytics tools. To spread the project results and increase the visibility of the project the partners are involved in these activities. To coordinate the activities and facilitate communication within the consortium, WP8 created an internal mailing list and a folder structure on Google Drive.

Furthermore, within the plan and strategy the different target groups were identified and the roles of the partners and the means of external communication and dissemination were explained in more detail. The means of external communication and dissemination include:

- project logo and icon
- project website
- social media channels (LinkedIn, Twitter)
- academic publications and conference attendances
- social microlearning
- ResearchGate
- press releases
- newsletters
- webinars
- podcasts
- interviews
- workshops, training and capacity building programme, and tutorials
- events and meetings
- promotional material
- templates for documents, presentations, etc.

To ensure a coherent and consistent picture of TRUSTS within these communication and dissemination activities, a design guide including the branding and visual language of the project was created. It includes information about the logo and the icon, its use, the RGB and CMYK colour codes for the logo, text and layout elements as well as typography for web and print. On the basis of this guide, the project logo and icon, project website[8], social media channels (LinkedIn[9], Twitter[10]) and document/slide templates, and ResearchGate account[11] were created. Furthermore, the main promotional materials (flyers, leaflets, postcards) were designed, which will be distributed next year when events are more likely to be held in person again.

[7] See https://www.trusts-data.eu/deliverables/
[8] See https://www.trusts-data.eu/
[9] See https://www.linkedin.com/company/trusts-trusted-secure-data-sharing-space/
[10] See https://twitter.com/TrustsData
[11] See https://www.researchgate.net/project/TRUSTS-Trusted-secure-data-sharing-space

Figure 21: TRUSTS logo and icon

Other communication activities such as newsletters, webinars, podcasts, interviews, etc. were and are performed during the lifetime of the project. Please find a detailed list of these communication and dissemination activities below.

Table 5: Other Public Non-Scientific Dissemination and Communication Activities in 2020

Type of dissemination and communication activities	**Title**	**Authors, Work Package, Lead Beneficiary**	**Date, year**	**Publisher, Place of publication, Relevant pages, URL**
Press Release 1 & Journalist call	TRUSTS: Innovationen für einen pan-europäischen Datenmarkt	Nina Popanton, WP8, DIO	07/09/2020	Nina Popanton via APA: https://www.ots.at/presseaussendung/OTS_20200907_OTS0005/trusts-innovationen-fuer-einen-pan-europaeischen-datenmarkt via website: https://www.trusts-data.eu/innovating-european-data-markets-trust/ Alexandra Garatzogianni via CORDIS: https://cordis.europa.eu/article/id/422093-trusts-innovating-european-data-markets-through-trust-security-and-federation EBOS via website http://www.ebos.com.cy/trust-innovating-european-data-markets-through-trust-security-and-federation
Press Release 2	TRUSTS Datenethik: Zentrale Regelungen für Datenaustausch	Nina Popanton, WP8, DIO	07/12/2020	Nina Popanton via APA: https://www.ots.at/presseaussendung/OTS_20201207_OTS0013/trusts-datenethik-zentrale-regelungen-fuer-datenaustausch via website: https://www.trusts-data.eu/trusts-ethics-key-regulations-of-data-sharing/ Alexandra Garatzogianni via CORDIS: https://cordis.europa.eu/article/id/428590-trusts-ethics-key-regulations-of-data-sharing-establishing-a-suitable-eu-data-governance-fram/de

Podcast 1	TRUSTS Podcast – Data Markets and Interoperability	Nina Popanton, WP8, DIO Stefan Gindl, WP3, RSA	28/09/2020	Nina Popanton via YouTube, Manuela Schlömmer via TRUSTS Website https://www.trusts-data.eu/trusts-podcast-data-markets-and-interoperability/
Podcast 2	TRUSTS Podcast - Business Perspective "How will Data Markets shape the European Industry?"	Nina Popanton, WP8, DIO; Bert Utermark, WP8, G1 Hosea Ofe, WP2, TUD	14/12/2020	Link from website to follow in the next annual dissemination report
Newsletter 1	TRUSTS quarterly	Manuela Schlömmer, Nina Popanton, WP8, DIO Gianna Avgousti, WP5, EBOS Technologies Ltd Alan Barnett, WP4, Dell EMC Lidia Dutkiewicz, KU Leuven	17/09/2020	Manuela Schlömmer via Sendinblue and TRUSTS website https://www.trusts-data.eu/trusts-quarterly/

		Bert Utermark, Andreas Huber, G1 Ioannis Markopoulos, FNET, Nora Gras, WP1, IDSA		
Newsletter 2	TRUSTS quarterly	Manuela Schlömmer, Nina Popanton, WP8, DIO Charlotte Ducuing, Yuliya Miadzvetskaya, WP6, KU Leuven Silvia Castellvi, WP1, IDSA Ioannis Markopoulus, WP2, FNET Natalia Simon, Silvia Castellvi, WP1, IDSA Ioannis Markopoulos, WP2, FNET	17 December 2020	Articles on TRUSTS website https://www.trusts-data.eu/news/

		Bert Utermark, WP7, G1 Benjamin Heitmann, WP3, FhG Martin Kaltenböck, Thomas Thurner, WP2 and WP3, SWC Andreas Trügler, WP4, KNOW Sebastian Steinbuß, WP1, IDSA Stefan Gindl, WP3 RSA FG Antragama Ewa Abbas, WP2, TUD		
Webinar 1	The Core of TRUSTS: Innovating European data markets through trust, security, and federation	Manuela Schlömmer, Peter A. Bruck, WP8, DIO Natalia Simon, Silvia Castellvi, WP1, IDSA Ioannis	29/10/2020	Manuela Schlömmer via TRUSTS website https://www.trusts-data.eu/webinar-the-core-of-trusts-innovating-european-data-markets-through-trust-security-and-federation/

		Markopoulos, WP2, FNET Bert Utermark, WP7, G1 Charlotte Ducuing, WP6, KU Leuven Benjamin Heitmann, WP3, FhG Martin Kaltenböck, Thomas Thurner, WP2 and WP3, SWC		
Interview 1	How can sovereign data exchange take place in Europe and which are the business benefits?	Nina Popanton, WP8, DIO Sebastian Steinbuss, WP1, IDSA	27/11/2020	Nina Popanton via TRUSTS website https://www.trusts-data.eu/how-can-sovereign-data-exchange-take-place-in-europe-and-which-are-the-business-benefits/
Interview 2 and 3	TRUSTS, European cloud and Gaia-X, and Austrian cloud and DIO	Nina Popanton, Peter A. Bruck, Günther Tschabuschnig, WP8, DIO	December 2020	Links to follow in the next annual dissemination report
Participation in conference	Handeln mit Big Data: Vom Technologie-	DIO, WP8	18/09/2019	DIO via website https://www.dataintelligence.at/de/events/data-

	Showcase zur profitablen Wertschöpfung. Highlight-Konferenz zur Vorstellung der Leistungen und Ergebnisse von Data Market Austria			market-austria-konferenz-2019-in-wien.html
Newsletter	Data Market Austria newsletter: includes text/link about requirements elicitation survey	SWC, WP2, WP3	26/02/2020	SWC via email
Participation in conference	The 14th International Conference on Research Challenges in Information Science	RSA FG, WP3	22-25/09/2020	http://www.rcis-conf.com/rcis2020/program.php
Participation in conference	Hannover Messe Digital Days	LUH, WP1	14-15/07/2020	https://www.hannovermesse.de/en/news/digital-days/hannover-messe-digital-days
Participation in conference	Research & Innovation Days	LUH, WP1	22-24/09/2020	https://research-innovation-days.ec.europa.eu/
Participation in conference	NGI Policy Summit	LUH, WP1	28-29/09/2020	https://summit.ngi.eu/
Article on website	New H2020 project TRUSTS for secure sharing of data kicks off!	EBOS, WP5	23/01/2020	EBOS via website http://www.ebos.com.cy/new-H2020-project-TRUSTS-for-secure-sharing-of-data-kicks-off
Article on website	The TRUSTS project partners reflect on	EBOS, WP5	24/06/2020	EBOS via website http://www.ebos.com.cy/the-trusts-project-partners-reflect-on-progress-

	progress accomplished towards a Trusted Secure Data Sharing Space and plan the way forward			accomplished-towards-a-trusted-secure-data-sharing-space-and-plan-the-way-forward
Webinar	IDSA Virtual Expo Live Session "Restoring Trust in Data Markets & Data Spaces – The Trusted Secure Data Sharing Space"	IDSA, LUH, WP1 FhG, WP3	07/05/2020	IDSA via YouTube https://www.youtube.com/playlist?list=PLjtVEFHmKqTum4mtp0_WjBoHoI0vh3DDj
Webinar	Live Session: TRUSTS, in the financial industry - enabling data sovereignty beyond existing solutions	LUH, WP1 EBOS, WP5 REL, WP3 FhG, WP3	29/09/2020	EBOS via website http://www.ebos.com.cy/trust-innovating-european-data-markets-through-trust-security-and-federation
Webinar	Live Session: TRUSTS, in the financial industry - enabling data sovereignty beyond existing solutions	LUH, IDSA, WP1 EBOS, WP5 REL, WP3 FhG, WP3 PB, WP3	12/11/2020	EBOS via website http://www.ebos.com.cy/trust-in-the-financial-industry-enabling-data-sovereignty-beyond-existing-solutions http://www.ebos.com.cy/trust-live-session LUH via YouTube https://www.youtube.com/watch?v=EUcO-SoO11s&t=0s Nina Popanton via TRUSTS website https://www.trusts-data.eu/financial-industry-needs-trusts/
Webinar	IDSA Live Session – Tech Talk "The IDS	IDSA, WP1 FhG, WP3	03/09/2020	IDSA via website https://www.internationaldataspaces.org/recorded-

	Information Model”			idsa-live-sessions/#_techtalks YouTube https://www.youtube.com/watch?v=V1WvJkaHQJ0

Table 6: Scientific publications by TRUSTS partners in 2020

Type of scientific publication	Title of scientific publication	DOI, ISSN or eSSN	Authors, Work Package, Lead Beneficiary	Title of the journal or equivalent	Number, date, year	Publisher, Place of publication, Relevant pages	Public & private publication[4]	Peer-review	Open Access
Publication in conference	Practice and Challenges of (De-)Anonymisation for Data Sharing	10.1007/978-3-030-50316-1_32	Alexandros Bampoulidis, Alessandro Bruni, Ioannis Markopoulos, Mihai Lupu	Research Challenges in Information Science. RCIS 2020. Lecture Notes in Business Information Processing	Vol. 385	Springer, Cham. https://doi.org/10.1007/978-3-030-50316-1_32	Public	Yes	Green
Article in journal	The recent case law of the CJEU on (joint) controllership: have we lost the purpose of 'purpose'?	ISSN: 0771-7784	Ducuing Charlotte, Schroers Jessica	Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht	Vol. 2020, iss. 6	Kluwer	To be public	Yes	No. An open access version will be accessible via the KU Leuven repository within some time

The deliverable was submitted on 31 March 2020 within the given time frame and made available on the website[12].

D8.2 Website update, materials

This deliverable starts with an introduction of the TRUSTS project including the objectives, channels, and target audiences. It continues with the website history, how the website has developed during the year, and shows the created templates and promotional material. Also the cooperation with and links to other projects are outlined. The deliverable ends with the next actions for the website and promotional material taking into account the research undertaken in WP2-6.

The basic website was set up prior to the beginning of the project in September 2019 and was revised by the consortium members in February and March 2020. It represents the main communication channel of the project and is regularly updated and filled with content, taking into account the progress within the project. Within the website update, a newsletter *Subscribe* button was added and the knowledge base was implemented as a submenu under *News & Events*. The knowledge platform is aimed at targeting the expert community and is an additional channel for dissemination and knowledge sharing including links to relevant articles and websites.

The next steps include an extra section for the stakeholder overview and Stakeholder Advisory Board, update and expansion of the use cases as well as the upload of research papers, reports, or other publications, which will be accessible to everyone according to the Open Access Policy of the EU.

The deliverable was submitted on 4 September 2020 and made available on the TRUSTS website.[13] The contractual due date was 30 June 2020. Reasons for the delay were the limited possibilities for settlement in the context of the COVID-19 crisis and the concomitant limited availability of various service providers.

3.8.3 Next Steps

In 2021 new communication activities are planned such as a webinar series, quarterly newsletters, podcasts, expert talks, guest comments, creation of an Ambassador Programme (e.g. early adopters, committed researchers, etc.), other stakeholder engagement activities and the creation of a Stakeholder Advisory Board with WP1. To have an overview of the concrete communication and dissemination activities in the upcoming year, a detailed communication roadmap including various cross-media activities will be created at the beginning of 2021.

The public project outcomes and activities of the different WPs will be regularly published and made available on the TRUSTS website and other communication channels and Open Access databases (scientific articles). In doing so, the website and communication channels are updated on a regular basis.

Together with LUH, Relational SA, SWC, G1, and FNET, DIO will establish a training and capacity building programme including e-learning to create awareness about the project and its results and train especially technical audiences. The benefits for different target groups should be conveyed.

[12] See https://www.trusts-data.eu/deliverables/

[13] See https://www.trusts-data.eu/deliverables/

Furthermore, the first of two public events will be organised in M18, where stakeholders in data economy and data science as well as policy makers and EU institutions and bodies get together. This is the perfect opportunity to present TRUSTS and its benefits and results directly to the participants. Depending on the situation within the pandemic, it will be held in person, online or in a hybrid way.

3.9 WP 9 Ethics requirements

3.9.1 Objectives

WP9 “Ethics requirements” was added by European Commision. The objective of WP9 is to ensure compliance with the “ethics requirements” described in the Grant Agreement, Annex 1. These are the following concrete goals:

- Templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) must be kept on file.
- The applicant must check if a declaration on compliance and/or authorisation is required under national law for collecting and processing personal data as described in the proposal. If yes, the declaration on compliance and/or authorisation must be kept on file.
- If no declaration on compliance or authorisation is required under the applicable national law, a statement from the designated Data Protection Officer that all personal data collection and processing will be carried out according to EU and national legislation must be kept on file.
- The beneficiary must explain in the grant agreement how all of the data they intend to process are relevant and limited to the purposes of the research project (in accordance with the ‘data minimisation ‘principle).
- Description of the anonymisation/pseudonymisation techniques that will be implemented must be submitted as a deliverable.
- The beneficiary must evaluate the ethics risks related to the data processing activities of the project. This includes also an opinion if data protection impact assessment should be conducted under art.35 General Data Protection Regulation 2016/679 and/or art.27 of the Directive 2016/680. The risk evaluation and the opinion must be submitted as a deliverable.
- In case the research involves profiling/ tracking, the beneficiary must provide an explanation how the data subjects will be informed of the existence of the profiling/ tracking, its possible consequences and how their fundamental rights will be safeguarded. This must be submitted as a deliverable.
- The beneficiary must provide details on the Artificial Intelligence/ Data Mining system and related decision making procedures including information about human actors’ roles and responsibilities. The beneficiary must also describe a set of precautions to eliminate or mitigate potential algorithmic biases and explain how the model will be able to justify the results it has provided for specific situations. This must be submitted as a deliverable.
- In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has a lawful basis for the data processing and that the appropriate technical and

organisational measures are in place to safeguard the rights of the data subjects must be submitted as a deliverable.

3.9.2 Progress achieved

In order to ensure compliance of the TRUSTS project with "ethics requirements" described in the Grant Agreements, the following process has been set up. A questionnaire was drawn by KU Leuven and circulated amongst all TRUSTS partners. It was accompanied by a Background Note providing further explanation on applicable data protection legal provisions in order to ease the filling of the questionnaire. The filling of the questionnaire was use case-specific. Three questionnaires were drawn, namely one questionnaire for every use case as coordinated by respective use case leaders. A virtual meeting was convened to have a general discussion between partners on the ethics requirements and on how to comply with them. A virtual meeting was convened for every use case in order to tailor the ethics deliverables. Based on the information gathered through the questionnaires and the virtual meetings, a first version of the ethics deliverables was drawn and circulated amongst the partners. After internal review amongst TRUSTS partners, all required ethics deliverables for WP 9 were submitted to the European Commission.

3.9.3 Next Steps

Ethics deliverables shall be considered as a consistent set of measures aimed at ensuring compliance with ethics requirements within the TRUSTS project. Finally, compliance with ethics and legal requirements are considered a continued effort by the partners, to be maintained throughout the project. After the submission of the ethics requirements, KU Leuven will keep providing guidance to the TRUSTS partners.

4 Progress within specific Leads

4.1 Scientific Lead

Objectives
The key objectives of scientific coordination in TRUSTS are to: - Ensure compliance with the H2020 OA policy. - Promote the application of good research practices. - Monitor and foster progress towards collaborative research within the project. - Create and enforce the structure for reporting on scientific progress. - Provide opportunities for identifying and/or enhancing research opportunities. - Ensure research activities remain focused on and cover ICT 13-2018-2019 Call's specific challenges and objectives. - Facilitate learning of research lessons at a metalevel

- Maximise research synergies and opportunities
Progress achieved
A structure and clear procedure for monitoring of research progress has been defined and communicated to the consortium. This enables the monitoring of papers that are being worked on, their relationship to TRUSTS tasks and specific challenges of the Call. As of today, the consortium has 2 published papers and 7 additional papers in the working. This is more than consistent, for this stage of the project, with the fact that TRUSTS is an Innovation Action. The Scientific coordinator also defined and delivered a presentation to the consortium defining 10 principles to be followed in TRUSTS for good research and collaborative practice. These principles, are detailed in a document on the shared drive and address the areas of: planning instead of spontaneity, transparency instead of secrecy, cross-partner collaboration and fostering of inclusive participation, linking and acknowledging, use of technology to lower administrative overhead, research integrity, ethics, reproducibility, research data and open source and Open Access.
Next Steps
- Monitoring progress and discussing with relevant consortium partners how to make sure that all of the specific challenges of the Call are addressed in our research. - Further strengthening links between the more research oriented and development oriented work packages (primarily WP3 and WP4) - Further encouraging experimentation and validation of key TRUSTS components.

4.2 Technical Lead

Objectives
The main objectives of the technical lead are: 1. architecture design in accordance with task T2.4. **(TL-O1)** 2. coordination of architectural alignment between work packages 3, 4 and 5. **(TL-O2)** 3. project management and oversight to execute WP3 according to DoA. **(TL-O3)**
Progress achieved
In the first year of the project, the main goal of the technical lead has been the establishment of a consensus amongst the technical project partners about the high level architectural aspects of the project. In particular, this consensus is most important for cross-cutting aspects of the project, such as the architectural paradigm, the reuse of existing software and non-functional requirements of strategic importance. Therefore the most important result of year 1 towards **objective TL-O1 (architecture design)**, is the initial

version of the TRUSTS platform architecture. The architecture represents the conceptual foundation for the implementation of the TRUSTS platform, and therefore reaching a consensus on the architecture enables all project partners with a technical view to agree on the most important abstract decisions, before realising them in their implementation. In addition, the architecture also allows the project partners with a non-technical view to contribute with cross-cutting requirements of strategic importance, such as having future proof characteristics, e.g., compliance with GAIA-X concepts.

With regards to objective **TL-O2 (coordination of architectural alignment in WP3/4/5)**, the technical lead has organised or initiated several activities on different scales within the project:

- Project wide activities:
  - Organisation of a 2-day tech workshop in M5;
  - Participating in the online plenary at M6;
- Work package specific activities:
  - Technical sessions in WP3 with external software owners from the IDS ecosystem;
  - Brainstorming session with participants of WP4 about the impact of security and privacy requirements on WP3.
  - A session on alignment of WP3 with the use case trials in WP5.
  - First definition of coarse-task backlog of services that need to be developed de novo and adaptations that have to be done to existing ones.
- Bilateral coordination and ideation sessions:
  - With leaders of use case trials from WP5.
  - With the leaders of the privacy enhancing technology work package (WP4).
  - With the leaders of the business model, exploitation & innovation impact assurance work package (WP7).

With regards to objective **TL-O3 (project management and oversight of WP3)**, the technical lead has established the following management instruments:

- A regular telephone conference for all WP3 participants (every two weeks). This allows task leaders to report on progress and obstacles, and provides an easy way for participants to reach out beyond the context of their own task without formal overhead to allow synchronisation between tasks.
- A regular telephone conference for all participants of the architecture design task T2.4, which takes place in alternating weeks to the WP3 telephone conference. It provides the technical participants an avenue to focus on the architectural design, without excluding technical expertise required to anchor the abstract architectural perspective in the technical details.
- A mailing list for WP3 participants to communicate without adding noise to the general project mailing list.
- Availability for telephone calls to exchange feedback and ideas on short notice whenever urgently required by a project participant.

In addition, the technical lead has participated in dissemination and outreach activities (cf. WP8):

- Web seminar: “IDSA Live Session: Restoring trust in data markets & data spaces (TRUSTS)”, May 2020.
- Web seminar: “The core of TRUSTS: Innovating European data markets through trust, security, and federation”, October 2020.
- Web seminar: ”TRUSTS in the Financial Industry - Enabling data sovereignty beyond existing solutions”, November 2020.

Next Steps

In year 2, towards **objective TL-O1 (architecture design)** the architecture specification will be iterated based on feedback from the use case partners and from the non-technical project partners. Together with the use case partners, the technical environment for testing the use case trials will be defined in multiple, iterative versions. Complementary to that, the technical impact of the requirements identified in the area of business models for data marketplaces and the legal requirements will be investigated and will be addressed if necessary through updates of the architecture.

The refinement of the architecture is also intertwined with the planned activities towards **objective TL-O2 (coordination of architectural alignment in WP3/4/5).** In particular, close interaction with the use case trials in WP5 and the integration of the privacy enhancing technologies from WP4 into the platform are expected to require a high degree of effort in year 2.

With regards to objective **TL-O3 (project management and oversight of WP3)**, all related activities from the first year will be continued and refined. If necessary, additional management instruments will be instated.

Finally, participation in dissemination and outreach activities continues to be a high priority.

4.3 Innovation Lead

Objectives

Innovation management ensures that the development of both market and technical problems will be accomplished during the project, while enabling the successful implementation of appropriate creative ideas, so that new and improved products, services and processes will belong to the project’s output ensuring thus its sustainable update beyond its duration.

Progress achieved

The innovation management methodology, relation to the projects WPs and focus areas have been defined:

Market and technical problems	Successful implementation	New and improved products, services and processes	Sustainability
• Which are the market (industries) problems • Which are the technical and operational problems • Which are the standardisation problems • Which are the policy problems (whey EU think trust is lost in data marketplaces?)	• How implementation of the E2E (platform, processes, etc.) promotes the envisaged innovation vs the state of the art		• How do we protect the investment (IPR management) • Which are going to be the standardisation/regulatory contributions • Significant papers • Community built • Seek activities for further funding of additional functionality
Target: • Analyse current gaps and trends (D2.1, D7.1, D6.2) • Define how TRUSTS will fill the gaps and take advantage of the trends (D2.2, D2.3, D6.3, D6,4, D7.2)	**Target:** • Define the architecture that leads to the envisaged innovation (D2.6, D2.7) • Implementation supporting the envisaged innovation (D3.9, D3.10, D3.11, D4.1, D4.2) • Evaluation of the implementation with real users (D5.10, D5.11)		**Target:** • Protect innovation (D7.4, D7.5) • Maximise impact through contribution to standards, scientific contributions and Innovation impact assurance (all other WP7 deliverables, all WP8 deliverables)

In detail the methodology adopted and actions performed are summarised in the following:

- Safeguard that in each deliverable we identify the innovation topics and if appropriate report then in a respective section according to the innovation focus areas and targets
- TRUSTS innovation registry was defined
- Align all leads' plans

Next Steps

In Year 2 the innovation management will focus on revealing innovation issues developed within each individual WP. These issues will be reported in the innovation registry and will be analysed to maximise their exploitation potential.

4.4 Security Lead

Objectives

From data security point of view, The TRUSTS project should be carefully evaluated for two main aspects:

1. GDPR Compliance -
   TRUSTS aims to create a GDPR-compliant European Data Marketplace by respecting the rules and principles through constant guidance from a leading expert partner in law and ethics in the Consortium, KUL, and by taking into account already existing national and international

initiatives.

2. Privacy Preserving capabilities -
   The TRUSTS partners will develop and improve privacy preserving technologies to foster the European Data Economy and at the same time provide business and ethical/legal tools to make these technologies easily adoptable and sustainable.

Under these two main pillars, we are keeping track of the project's advancement while ensuring that outcomes are compliant and safe from a security point of view.

Progress achieved

Currently, WP3, WP4 & WP6 have advanced in the security comprehension, where we better understand how the deliverables and outcomes should address security issues and potential vulnerabilities under different scenarios.
As a conclusion, the progress of the security-related issues goes according to plan.

Next Steps

While solution maturing and getting ready for implementation, we should keep track of the ethics, GDPR and privacy preserving modules and approach.

4.5 Legal & Ethical Lead

Objectives

Our main objective is to develop a robust legal and ethical framework for the TRUSTS Platform to ensure sustainability and compliance of the innovation brought by the project with all relevant regulations and ethics principles. This objective targets both the outcome of the project (i.e., the TRUSTS platform) and the individual use-cases. The work varies from general guidance of the consortium towards legal and ethical compliance, via guidance towards ethically compliant trials and testing as well as guidance in taking into account and embedding into the developed technologies of the key principles and rules, to research of aspects of the main legal frameworks, inter alia data protection, competition, consumer protection, that are specific to the development of a solution for sharing, computing and extracting the desired value out of personal and industrial data.
Based on this work, WP6 also aims to make recommendations as for whether and how the legal framework should evolve in order to rightly regulate data market ecosystems.
In order to achieve these goals, WP6 shall identify relevant overarching legal rules and ethical principles and provide guidance for their implementation in the course of the project's development. The result of this WP will be a set of requirements, which will enable the continuous monitoring of the work progresses, the final evaluation of compliance of the technological solution developed and recommendations for policy makers and stakeholders in the field.
The various tasks of WP6 should be viewed as a continued effort towards these overall objectives.

Progress achieved
KUL addressed all the ethics requirements of the Commission from WP9. Furthermore, KUL finalised D6.2, which will be submitted by the end of October 2020. KUL is also working on D6.1 to be submitted in February 2021.
Next Steps
D6.2 will be submitted at the end of October. After the submission we will start working on D6.1 devoted to Research Ethics. This deliverable will provide all information regarding the compliance of the project research activities with research ethics and, in particular, with the H2020 Programme Ethics Guidance. This deliverable will be submitted by the end of February 2021.

4.6 Communication & Community Building Lead

Objectives
The main objectives of WP8 is to ensure efficient communication and dissemination within and outside the project, create engaging online content and engage relevant stakeholders to achieve sustainable results beyond the lifetime of the project. In 2020 the basis for the promotion of the project has been set - the branding is completed, now the project must find its public reception. To achieve this, WP8 spreads information on TRUSTS' progress continuously towards the public and all relevant target groups (journalists, researchers, etc.). Channels have been established and contact points to the community have been created, to ensure efficient communication within and outside the project. For 2020, a communications roadmap has been set-up and pursued; a strategic communication plan will be created for 2021 too so that TRUSTS remains present in the media landscape as well as on relevant social media platforms. The project's stakeholders have been identified by T7.2, WP8 has suggested specific communication activities to engage with those stakeholder to a maximum extent - those engagement activities will be carried out in the following phases of the project. Online activities are increasing and also the reception (followers, reactions, etc. on social media platforms) is gradually rising. To ensure open access to research results, the deliverables have been published on the project's website. WP8 has been involved in the establishment of an external and independent Stakeholder Advisory Board (SAB, lead: WP1), and will continue to do so and keep in fruitful contact with the members of SAB.
Progress achieved
So far, deliverables D8.1 and D8.2 have been submitted. The second deliverable has been handed in with a little delay due to coordination difficulties with and limited availability of service providers during the corona crisis. The corporate design, public appearance, and promotional materials have been developed; relevant channels (website; social media: Twitter, LinkedIn, YouTube, ResearchGate) have been established and are continuously updated and filled with content. The expansion of the network has started and is in progress - special efforts are being made to reach the relevant target groups and to draw their attention to TRUSTS or to engage them in the project (through workshops, participation of the

consortium members in meetings, events and other activities, etc.). Especially in Austria, journalists from relevant media are already aware of the project, which makes it easier to achieve publications in the future.
As far as the Capacity Building Activities (D8.6 and D8.7) are concerned, a suite of outreach and capacity building tools has started to be developed. These tools will combine a range of materials on the matter (**presentations** and **multimedia** content (i.e., video tutorials)), drawing on contents elaborated in other modules, and turn them into formats that can be used in different types of capacity building exercises. These exercises will include online, distance learning elements (e.g. webinars), and actual face-to-face meetings. They will be combined wherever possible, giving insights into the benefits of "blended learning".

Furthermore, Relational SA started to develop a method to analyse the social awareness of emerging technologies based on Twitter data mining. First, the natural language processing module in the Thomson Data Analyser will be applied to extract the keywords from tweets. Second, social awareness information will be analysed by applying text mining and social network analysis; the social awareness of emerging technologies will be subsequently mined using a time-slicing based awareness information map. Finally, the emerging data-driven innovation technologies will be given as a case study to analyse the effectiveness and feasibility of the method.

Next Steps

Currently, the remaining activities of the Communication Plan 2020 (additional newsletter, explainer video, additional podcast, additional press release, etc.) are being fully implemented to consolidate the media basis of TRUSTS.
At the beginning of the upcoming year, a strategically founded and target-group-tailored communication roadmap for 2021 will be developed. This will ensure on the one hand, that TRUSTS as well as the project's progress and results are visible in the media and, on the other hand, that the various stakeholders of the project are given the opportunity to interact with the consortium. The communication plan for 2022 will build on the strategic considerations and practical implementations of previous media plans to have a coherent and consistent communication package in place by the end of the project.
A special focus for 2021 will be the establishment of strategic cooperations with relevant media and particularly influential journalists. A media stakeholder network should be set up to ensure that the contents published by TRUSTS are adopted with great willingness. This special focus will also benefit the success of the Stakeholder Engagement Activities (T7.2) and integrate the media stakeholders into the network of all project stakeholders.
The next deliverable D8.3 Annual Dissemination Report I is due on 31 December 2020.

4.7 Business & Exploitation Lead

Objectives

Ultimate goal of business & exploitation planning as well as innovation impact assurance is to create a

sustainable business model and plan (incl. products & service portfolio, clear SLAs, pricing and billing etc.) for the TRUSTS Platform supported by a wide-reaching Data Innovation Environment. In doing so, it has to be ascertained that the governance and business model for the data marketplace adheres to (privacy) regulation, provides smart contracting to assure quality and service levels, and incentivizes providers, users and owners of data.
Achieving this objective will require to:

A. Analyze the market and build a community of stakeholders (SMEs, start-ups, large enterprises,academics, public administration) around the Data-Services Ecosystem that operate in a clearly regulated environment using innovative business models that ensure the long-term sustainability of the Data-Services Ecosystem beyond the end of the funding period.
B. Undertake standardization activities in view of supporting the standardization of data sharing platform
C. Undertake innovation and IPR management activities
D. Develop an impactful, realistic yet ambitious business plan for paving the way to the successful commercialisation of the TRUSTS Platform.

Progress achieved

Work within the specific work tasks of work package WP7 “Business model, exploitation & innovation impact assurance” is on track (see section on work package WP7, above). However, the role of the Business and Exploitation Lead goes beyond the coordination of the work package activities.
The project addresses the specific challenge by focusing on two complementary aspects of the problems hampering the growth of the data economy:

1. Technology: by providing a new state-of-the-art for specific challenges such as that of a secure platform, vitally needed for different data providers to interact confidently and successfully in a market; and
2. Business (commercial, operational, legal, standardization): by developing and testing innovative business models and the effects of current, and future regulations, as threats and incentives for data enterprises.

Therefore, we took an active role in the project to mitigate risks inherent in the dichotomy of R&D project activities on the one side with their focus on value creation in specific domains, and the project aspiration to deliver a commercially sustainable datamarket embedded in a vibrant ecosystem, with a focus on adequate value capture, on the other side.

- Project wide activities:
    - Participation and contribution to Management Board meetings, as per the project governance structure
    - Participation and contribution to the kick-off in M1
    - Participation and contribution to the online plenary in M6, alerting and aligning all consortia partners on the mandate of federatedness (platform interoperability and technical implementation of TRUSTS as a federator for other data markets), and providing a forum for discussion around a draft taxonomy
    - Participation and contribution to monthly consortia calls
    - Organisation of an AllHands “Positioning of TRUSTS” workshop in M10
- Work package specific activities:
    - For detail: See section on work package WP7

- Bilateral coordination and ideation sessions:
    - Regular interaction with prior DMA consortia partners, and stakeholders of the Austrian data landscape
    - Close coordination with and direct support of task leader 2.1 “EU and worldwide data market” in task planning and tactics ideation, thereby increasing project-relevance of market research and strengthening the linkage to task 7.1
    - Close coordination with the Technical Lead and regular participation in the weekly calls of task T2.4 “Architecture design and technical specifications”, thereby tapping into the planning of the technical implementation in work package WP3.
    - Close coordination with the task leader T3.3 “Interoperability Solutions” to jointly advocate interoperability beyond demonstration of principal technical feasibility
    - Close coordination with work package WP8 aligning on and creating synergies between stakeholder engagement, community building and project communication.

Next Steps

Current activities will be continued. Additionally, in year 2 of the project, the Business & Exploitation Lead, utilizing task 7.6 “Innovation Impact Insurance” as primary conduit, will additionally focus on collaboratively developing answers to the following critical questions (selection):

1. How can TRUSTS mitigate a potential shortfall / resource crunch effected by the changed environment related to the Data Market Austria? This data market other than assumed not being operational, adversely impacts 1) reusability of components, 2) conjoint development and testing in the field of data market federation, 3) readily accessible data market users and stakeholders for identification and addressing of real-life challenges and emerging requirements.
2. How can TRUSTS optimize the exploitation of R&D outputs around the defined three use cases with respect to data trading as opposed to mere data exchange & transformation?
3. How can TRUSTS meaningfully and at scale attract early adopters, particularly data buyers and sellers, as well as data markets for federation, whilst the platform is under development and no operating company is in place?
4. How can TRUSTS adequately and in meaningful formats engage with external stakeholders, in light of the COVID crisis?
5. How does TRUSTS contribute and link to artefacts and participants within the evolving European data economy, leverage and collaborate with parallel national and pan-European initiatives and projects, and ascertain a meaningful and sustainable contribution in support of the European Data Strategy?

5 Data Management Plan

5.1 Overview

Concerning the management of datasets created, processed and published within the TRUSTS project, the Data Management Plan, DMP, (D1.6) provides information on TRUSTS data management policy and key information. This includes the organisational and technical measures regarding data collection, handling and storage of data, as well as key aspects such as the responsibilities of the respective project partners, the compliance with the FAIR data principles (Findable, Accessible, Interoperable, Reusable) and information on data volume, access, licensing and integration features, in accordance with the relevant legal framework and in particular the GDPR. The DMP will be regularly updated to reflect the development and progress of the project in terms of Data Management. Updates of the TRUSTS DMP document will be provided in M24 and M36, respectively.

5.2 Purpose

The project's Data Management Plan, DMP, (D1.6) lists all relevant information on current and planned data management activities. It is based on the template for the ERC Open Research Data Management Plan. In summary, the management of research data in the TRUSTS project is based on the following rules:

- Provide a maximum level of security for sensitive data and personal data, including the exchange of personal and/or sensitive data between selected partners
- Use well-known, established repositories for publishing and archiving non-sensitive research data
- Encourage data providers to make non-sensitive data available using Creative Commons licences, e.g. CC-BY
- Raise awareness among researchers, companies and public stakeholders for the importance of making non-sensitive data available to the public

5.3 State of the art

In the following, an overview of relevant data activities from the start of the TRUSTS project is provided. It has to be noted that data has become an important raw material that is of high importance in nearly every industry sector worldwide. As such, the free flow of non-personal data is a prerequisite for a competitive data economy within the Digital Single Market (DSM). The DSM aims to fully unleash the data economy, allowing a free flow of data and therefore enabling companies and public stakeholders to store and process non-personal data wherever they choose in the EU. The General Data Protection Regulation (GDPR), on the other hand, already provides for the free movement of personal data within the Union, next to its primary goal of protecting personal data. The FAIR principles were established in 2016 by the FORCE 11 group, focusing on the optimal preparation of research data for humans and machines. In this context, FAIR data does not necessarily mean completely open data, but rather data to be '*as open as possible, as closed as*

necessary'. This is especially important when dealing with industrial partners and building sustainable business models.

As such, the (data) platforms which are needed have to consider all three aspects, DSM, GDPR and FAIR: considering all aspects, data can be traded, exchanged and published in a trustworthy and secure way providing clear legal and ethical frameworks, where data based services and related software & tools can be offered and easily used, and where data professionals can receive training to improve their knowledge and skills. Within the TRUSTS project, datasets of various natures are collected, processed or generated. This includes data that is already existing, e.g. anonymized customer relationship management (CRM) data, and new data such as metadata and project management data that is created as the project progresses.

5.4 DSM, GDPR and FAIR Data Activities by partners

All data-related activities within TRUSTS are carried out in accordance with the relevant legal framework and in particular the GDPR. Moreover it detailed data characteristics, privacy preserving security plans and authorisations and answering data security and privacy questions, such as where the data will be physically processed and what physical security protection features and privacy protocols are implemented. For overall activities, please see section 3.6, WP 6 Legal & Ethical Framework. Within the TRUSTS project, we the platform enables

- a fully operational, GDPR- and FAIR compliant European Data Marketplace for personal and non-personal data targeting individual and industrial use by leveraging existing data marketplaces (Industrial Data Space, Data Market Austria) and enriching them with new functionalities and services to scale out;
- demonstrate and realize the potential of the TRUSTS Platform in three use cases targeting the industry sectors of corporate business data in the financial and operator industries while ensuring it is supported by a viable, compliant and impactful governance, legal and business model.

Findability and **accessibility** of the public data within TRUSTS is ensured by publishing in data repositories (e.g. (https://data.uni-hannover.de with a Digital Object Identifier (DOI)) and on the TRUSTS website (https://www.trusts-data.eu/). This includes e.g. data typical for general project management processes collected by LUH and conclusive, and if necessary anonymized data collections regarding the performance and outcome of the project. Openly available data will include the bibliography of publications and public deliverables regarding the project and their underlying data, text documents, photos, time tables, deliverable plans and information sheets. Full, detailed metadata (descriptive, administrative and structural) will be provided for each data set to be published in the repository. Metadata and semantic layer information regarding the TRUSTS data platform are made available using the TRUSTS Knowledge Graph, which will be established by SWC. SWC will also support the harvesting and processing of TRUSTS metadata and controlled vocabularies. Regarding the associated metadata, the partner SWC is involved in the development of the TRUSTS metadata model. This schema will be made publicly available under an open licence (e.g. CC BY) to ensure broad use and adoption. TRUSTS metadata can be made available to enable search and recommender features, if the data owner (which is not TRUSTS) agrees on this to publish their metadata under an open licence. Metadata and controlled vocabularies will be stored in an RDF triple store. Metadata will be contributed by several partners, e.g. RSA, DIO, EOBS and REL. Other outcomes from

the project such as open online courseware on business model innovation and open data well as data regarding teaching programs are published by TUD data via 4TU.Centre for Research Data in an anonymized manner (https://researchdata.4tu.nl/ also with a DOI).

Interoperability of published datasets is ensured by using the DataCite DOI system with data publications in respective public repositories. By default, once a dataset is registered within the DataCite system, metadata will be also available in schema.org and JSON format. The expected data formats will include tables (.csv and .xlsx) but also reports containing interpreted data (.docx). Expected file size will be 1-10 MB or smaller. All files will be named according to a similar structure. SWC works in TRUSTS on the metadata and semantic layer as well as on interoperability. This means a TRUSTS information model and metadata schema is developed on top of existing standards or models in place as e.g. the IDS schema or the DMA metadata model, DCAT-AP for datasets or schema.org for data services. Such models and schemas will be mapped and/or linked to other relevant existing models and schemas. This enables interoperability and metadata (and data) acquisition for TRUSTS. Within Data marketplaces interoperability solutions, RSA works in the area of data standardisation. The outputs of this task will guide our actions relevant to data interoperability.

Reusability: The data resulting from the project and the data shared on the TRUSTS platform will be of a mixed nature (i.e., non-sensitive project data and sensitive personal and industrial/non-personal data). By default, only non-sensitive data or if necessary anonymized data on the performance of TRUSTS will be published on the TRUSTS website and in the repositories used, e.g. the LUH data repository and the 4TU.Centre for Research Data. For such data, open licenses such as a CC-BY 4.0 license is used. Both repositories offer long term preservation (>10 years), maintaining their integrity and authenticity over time. For public data, TRUSTS will secure interoperability and reusability through the complementary metadata and readme-files attached to each dataset. In addition, the TRUSTS website is available at the Internet archive. The URL has been reported to the Wayback Machine and is crawled regularly. The TRUSTS metadata schema / model will be made publicly available under an open license (e.g. CC BY) to ensure broad use and adoption. Metadata and semantic layer information regarding the TRUSTS data platform will be made available using the TRUSTS Knowledge Graph. Expected (sensitive) data outputs from the partners remain re-usable for TRUSTS partners during the project period, according to the consortium agreement. As a legal and ethical partner, KUL does a continuous monitoring of legal and political initiatives contributing to re-use of data as well as study the available scholarly work on the topic.

Allocation of Resources and Data Security: LUH is responsible for ensuring the implementation of the DMP. As such, staff time has been allocated in the proposed budget to cover the costs of preparing data and documentation for archiving. All research data collected as part of this project is owned by the respective partner who generated the dataset. The Principal Investigator of this project will take responsibility for the collection, management, and sharing of the research data. SWC is responsible for the metadata and semantic layer in TRUSTS. LST has set up a cloud environment (hosted on EU google servers) which allows the TRUSTS partners to develop the needed tools for the project in a secure environment. Backups will be taken periodically and a restoration process will be described in case of a failure. The development environment is accessible only to specific people related to the technical WPs and their applications and is constantly monitored. In addition, data is stored locally at secured servers provided by other partners. Further legal, copyright and security issues are a part of the following research. This includes the set-up of appropriate mechanisms to check the integrity and security of the applications that will be on boarded to the TRUSTS data marketplace. All transactions will be logged appropriately to maintain the appropriate quality, security and traceability levels.

With regards to data anonymization and de-anonymization, TRUSTS will comply with their obligations determined by the data owners. As such it is likely that only experimental data openly are made openly available, e.g. by the partner RSA. Importantly, bank and stakeholder data which will be collected, analysed and processed within TRUSTS will not be made openly accessible since the data is expected to contain sensitive information about physical persons and/or legal entities. All partners will ensure that the data processing will follow a GDPR compliant process and that data is properly anonymized and masked for processing. For example, REL, in collaboration with the creditor organizations cooperating within TRUSTS, will perform data anonymization/masking techniques that will protect and anonymize input data owned by creditors, before any interaction with TRUSTS data marketplace takes place.

Ethical aspects: Within TRUSTS, KUL is dedicated to ensure that legal requirements are complied with throughout the project, in particular with respect to data protection law, and that data processing activities are ethical. Based on a sound analysis of the ethical and legal frameworks applicable to the project, KUL will elaborate guidelines and investigate legal paths in order to ensure that, on the one hand, data subjects and data owners remain in control of their personal data and subsequent use, and, on the other hand, that industrial data is shared and traded in compliance with legal rights and fair remuneration of data owners. The mixed nature of the data requires that a delicate balance be sustained between the economic and non-economic interests (i.e. in the context of FAIR data) of the multiple actors involved at different levels of the digital value chain. This balance requires to take into consideration the regulatory framework applicable to individuals as producers and consumers of data (i.e., the GDPR, consumer protection law, unfair commercial practices directive etc.). It also involves the regulatory and ethical framework applicable to entities active on the DSM with regards to industrial data (i.e., the regulation on the free flow of non-personal data, platform regulation, competition law, intellectual property law, the AML directive, codes of conduct, etc.).

5.5 Processed and published data(sets) as of December 2020

So far, the published deliverables with included data have been made available on the TRUSTS website by the partner DIO. The respective items for the bibliography will be described in Dublin Core. The publications and the underlying public data will be described in the metadata format of the respective repository, will receive an identifier such as DOI or Handle wherever possible and will be licensed under CC0 or CC-BY 4.0. Openly available data includes a bibliography of publications regarding the project (in Text and XML format), as well as publications and underlying data, wherever possible according to H2020 open access policy and open research data pilot.

5.6 Next steps

As new data types and workflows are expected to emerge during the project duration, updates of the TRUSTS DMP document will be provided in M24 and M36, which will show in-depth information on the processed datasets and workflows.

6 Conclusions and Next Actions

The present deliverable D1.2 summarises the overall progress per Work Package and specific lead performed by the TRUSTS consortium during the first project year. For Each Work Package (WP) and for each specific Lead there are reports on overall objectives, achieved progress and next steps, including planning for the upcoming project months. While Chapter 3 focuses at the level of the project's Work Packages, Chapter 4 integrates the progress, status and next steps of the assigned Project Leads for TRUSTS, namely Scientific Lead, Technical Lead, Innovation Lead, Security Lead, Legal and Ethical Lead, Communication and Community Building Lead and Business and Exploitation Lead. Chapter 5 constitutes an update of the Data Management Plan, containing State of the Art, DSM, GDPR and FAIR Data Activities by partners and Processed and published data sets in the first year of the TRUSTS Project. D1.2 will be respectively updated in M24 and M36, reflecting thus the progress, status and planning of the TRUSTS consortium at task, WP and Lead levels.