TRUSTS
Trusted Secure Data Sharing Space

D6.3 'Legal and ethical assessment'

Authors: **Gugliotta Lorenzo (CiTiP – KU Leuven)**

September 2022

TRUSTS Trusted Secure Data Sharing Space

D6.3 'Legal and Ethical assessment'

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	D6.3 'Legal and Ethical assessment'		
Work Package	WP6		
Contractual due date	M33	Actual submission date	07/10/2022
Nature	Report	Dissemination Level	Public
Lead Beneficiary	KUL		
Responsible Author	Gugliotta Lorenzo		
Contributions from	eBOS, Dell, NOVA, Relational		

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete[1]	Changes	Contributor(s)
V0.1	01/03/2022	10%	Initial Deliverable Structure	Gugliotta Lorenzo (KUL)
V0.2	31/05/2022	40%	1st Version	Gugliotta Lorenzo (KUL)
V0.3	21/09/2022	60%	2nd Version	Gugliotta Lorenzo (KUL)
V0.4	28/09/2022	90%	Content and review	Gianna Avgousti (eBOS), Ohad Arnon (Dell), Dominik Kowald (KNOW)
V0.5	30/09/2022	95%	Addressing peer review comments	Gugliotta Lorenzo (KUL)
V1.0	06/10/2022	100%	Submission version	Gugliotta Lorenzo (KUL)

Disclaimer

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
AI	Artificial Intelligence
AML	Anti-Money Laundering
AMLD	Anti-Money Laundering Directive
29WP	Article 29 Working Party
B2C	Business-to-Consumers
CJEU	Court of Justice of the European Union
CRM	Customer Relationship Management
DCD	Digital Content Directive
DGA	Data Governance Act
DL	Deep Learning
DMA	Data Market Austria
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Digital Services Act
eBOS	eBos Technologies Limited
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
EUCFR	European Union Charter of Fundamental Rights
FATF	Financial Action Task Force on Money Laundering
FIU	Financial Intelligence Units
FL	Federated Learning
FNET	Forthnet-Elliniki Etairia Tilepikoinonion kai Tilematikon Efarmogon A.E.
FORTH	Foundation for Research and Technology - Hellas
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
HFL	Horizontal Federated Learning
IDSA	International Data Spaces e.V.
KNOW	Know Center GmbH

KUL	Katholieke Universiteit Leuven
KYC	Know-Your-Customer
ML	Machine learning
ML/FT	Money laundering and financing of terrorism
MPC	Multi-Party Computation
NBA	Next-Best-Action
P2B	Platform to Business
PEP	Politically Exposed Person
PET	Privacy-Enhancing Technique
PII	Personal Identifying Information
PSI	Private Set Intersection
RE	Recommender Engine
SCaR	Scalable Recommender System
SME	Small-Medium Enterprise
TFEU	Treaty on the Functioning of the European Union
TRM	Transaction Monitoring
TRUSTS	Trusted Secure Data Sharing Space
UC	Use Case
UCPD	Unfair Commercial Practices Directive
VFL	Vertical Federated Learning
WP	Work Package

1 Executive Summary

Deliverable D6.3 titled 'Legal and ethical assessment' provides the evaluation and validation of the TRUSTS project and activities from a legal and ethical perspective. In so doing, D6.3 takes stock of the research carried out in Deliverable D6.2 'Legal and ethical framework' and assesses to what extent and with which methodology the requirements identified in that deliverable have been implemented in the TRUSTS platform. The assessment is not confined to the compliance of the TRUSTS platform with the legal and ethical requirement: it also acknowledges that the observance of these requirements is not always straightforward, and that the applicable legal framework is prone to favouring more than one approach. In this vein, the present deliverable delves into the legal and ethical debate surrounding compliance with the (mostly evolving) legal framework applicable to several features and operations of the TRUSTS platform.

This deliverable bridges the requirements elicitation phase of Work Package (WP) 6 – concluded in Deliverable D6.2 and accompanied by a guidance process on those requirements as part of Task 6.3 – and the recommendation phase that will be the subject of Deliverable D6.4. Deliverable D6.3 checks the relationship between the TRUSTS projects and the applicable legal and ethical requirements, acknowledges the outstanding legal and/implementation challenges and opportunities, and provides material for the elaboration of legal and policy recommendations.

The researchers of KUL adopted a flexible methodological approach to this deliverable (described in Chapter 3) due to the multi-faceted nature of the deliverable. First, since the deliverable needs to account for the implementation by the TRUSTS Consortium of legal and ethical requirements, KUL researchers – as required as part of Task 6.3 – initiated a continuous guidance process with TRUSTS Consortium Partners to discuss legal and ethical issues and questions. As part of this approach, KUL researchers engaged in general and ad-hoc meetings to facilitate the understanding of certain legal and ethical requirements or questions. Then, since the deliverable also needs to take stock of the implementation process and pave the way for recommendations, KUL researchers also adopted a continuous research methodology to be up to date with regard to the latest developments in the legal frameworks applying to TRUSTS activities and operations. This research contributed to the discussion of the outstanding legal and ethical aspects concerning the Use Cases and the TRUSTS platform as a whole.

The present deliverable adopts a top-to-bottom approach whereby the core components of the TRUSTS platform, which enable the main operations, are first presented and assessed in general terms and then considered in their application under the various Use Cases. In this vein, the deliverable has assessed in Chapter 4 the legal and ethical implications of the TRUSTS Federated Learning (FL)-based model and of the TRUSTS anonymisation applications. The assessment has focused on the ability of these two components, and of their interaction, to minimise the data protection and privacy risks while enabling cooperation on data sets – including personal data – between several organisations with the support of data analytics and artificial intelligence (AI) techniques. This assessment has shown that the TRUSTS platform adopts state-of-the-art methods and techniques to combine data protection and data utility in a complex data marketplace potentially appealing to organisations in different sectors.

While the main applicable legal framework in the above assessment is the EU data protection framework, the deliverable has also analysed the impact and implications of specific legal frameworks to the TRUSTS platform and assessed how the platform is equipped to comply with them. This assessment

has focused on both existing laws and ethical principles – i.e., EU legal instruments governing digital markets and digital services, as well as the EU competition law and consumer protection framework – and on proposed legislation – i.e., the Data Governance Act (DGA) and the AI Act. Particular attention was paid – as per the objectives of Task 6.3 – to the competition law implications of business agreements between organisations participating in the TRUSTS platform operations, and to the consumer protection implications of market practices based by AI-enabled recommendations given by TRUSTS services. The importance of these frameworks is introduced in Chapter 4 and then elaborated on in Chapter 6, where the deliverable assesses the safeguards of the TRUSTS Recommender System (mainly responsible for the AI-based recommendations under UC2 and UC3) against the applicable legal rules and ethical principles.

Next, the deliverable delves specifically into the three TRUSTS Use Cases. The deliverable provides a legal and ethical assessment of each UC taking stock of the assessment of the two core TRUSTS pillars (i.e., Federated Learning and anomymisation applications), and with reference to the various applicable legal frameworks. The focus is on the envisaged deployment of the three UCs in real life. The deliverable describes succinctly the main purpose and workflow of each UC, outlines the actors involved as well as their roles & responsibilities, and subsequently provides the legal and ethical assessment with an open approach that accounts for as many possible real-life adaptations as possible of the basic UC scenarios. In contrast, Chapter 7 provides the legal and ethical assessment of the UC pilots, i.e., the internal project activities to simulate and test the process under each UC.

With regard in particular to UC1, the outstanding legal and ethical questions left open are dealt with in the subsequent chapter. It devotes a thorough – albeit initial and non-comprehensive – discussion to the legitimacy of processing of personal data for Anti-Money Laundering (AML) purposes, which is relevant to UC1 in the TRUSTS project. The discussion tackles the relationship between these two legal frameworks both from the perspective of public powers enacting AML laws that call for personal data processing; and from the perspective of private actors called upon to comply with these laws by carrying out one or more personal data processing operations. With regard to the first perspective (i.e., public powers), the discussion starts from the different – and at times diverging – aims and principles of data protection and AML legislations; delves into the limitations to the fundamental rights to privacy and data protection that can derive from EU or national legislation; and examines, through a review of recent case law of the Court of Justice of the EU (CJEU), the main criteria that AML laws should meet in order to be found compatible with these fundamental rights, the main focus being the proportionality and necessity tests. With regard to the second perspective (i.e., private actors), the discussion starts from the lawful grounds for processing under the General Data Protection Regulation (GDPR) and assesses which is likely to be the most suitable one under AML law; then applies the proportionality and necessity tests to private data processing operations with a particular focus on the AI-based component of TRUSTS AML applications, especially reviewed under Article 22 GDPR.

2 Introduction

Deliverable D6.3 is the third legal deliverable in Trusted Secure Data Sharing Space (TRUSTS), which follows up on the work performed in Deliverables D6.1 and D6.2 as well as Work Package (WP) 9 relating to ethics and legal requirements of the project. The present deliverable provides the following content:

- The methodology used by KUL researchers to provide guidance and oversight to TRUSTS Consortium and to facilitate the implementation of the legal and ethical requirements.
- It also describes the approach and methodology used to provide clarification to legal and ethical questions and issues, and update them on the evolving legal landscape, throughout the implementation phase;
- The results of the legal and ethical assessment of the TRUSTS platform in which KUL has validated the project from the legal and ethical point of view. The assessment covers both the core TRUSTS processes and technologies, as they are supposed to be deployed in real life, and the implementation phase, including the deployment of the three Use Case (UC) pilots; and
- A discussion on the outstanding legal and ethical issues stemming from the frameworks applying to the TRUSTS project and that might need to be subject to an ongoing analysis vis-à-vis the development of the legal framework at European Union (EU) level.

2.1 Mapping Projects' Outputs

The purpose of this section is to map the TRUSTS Grant Agreement (GA) 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

TRUSTS Task		Respective Document Chapter(s)	Justification
T6.3 Oversight, validation and update	*In this task, KUL, in close collaboration with the technical partners responsible for defining the platform architecture and developing the platform technologies, will guide and assess the integration of the legal and ethical requirements in the design of the platform. As the technical development of the project evolves, the task will: a) provide oversight and guidance on the implementation of the legal and ethical requirements; b) provide clarification on legal and ethical issues that may*	*Chapter 3*	*Chapter 3 describes the methodology used for the legal and ethical assessment and addresses in particular points a) and d) of the description.*
		Chapter 4	*Chapter 4 assesses the core TRUSTS components and architecture from a legal and ethical perspective, and addresses in particular point e) of the description.*
		Chapter 5	*Chapter 5 develops the*

arise; c) potentially identify legal and ethical barriers based on the research conducted in T6.3; d) keep the partners updated with regards to future legal developments that are relevant to the project; e) validate the project from the legal and ethical point of view. *The task will result in Deliverable D6.3 Legal and Ethical Assessment.*		*assessment focusing on the three use cases envisaged by TRUSTS, also addressing point e) of the description.*
	Chapter 6	*Chapter 6 elaborates on the outstanding legal issues stemming from the deployment of the use cases, and addresses in particular point b) of the description.*
	Chapter 7	*Chapter 7 provides the assessment of the use case pilots.*

2.2 Deliverable Overview and Report Structure

The deliverable is structured as follows:

Chapter 3 describes the methodological approach used by KUL to ensure guidance, oversight, and validation throughout the implementation phase, and to collect input from TRUSTS Consortium members on the implementation of the legal and ethical requirements.

Chapter 4 provides the legal and ethical assessment of the TRUSTS platform by analysing first its core components (Federated Learning model and anonymisation techniques); subsequently the responsibilities of TRUSTS under EU current and proposed platform regulation rules; and finally, the implications of competition and consumer protection law for TRUSTS, especially given the use of Artificial Intelligence (AI) and Machine Learning (ML) techniques in the three UCs.

Chapter 5 provides the specific legal and ethical assessment of the three UCs as they are supposed to be deployed in real-life scenarios.

Chapter 6 provides the analysis of outstanding legal issues and questions concerning the legal frameworks applying to the TRUSTS project and workflows across the three UCs; and

Chapter 7 provides the legal and ethical assessment of the UC pilots deployed during the project to test the three UCs.

3 Methodology

This Chapter explains the approach taken by the TRUSTS Consortium supporting in the implementation of the TRUSTS platform according to the identified legal and ethical requirements.

The methodological approach to this deliverable comprised of the following strategies:

- A constant guidance process carried out by KUL to the TRUSTS Consortium after the completion of Deliverable D6.2 (Legal and ethical requirements);
- Ad-hoc individual and wider meetings devoted to discussing specific legal and/or ethical questions; and
- As far as the research-based part of the present deliverable is concerned, continuous research and updates on the evolving EU legal frameworks applying to TRUSTS operations.

The details of each strategy are offered below.

3.1 Guidance to TRUSTS partners

In line with the Terms of Reference, KUL has ensured availability to provide legal and ethical guidance to the core TRUSTS tasks throughout the course of the project.

After the completion of Deliverable D6.2 (Legal and ethical requirements), which described the applicable legal frameworks to be taken into account, KUL circulated the deliverable to all TRUSTS partners and accompanied it with a list of legal and ethical requirements extracted from the deliverable. The figure below provides a snapshot of this list.

Figure 1: Snapshot of the list of legal and ethical requirements

#	Area	Requirement	Legal base	Reference in 6.2
1	Data protection	Identify the legal entity(ies) that qualify as data controller(s), i.e. as "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"	Art. 4(7) GDPR	3.1.1
2	Data protection	Identify whether, according to the role of more than one entity in TRUSTS, there is joint controllership shared by two or more legal entities	Art. 26 GDPR	3.1.1
3	Data protection	If there is joint controllership, data controllers shall "in a transparent manner determine their respective responsibilities for compliance with the obligations under [the GDPR], in particular as regards the exercising of the rights of the data subject […], by means of an arrangement between them"	Art. 26 GDPR	3.1.1
4	Data protection	Arrangements between controllers shall "duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects" and its "essence" shall be made available to the data subjects	Art. 26 GDPR	3.1.1
5	Data protection	Data controller(s) shall provide data subjects with the identification of recipients or categories of recipients	Art. 13 and 14 GDPR	3.1.1

The purpose of this list was twofold: first, it was aimed to make it easier for TRUSTS partners to assimilate the content of Deliverable D6.2 and to focus on the most important requirements steering the development of the technology for the TRUSTS platform going forward; and second, to provide a list of references sufficiently easy to monitor to model and adapt the legal and ethical guidance during the implementation of the requirements.

Along with this list, KUL provided guidance and validation support for the TRUSTS technology and processes during technical meetings and workshops. KUL researchers working on the project would participate in meetings devoted to discussing the technical content of the TRUSTS platform, and provide overviews of the main legal and ethical principles – mainly related to data protection and privacy, and data flows – applying to TRUSTS; KUL researches would also give both solicited and unsolicited advice

about potential legal and ethical hurdles that a given course of action or solution could have generated, as well as possible workarounds and solutions.

One final tool to support the continuous guidance to TRUSTS partners and to perform the validation of the project under Task 6.3 was the legal and ethical checklist (see Annex I). This document was used as a data collection input from the TRUSTS partners concerning the methods they used and the solutions they found to meet the legal and ethical requirements. The process to develop and deploy the legal and ethical checklist was the following:

- First, KUL researchers reviewed the initial list of legal and ethical requirements (the one circulated to all TRUSTS partners in M25) and updated it by cutting irrelevant requirements and adding new ones and/or reformulating existing ones;
- Second, KUL researchers presented the legal and ethical checklist during a Consortium plenary to stimulate interest and raise awareness about the exercise; and
- Finally, KUL researchers circulated the checklist asking TRUSTS partners to provide their own input. They then collected and analysed this input and used it to enrich the legal and ethical assessment provided in the present deliverable.

3.2 Ad-hoc meetings

KUL's general guidance and validation work was enriched by specific guidance provided to individual Consortium members. Given the wide-ranging nature of the legal and ethical requirements across the activities of the whole TRUSTS Consortium, individual members were often in need for ad-hoc advice and opinions on legal and ethical matters.

Individual Consortium members would therefore contact KUL researchers – either during general meetings or via email – and request a meeting. During the meeting KUL researchers would listen to the legal or ethical problem/question being raised, provide some initial guidance and, depending on the nature and extent of the request, provide additional, more well thought-through answers in a few days' time.

KUL and individual Consortium members held several ad-hoc meetings in particular after the release of Deliverable D6.2 and particularly on questions related to data protection law. The topics discussed during ad-hoc meetings were the following:

- General data protection law requirements and principles;
- Best strategies to select the correct lawful ground (Article 6 GDPR) for processing personal data;
- The legal and ethical issues surrounding the processing of personal (customer) data by obliged entities under Anti-Money Laundering (AML) law to detect suspicious transactions, especially with AI-enabled tools;
- The legal and ethical issues surrounding the use of personal data as training data to develop AI-driven AML tools to be subsequently deployed in real-life scenarios;
- Opportunities and limitations related to the scientific research exception for further processing of personal data; and
- The EU legal framework regulating data flows and data exchanges.

To the extent that the content of ad-hoc meetings might have been relevant to other Consortium partners, KUL researchers would make sure to update the rest of the Consortium and share the answers through the general mailing list and/or to other interested Consortium members.

3.3 Continuous research

In parallel to the activities described above, KUL researchers have continued to carry out legal research in the fields relevant to the TRUSTS project. This was done with a twofold objective:

- First, in order to provide the academic soundness necessary to substantiate the legal and ethical assessment of the project; and
- Second, to enrich the legal analysis carried out in this deliverable and to have a better view of the outstanding legal challenges and opportunities in the relevant legal frameworks, as current law stands and taking into account current legislative proposals. The ultimate goal was to have a thorough legal analysis capable of generating meaningful policy recommendations in Deliverable D6.4.

Legal research was carried out in particular in the fields of data protection and privacy law, in conjunction with legal and ethical perspectives on the use of AI and ML; AML law and its interplay with data protection law including with the use of AI; competition law; consumer protection law; and platform regulation law.

4 TRUSTS platform implementation: Legal and Ethical Assessment

This chapter describes the legal and ethical considerations raised by the implementation of the legal and ethical requirements into the TRUSTS platform. The chapter is broken down in three sections, each focusing on requirements belonging to a specific legal framework applicable to the TRUSTS platform. Each section lists all the requirements in scope of the project, explains to what extent they have been met by the platform, and highlights challenges and specific issues when relevant.

The applicable legal frameworks are the following: data protection (pursuant to the General Data Protection Regulation[2] (GDPR) and to the E-Privacy Directive[3]); responsibilities of online platforms and online intermediation services (pursuant to the Platform-to-business (P2B) Regulation,[4] the E-Commerce Directive,[5] the Digital Content Directive,[6] and – for illustrative purposes only – the most recent legislative proposals for the Data Governance Act[7] and the Digital Services Act (DSA);[8] competition law, pursuant to Articles 101 and 102 TFEU; unfair commercial practices, pursuant to the Unfair Commercial Practices Directive.[9]

4.1 Data protection and Privacy

This section is devoted to reporting on the implementation of the data protection requirements into the TRUSTS platform. TRUSTS will enable the use of functionalities that entail the use, inter alia, of personal data either for training an AI-enabled analytics model or for using TRUSTS' services and applications. It is

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[4] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

[5] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[6] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

[7] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act).

[8] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

[9] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').

therefore essential that TRUSTS relies on processes and technologies that allow for full compliance with data protection law, including EU fundamental rights to privacy and data protection.

The TRUSTS platform is predicated on the principle that the less data transfers are carried out, the lower the impact on the protection of personal data involved in the transfer. Therefore, the TRUSTS Partners have elaborated privacy-preserving techniques and approaches enabling collaboration on and exchange of models between entities working on data (whether personal or non-personal), while minimising the need for data transfers.

This is made possible by an architecture based on the interaction between 'nodes', each belonging to one participating organisation and allowing:

i. interface with the TRUSTS platform;
ii. interface with the trusted connector that enables connections between nodes;
iii. usage control systems; and
iv. access to the smart contract executor.[10]

The advantage of this architecture is flexibility, which allows for two different collaborative models:

a. Subscribers can use the assets developed and enhanced by other entities on their own premises by downloading an **application** that will run the available functionalities outside of the TRUSTS platform. This exempts the subscriber from having to import the data – personal or non-personal – it holds; or
b. Subscribers can use the **services** offered on the TRUSTS platform, by importing their data and leveraging the technology embedded in the TRUSTS service. The services run on the TRUSTS platform, whereas the applications run on the subscriber's premises.

All the three UCs envisaged in the TRUSTS project, which include both approaches mentioned above, are based on complex data interactions and operations that rely on advanced analytics, including with the use of AI/ML and that involve, at different stages, the use of personal data.

In order for these two approaches to work while fully complying with data protection law, the TRUSTS Consortium has investigated and developed ways enabling various entities to cooperate based on the data each of them holds without having to transfer the data sets to other entities and/or having to anonymise and de-anonymise large parts of such data sets. The TRUSTS Consortium has therefore privileged state-of-the-art techniques that rely on advanced cryptographic solutions capable, inter alia, of supporting complex data analytics processes: Homomorphic Encryption (HE); Deep Learning (DL) & Federated Learning (FL); Multi-Party Computation (MPC) based on Private Set Intersection (PSI).

4.1.1 Advanced privacy-preserving techniques and Federated Learning

This section introduces the use of advance privacy-preserving techniques before leaving room, in the next section, to the legal and ethical assessment of the solutions developed by TRUSTS.

[10] This component allows the execution of smart contracts necessary for the completion of data exchange operations between entities.

Due to the increasing processing power and predictive capabilities of AI/ML models, the use of such techniques is a source of concern for data protection as they generally allow for more insightful analysis of data and tend to require large amounts of personal data for training and development. AI/ML techniques based on FL can, however, contribute to mitigating these data protection concerns while leveraging the utility-generating power of AI/ML. The key principle of FL is to decentralise the provision of personal data. This makes it different from traditional approaches based on the centralisation of data provision, which requires multiple transfers of data from the participating entities all the way to the central model.

A typical FL-based process for TRUSTS (typically Vertical FL, or VFL) involves the following steps:

a. each participant downloads or receives a copy of the central model;
b. each participant updates the model by importing the data it holds on to its premises;
c. each participant transfers the model back to the central server; and
d. the central server performs aggregation on the various updates received from the participants.

Depending on the UC, the participants may also apply anonymisation techniques on some of all the data used to update the model locally. FL-based configurations contribute to complying with three key principles of the GDPR:

- First, privacy by design.
    - FL is conceived with the aim of preserving privacy as one of its core principles, and because of this it enables participating entities to comply with Article 25(1) GDPR;
- Second, purpose limitation.
    - Thanks to the decentralised architecture, the data included in the models shared by each participant are less likely to be combined at central level and processed for purposes that are incompatible with the initial purpose. This facilitates compliance with Article 5(1)(b) GDPR; and
- Third, data minimisation.
    - By making it unnecessary to engage in traditional transfers of personal data, FL in principle exempts entities from having to duplicate their data sets and applying extra safeguards to their original copies and/or destroying it. This facilitates compliance with Article 5(1)(c) GDPR.

4.1.2 TRUSTS approach: Federated Learning enhanced with cryptographic methods

In order to adapt to the needs of the three TRUSTS UCs, the TRUSTS consortium has developed a flexible solution leveraging the potential of FL enhanced with cryptographic methods such as HE and MPC. The model leverages two innovative approaches to privacy-preserving data analysis. The data protection implications of both approaches are assessed broadly in the following subsections.

4.1.2.1 Federated Learning

The TRUSTS platform allows for joint data collaboration using **Federated Learning (FL)** models, and more specifically Vertical Federated Learning (VFL).[11] The model adopted by TRUSTS allows various entities to individually download and apply the FL algorithm locally to their own data sets, thereby using each entity's data – including personal data – to train the algorithm locally. Subsequently, the entities send their locally trained models or inferences to the central server for aggregation. The entities can perform this process several times and share the trained models with each other to re-train the algorithm and arrive at an overall better performance (ensemble learning). The initial training data are not shared between entities.

Here an observation is made in regard to the key elements of the FL-based model that have a bearing on the compliance with legal and ethical requirements related to the protection of personal data.

Table 2: Legal and ethical considerations concerning the TRUSTS FL-based model

Aspect	Assessment
Data minimisation	By 'bringing' the algorithm all the way to the local data set, the FL models indirectly allows the participating entities to achieve results with less data. The data sets are processed locally and then never shared between entities. This means that personal data do not leave the premises of the participating entities, hence fewer or even no personal data is used (centrally and/or between entities) compared to a situation whereby the initial data sets were to be transferred to the central algorithm for analysis. This feature facilitates compliance with the data minimisation principle.
Purpose limitation	The federated nature of the TRUSTS FL model facilitates compliance with the purpose limitation principle because data is less likely to be combined. Because the data is not collected and processed centrally, it is less likely that the data is combined in different ways and potentially used for purposes other than the original ones, and possibly incompatible with them. The TRUSTS FL model facilitates compliance with the purpose limitation principle in another way too. By having the entities train the ML model locally, the number and extent of data processing operations can be drastically reduced vis-à-vis a situation whereby all participating entities needed to transfer their personal data sets to the central server for data analysis and training. This exempts the entities from having to, for instance, encrypt the data, transfer them to the server, and then transfer the results between each other, which

[11] VFL is a variant of FL modelling that is applicable to the cases where two or more data sets share the same sample ID space but differ in feature space.

	would constitute three distinct processing operations on top of the initial collection. The mechanics of the FL-based model therefore increases compliance with the purpose limitation principle.
Data security: Data leakage	While protecting the data better than in common ML-based models, it has been found that 'pure' FL-based models are not immune to leakages of training data. Cryptographic methods described in the subsection below are intended to reinforce the data security performance of the FL model in this department. Moreover, the literature has highlighted that, as far as horizontal FL is concerned, knowledge of the transmitted model gradients may be enough to arrive at the original training data.
Data security: Poisoning attacks	Also, one important data security aspect concerns poisoning attacks. FL models can be subject to data poisoning attacks – whereby the attacker disrupts the data provided locally – and to model poisoning attacks – whereby the attacker disrupts the entire model sent over to the central server.[12] The TRUSTS FL model does not provide for specific countermeasures in this department; however, the expectedly high participation of entities collaborating on the data via the FL model is likely to dilute the effect of isolated attacks on data or the models.
Data security: Membership inference attacks	Moreover, the TRUSTS FL model is likely to be more resistant to membership inference attacks than centralised adversarial ML models due to a) the higher amount of data required by default by a FL model compared to a traditional ML model; and b) the fact that a high number of participating entities is likely to increase the amount of data even further, making it unlikely for an attacker to replicate the model for a membership inference attack. It can therefore be argued that the TRUSTS FL model relies on its network effects to discourage the success of membership inference attacks.
Data security: Property inference attacks	Despite targeting specifically FL models as opposed to traditional models, property inference attacks are also unlikely to succeed against the TRUSTS FL model. This is because such attacks typically need a very small number of participating entities; very specific properties of the data sets used by each entity; and very specific training settings for each entity. However, the TRUSTS FL model is likely to be used by several participants over many repetitions; moreover, the data sets are likely to have (significant) overlaps across different entities and their

[12] See e.g.: Rossello, Díaz Morales, Muñoz-González, *Data protection by design in AI? The case of federated learning*, Computerrecht 2021/116 (2021).

	training settings are unlikely to be as different as to allow – taking into account also the number of participating entities – easy property inference attacks.

Subsections 5.2.2.1 and 5.3.2.1 provide a legal and ethical assessment of the envisaged use of the FL & MPC-based model developed by TRUSTS in the three UCs from a data protection and privacy point of view. It is to be noted that the assessment covers the real-life scenarios intended to be created after the completion of the project. The activities carried out to prepare and test the pilots under each UC are assessed in Chapter 7.

4.1.2.2 Cryptographic methods

Because of the security and potentially privacy-threatening challenges highlighted above, the literature has made research on combining FL models (including the transfer of locally trained models to the central server) with techniques intended to reduce the risk of leaking. Based on the major findings in the literature and on previous experience, the TRUSTS Consortium has decided to enhance FL by combining it with cryptographic methods. In particular, two methods have been found suited to the task at hand: MPC and HE.

One innovative technique to enhance the privacy-preserving potential of FL is **MPC**, which is a privacy-enhancing technique (PET) designed to address the issue. A party is confronted with when it needs to perform a joint data analysis with one or more other parties it does not (fully) trust.[13] While addressing trust issues, MPC can also contribute to enabling GDPR-compliant data sharing thanks to its key feature: the organisations using a MPC protocol (based on mathematically enabled cryptography) only get to have access to the output of the analysis and not to the whole set of data originally input by each organisation.[14] In this sense, MPC can represent a useful anonymisation technique and enable data controllers to comply with the principle of data minimisation,[15] insofar as it greatly reduces the amount of data that concurrent parties need to have access to during the data processing operation.

Typical MPC models, as the one used by the TRUSTS platform, are broken down into two main phases, the input phase and output phase:

- The **input phase**. In this phase, a PSI protocol – developed during the SafeDEED project – encrypts the data sets of each of the participating entities and then the selected data are fed into the MPC protocol for computation; and

[13] See e.g.: Helminger, Rechberger, *Multi-Party Computation in the GDPR*, In Privacy Symposium 2022 – Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT); Evans, Kolesnikov, Rosulek, *A Pragmatic Introduction to Secure Multi-Party Computation, Foundations and Trends*, in *Privacy and Security*: Vol. 2, No. 2-3, pp 70–246, 2018.

[14] Ibid., p. 3; Antignac, Le Métayer, *Privacy by Design: From Technologies to Architectures*, in: Preneel, Ikonomou (eds), *Privacy Technologies and Policy*, APF 2014, Lecture Notes in Computer Science, vol. 8450, Springer, Cham, pp. 398-414.

[15] Helminger, Rechberger, cited supra, note 17, p. 8-9; 11-13; Agencia Española de Protección de Datos (Spanish Data Protection Authority), *Encryption and privacy III: homomorphic encryption*, 2020, URL: https://www.aepd.es/en/prensa-y-comunicacion/blog/encryption-privacy-iii-homomorphic-encryption.

- The **output phase**. In this phase, the participating entities receive the result of the computation, i.e., the intersection of the data they were interested in accessing.

The two phases have different data protection implications. In the *input phase*, if the data at issue is personal, the data controller needs to make sure to comply with data protection obligations because the activity would constitute personal data processing despite the safeguards guaranteed by encryption. The *output phase* might result in personal data being disclosed and transferred to the various participating entities. Since the data protection implications of MPC depend on the specifics of each case, subsections 5.2.2.1 and 5.3.2.1 focus on the input and output phases related to UC2 and UC3, respectively, and draw the conclusions in terms of safeguarding the rights of the data subjects through MPC.

The TRUSTS Consortium has applied an enhanced version of the PSI MPC protocol developed in SafeDEED to the TRUSTS FL model. Here an observation is made for the common elements that contribute to bring the whole model in line with legal and ethical requirements.[16]

Table 3: Legal and ethical considerations concerning the TRUSTS MPC-based model

Aspect	Assessment
Privacy and data protection by design	The MPC technology is a PET that allows the TRUSTS platform to comply with Article 25(1) GDPR on data protection by design. The MPC is indeed amongst the technical and organisational measures referred to in that article, which are designed to include adequate safeguards to protect the rights of the data subjects.
Data minimisation	The MPC technology allows two or more participants to cooperate on data provided by each of them without sharing their whole data sets. The computation made possible by the MPC technology only discloses the intersection of data necessary to all parties. Therefore, it contributes to complying with the data minimisation principle, because it reduces substantially the amount of data that are disclosed and jointly processed by the participants.
Encryption	During the 'input' phase of the MPC process, i.e., when the participating entities feed the MPC protocol with their data, such data are encrypted, and the protocol runs on encrypted data. Because encrypted data are personal data as per the GDPR, this activity qualifies as processing of personal data. However, two elements make the processing more in line with the objective of preserving the rights of the data subjects: - First, the encryption applied by the MPC protocol provides more guarantees to the data subjects than if the processing were to take place with no encryption; and - Second, the computation of the protocol takes place on encrypted data that are therefore not visible to the other

[16] Deliverables D4.1 and D4.2 offer a detailed description of the technology supporting the FL and MPC model.

	participant(s) as long as the computation runs.

Another technique that can be combined with FL models to enhance privacy is HE. The principle of HE is that all participants to the data processing encrypt their own data sets prior to the processing, then send the encrypted data sets to a receiver which combines the mutually interesting functions of the data sets without any participants or receivers having access to the input data of other participants nor to the result of the analysis.

The TRUSTS Consortium has applied a multi-key HE scheme to a FL model. The multi-key scheme is based on the idea that the participating entities encrypt their data sets with reference to a common public key but keeping their private keys secret, send their encrypted data to the server that computes an encrypted sum of all data, and sends the sum back to the entities. The entities then partially decrypt the data from the sum and combine the partial decryptions together: this process provides the intersection of data the entities are interested in without disclosing the initial data.[17] The TRUSTS consortium has then combined this HE scheme with a FL model[18] and found that the privacy-enhancing effect of HE not only does not negatively affect the learning efficiency of the FL model, but actually improves it.

4.1.3 Data anonymisation

Data anonymisation techniques are techniques used to minimise the impact of data processing on the right to privacy and data protection of data subjects. The goal of anonymisation techniques is to render the personal data 'anonymous', i.e., no longer personal data and hence no longer subject to the purview of the GDPR. This leads to two well-known challenges in the literature:

- First, from a data utility point of view, the more effective the anonymisation techniques is in stripping away the data of its identifying attributes, the more likely the negative impact on the informational and/or statistical value of the data. Advanced techniques are increasingly leading to a better privacy-utility trade-off, but the challenge persists;
- Second, from a legal point of view, a distinction needs to be made between 'anonymised' and 'anonymous' data. Although the goal of anonymisation techniques is to make the data 'anonymous', the only guarantee one can have as a result of applying such techniques is that the data have been 'anonymised'. This is due to the particularly wide definition of 'personal data' in the GDPR,[19] which makes it possible that certain 'anonymised' data are still 'personal' in legal terms insofar as they can make an individual identifiable, "directly or indirectly".[20] It is in this

[17] See Deliverable D4.2 for a detailed description of this HE-based process.
[18] Apache SystemDS.
[19] Article 4(1) GDPR: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
[20] Ibid.

context that, based on the CJEU's judgment in *Breyer*,[21] the literature has developed a 'relative' approach to data anonymisation.[22]

Traditional anonymisation techniques relying on the removal of personal identifying information (PII) have been shown to be ineffective due to the de-anonymisation risks posed by high processing power and combination capabilities of current data analysis software. Therefore, the mere removal of PII does not guarantee anonymous data. Consequently, privacy models to anonymise data need to be more targeted and go beyond the mere removal of (some) PII.

UC2 relies on anonymisation techniques so as not to create a situation whereby the TRUSTS platform processes data that were not previously anonymised. In the case of UC2, Customer relationship management (CRM) and financial data sets are both candidates for the anonymisation techniques offered by TRUSTS. The TRUSTS platform provides an anonymisation approach based on techniques intending not only to anonymise the data, but also to lower the risk of re-identification (or de-anonymisation). The privacy model approach that TRUSTS relies upon is two-tiered:

- In a first step, the recommended models to be applied are generalisation techniques, i.e., k-anonimity and l-diversity (see also Deliverable D4.2);
- In a second step, TRUSTS provides also full suppression techniques to each data set. Due to its high impact on data utility, however, this model is however recommended only as a last resort measure, when the risk analysis shows that it is necessary to achieve a minimum degree of privacy in light of the context and potential impact of the data processing.

In the case of UC2, the ideal outcomes are CRM data containing services and location at the level of postal code; and financial data sets that contain aggregated location-based information.

In its approach the TRUSTS consortium paid attention to two key aspects: first, the need for a thorough risk analysis serving as input to the anonymisation process, in order to determine the required amount and nature of anonymisation; and second, the need to tailor the privacy models to the needs of very different data sets. Starting from the experience in the SafeDEED project, the TRUSTS consortium updated the privacy modules into an application that is envisaged to be uploaded to the TRUSTS platform. This is going to contribute to the platform's compliance with data protection rules by providing subscribers with a downloadable tool to anonymise data sets.

Because the use of the TRUSTS anonymisation application constitutes data processing within the meaning of Article 4(2) GDPR, it is necessary to assess the extent to which the application enables TRUSTS subscribers to comply with the legal requirements for processing personal data. In particular, it is necessary to define: the nature of the data set at hand; the nature of the processing; the definition of the entity(ies) qualifying as controller(s); the purpose and lawful ground for processing; and the safeguards that can be applied. This analysis is carried out for typical data sets under UC2 and UC3 (see Sections 5.2.2.1 and 5.3.2.1).

[21] Case C-582/14, *Patrick Breyer v Federal Republic of Germany*, judgment of 19 October 2016, ECLI:EU:C:2016:779.
[22] See Deliverable D6.2 for more details on the debate between the absolute vs. relative approach to data anonymisation.

4.2 Responsibilities of the TRUSTS platform as provider of online data-related services

This section is devoted to the requirements stemming from the legislation regulating online services. As shown in Deliverable D6.2, there are more than one legal framework applying to entities providing services online: the E-Commerce Directive, the P2B Regulation, and the Digital Content Directive (DCD). Each legal instrument targets a slightly different type of entity – i.e., 'provider of information society services' in the E-Commerce Directive,[23] 'online intermediation services' in the P2B Regulation,[24] 'digital service' in the Digital Content Directive[25] – and regulates different responsibilities of those entities.

Subsection 4.2.1 discusses whether the TRUSTS platform is likely to fall within each of the two definitions, identifies the requirements applying to the TRUSTS platform as a result of the answer to this question, and discusses to what extent the TRUSTS platform complies or is ready to comply with these requirements.

Moreover, subsection 4.2.2 provides an analysis of the relationship between the TRUSTS platform and the legislative proposals of the DSA, and the Data Governance Act (DGA) currently being discussed by the EU co-legislators. Depending on the potential applicability of either instrument to the TRUSTS platform, based on the available texts, identifies potential requirements and discuss the platform's readiness vis-à-vis them.

4.2.1 Current legislation on online services

An analysis is provided on the applicability of the E-Commerce Directive and the P2B Regulation in succession, and then the subsection groups together the requirements pertaining to this area of law. These two legal instruments govern certain aspects of online services from two different perspectives. The E-Commerce Directive aims to remove legal obstacles to the development of EU-wide online and digital services so that they could concretely benefit from the internal market integration; the P2B Regulation is intended to address the behaviour of online services and its impact on the fairness, transparency, and predictability of business relations, [26] and has a strong complementarity with competition law.[27]

[23] Article 2(b) of the E-Commerce Directive.
[24] Article 2(2) of the P2B Regulation.
[25] Article 2(2) of the Digital Content Directive.
[26] See e.g. V. Dan Roman, *Platform-to-Business Regulation—Where Does it Fit in the EU Antitrust Constellation?*, Journal of European Competition Law & Practice, 2021, Vol. 12, No. 1.
[27] European Commission, Staff Working Document Impact Assessment accompanying the document "Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services", SWD(2018) 138 final, p.3.

4.2.1.1 E-Commerce Directive

The **E-Commerce Directive** regulates providers of information society services, that are defined in Directive (EU) 2015/1535[28] as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[29]

The definition comprises of three distinct criteria. The service needs to be provided

a. electronically, including via the internet;
b. at the individual request of a recipient; and
c. against remuneration and not for free.

This is a very generic definition that encompasses a wide range of services. What is noteworthy is that, according to the definition of 'recipient', the service falling within the scope of the Directive can be services offered to natural and legal persons alike. Hence, the E-Commerce Directive does not limit its scope to services offered to consumers, and it applies also to business-to-business relationships. According to this generic definition, it can be argued that the services provided by TRUSTS are likely to fall within the scope of application of the E-Commerce Directive.

4.2.1.2 Platform-to-Business Regulation

The above analysis allows us to conclude that the TRUSTS platform can satisfy the first limb of the definition of online intermediation service pursuant to the **P2B Regulation**.[30] The second and third limbs are as follows: in order to be qualifying as online intermediation service, an information society service needs to:

- "allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded"; and
- "be provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers."

As mentioned in Deliverable D6.2, the analysis of whether the TRUSTS platform falls within this definition needs to be carried out *in concreto*, i.e., such a platform does not per se fall within or outside the definition, but it depends on what transactions are executed by means of the platform.

To start with, let us analyse the three Use Cases envisaged in the project to conclude whether in those scenarios the TRUSTS platform would qualify as online intermediation service. For a detailed description of the three Use Cases see Chapter 5 below and Deliverables D5.5, D5.7 and D5.9. Let us point out the main features of the relationship between actors within each Use Case for the purposes of the P2B Regulation.

[28] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.
[29] Ibidem, Article 1(b).
[30] Which recites as follows: "[online intermediation services need to] constitute information society services within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council".

Use Case 1

In UC1 the TRUSTS platform is expected to sit in between two categories of businesses: on the one hand, the provider of a service to carry out AML checks on data via advanced data analytics and correlation; on the other hand, entities that are required by law to carry out such checks and rely on the AML check service. The participation of those business users is regulated via contractual relationship expected to be based on smart contracts, which satisfies the third limb of the definition of 'online intermediation service'.

When checking the factual scenario envisaged under UC1 against the second limb of the definition, it can be noticed right away that the definition requires a missing element: the offering of goods or services to *consumers*. In UC1 the TRUSTS platform acts as an intermediation service but does so between two groups of business users – the provider of the AML service and the corporate customer required to carry out AML checks. First, direct transactions with consumers are not envisaged on the platform; this is not a decisive criterion, as the P2B Regulation is neutral as to *where the transactions are ultimately concluded*; however, it cannot be said that the TRUSTS platform enables business users to target consumers, because the activity facilitated by the platform is the execution of AML checks for regulatory purposes.

It must therefore be concluded that under UC1 as currently envisaged the TRUSTS platform does not qualify as online intermediation service within the meaning of Article 2 of the P2B Regulation.

Use Case 2

As in UC1, also in UC2 the TRUSTS platform is expected to be an intermediary between two groups of business users, also based on contractual relationship between each user and the platform. On the one hand, the provider of data correlation services and big data analytics for marketing, which is allowed by TRUSTS to provide its services via the platform and reach a number of customers; and on the other hand, other business users – such as telecommunication providers or banks – interested in:

a. exchanging data between themselves and
b. using the analytics and correlation service to gain insights on customer groups for targeted advertising activities.

As in UC1, also UC2 does not foresee the role of the TRUSTS platform as a direct intermediary between business users providing services and consumers, because the transactions envisaged would be concluded between two categories of business users (between the service provider and a bank; or between a bank and a telecommunication provider). The difference compared to UC1 is that the transactions facilitated on the TRUSTS platform do not end further down the line with business actors involved: the ultimate objective of such transactions is to enable business users to target consumers with tailored advertising and marketing. The question is to what extent the link with the role of consumers down the line of these transactions is sufficient to trigger the application of the definition at issue.

It can be argued that the most straightforward part of the definition is the following: "[…] with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded". UC2 appears to satisfy these requirements, because

a. the objective of the transactions enabled by the TRUSTS platform would indeed be to facilitate business users to offer services or goods to consumers at a later stage; and

b. the fact that these B2C transactions take place outside TRUSTS would not be an obstacle to the applying the definition.

The most problematic part of the definition is what comes before the above-mentioned sentence. Article 2(a) states that for the Regulation to apply the service needs to "allow business users to offer goods or services to consumers". This sentence could be the subject of a narrower or broader interpretation.

- In a narrower sense, it could be argued that the Regulation requires the platform to directly allow business users to present their offer to visiting consumers, and that therefore the platform needs to act as a space that consumer can visit, while the actual transaction may take place on another platform (e.g., a space managed by the business user; a payment service platform; etc.). In this sense, the TRUSTS platform would not meet this requirement under UC2 because services are only offered *by* business users *to* other business users.
- In a broader sense, however, it could also be argued that the term 'allow' is detached from the actual place where goods or services are offered to consumers, and that the service merely needs to increase the likelihood of business users to be able to subsequently reach out to consumers. In UC2, this would amount to equipping business users with knowledge and insights – thanks to the analytics and correlation service – to offer their services to consumers.

Here it is argued that the former interpretation is to be privileged for being in line with the spirit of the Regulation.

First, Recital 9 provides a hint at this when discussing the geographic scope of the Regulation: "[…] the business users or corporate website users should, *through the provision of those services, offer their goods or services to consumers* located in the Union at least for part of the transaction."[31] Leaving aside the jurisdictional issue, it appears that the Regulation considers that the offer of good and services by business users is to be made through the online intermediation service.

Second, Recital 10 introduces the definition of Article 2(a) and mentions "business-to-consumer relations […] intermediated online by providers operating multi-sided services", before leaving room to Recital 11 that mentions examples of services falling outside the scope of the Regulation. Amongst these are "pure business-to-business online intermediation services which are not offered to consumers". These sentences reinforce the interpretation according to which the definition of Article 2(a) requires a direct presence of consumers that are offered goods or services directly on the platform. As such, it can be argued that the TRUSTS platform does not qualify as such a service as far as UC2 is concerned.

Use Case 3

As in UC1 and UC2, also in UC3 the TRUSTS platform acts as an intermediary between two groups of business users based on contractual relationships. However, similarly to UC2, the services offered in the UC3 scenario are traded between two distinct categories of business users – i.e., provider of data analytics and AI-based customer assistance technologies, on one side, and financial institutions interested in using this service to better follow up on debtors on the other side. Once again, no services are directly offered to consumers through the platform which means that, according to the above analysis, the P2B Regulation is not applicable in this specific case.

TRUSTS platform beyond the Use Cases

[31] Recital 9 of the P2B Regulation, emphasis added.

The UC analysis just concluded that the TRUSTS platform is unlikely to qualify as an online intermediation service in the scenarios related to the three UCs. However, as mentioned in Deliverable D6.2, the analysis of whether the TRUSTS platform falls within this definition needs to be carried out *in concreto*, i.e., it depends on what transactions are executed by means of the platform. This means that the legal assessment with regard to the P2B Regulation should always be 'in active mode' during the lifecycle of the TRUSTS platform and cover possible extensions and additions to the services and business model of TRUSTS. For instance, the TRUSTS platform might in the future be used to enable SMEs with low levels of digitalisation to create data spaces and exchange data with restaurants and app providers to share services with users. In such a hypothetical case, the P2B Regulation would be likely to be applicable to the TRUSTS platform because the only remaining element of the definition under Article 2(a), i.e., the fact that the service needs to "allow business users to offer goods or services to consumers" would be satisfied.

4.2.1.3 Digital Content Directive

The analysis conducted above on the P2B Regulation allows us to make a transition to the Digital Content Directive. This is because, as was established that the P2B Regulation would not apply to the scenarios envisaged under the three use cases, nor would the **Digital Content Directive**, since it requires unequivocally a direct relationship between the service provider and the consumer. First, Article 1 on the purpose of the directive informs that the directive lays down "common rules on certain requirements concerning contracts between traders and consumers for the supply of digital content or digital services". With this, the directive already establishes that its scope is limited to contracts between traders and consumers. However, the definition of 'digital service' designates either:

a) a service that allows the consumer to create, process, store, or access data in digital form; or
b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service.[32]

The letter a) of this definition refers to consumers being one party to a contractual relationship involving some form of activity with data in digital form. The letter b) is a little more intricate. First, it focuses on a broader range of activities such as sharing of data, and envisages the case where such data are not uploaded or created by consumers, but by *other users*.

To recap, it can be said that a digital services within the meaning of Article 2(2) of the Digital Content Directive is found in the following circumstances:

- A service allowing consumers to create, process, store and access data in a digital form; or
- A service allowing some entities to share or interact with data in digital form that have been created or uploaded by consumers; or
- A service allowing some entities to share or interact with data in digital form that have been created or uploaded by other users of the service, not necessarily consumers.

The third bullet point above in theory envisages a situation whereby consumers are not involved, i.e., are neither partners to the contract for the provision of digital content, nor have created or uploaded the content that is the object of that contract.

[32] Article 2(2) of the Digital Content Directive.

Recital 18 states something crucial for the application of the Directive to the TRUSTS platform: "Platform providers could be considered to be traders under this Directive if they act for purposes relating to their own business and as the direct contractual partner of the consumer for the supply of digital content or a digital service". In other words, two requirements are to be met for the TRUSTS platform to fall within the directive's scope:

a. consumers need to be one party to the transaction; and
b. platforms need to present the key features of traders, i.e., not act as intermediaries between traders and consumers, but offer services themselves to consumers.

The table below sums up the analysis of the TRUSTS platform as it stands vis-à-vis the requirements of the P2B Regulation.

Table 4: Requirements related to the E-Commerce Directive and the P2B Regulation

Requirement / Question	**Explanation**
Has it been established whether the TRUSTS platform is likely to fall within the definition of 'information society service' as per Art. 2(a) of the E-Commerce Directive?	Yes. Given the wide and far-reaching definition of 'information society service' in the E-Commerce Directive, the services provided by the TRUSTS platform are likely to fall within the scope of application of that directive.
Has it been established whether the TRUSTS platform is likely to fall within the definition of 'online intermediation service' (Art. 2(2) P2B Regulation)	Yes. It can be argued that, based on the workflows envisaged under the three TRUSTS UCs, the services provided by the TRUSTS platform are unlikely to fall within the definition of 'online intermediation service'. However, this should be subject to ongoing analysis during the real-life deployment of the TRUSTS platform, potentially beyond the three UCs.

4.2.2 Legislative proposal on data governance

This subsection focuses on the novelty potentially brought about by the proposal for the DGA. It is worth stressing that the below analysis and the potential requirements identified are provided for illustrative purposes only, and to enable the TRUSTS platform to be as future-proof as possible with regard to the principles of upcoming legislation. The analysis and the individual requirements are likely to be subject to change as the legislative process for this proposal is still ongoing.

Amongst other things, the DGA proposal aims to further regulate the sharing of data in the digital marketplace with a view to increasing trust in entities acting as intermediaries between businesses.[33]

[33] DGA proposal, p. 1.

The DGA may actually be the first EU legal instruments to regulate the *sharing* of data in the EU, which is currently not at the core of any other legal instrument pertaining to data.

These paragraphs assess the potential impact of the DGA proposal on the TRUSTS platform, exploring the relationship of this proposal with the existing legal framework on data, and extract potential requirements worth taking into account.

The analysis focuses on Chapter III of the DGA proposal, which aims to regulate *data sharing services* by introducing a set of legal obligations. Data sharing is defined as an activity in Article 2 of the proposal as "the provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, directly or through an intermediary". It basically covers any type of situation whereby data are shared in whatever form outside the scope of legal obligations for a multitude of possible uses. Building on this definition, Article 9 of the DGA proposal distinguishes three types of data sharing services, i.e.:

- *Intermediation services between business data holders and data users*: such services are defined as services enabling the exchange of data between these categories of actors, including services that make available technical or other means for such exchanges;[34]
- *Intermediation services between data subjects and data users*, along the above lines;[35]
- Data cooperatives, i.e., services that can be entrusted by SMEs or micro-enterprises with negotiating terms and conditions for data processing and representing their interests on data processing purposes.[36]

Now it is time to address the question as to whether the TRUSTS platform may fall within any of the above definitions.

Intermediation services between business data holders and data users. Article 9(1)(a) of the DGA proposal provides examples of business realities that could satisfy the requirements of the definition: the article states that such services "may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users". Recital 22 of the proposal narrows down the definition, and excludes from the concept of intermediation services those services that:

- Amount to cloud services; or
- Enable the exchange of data between closed groups of data holders and users; or
- Obtain data from data holders *without establishing a direct relationship between data holders and data users*.

As the TRUSTS platform is not a cloud service provider and is virtually open to an indefinite set of data holders and users, the most important criterion seems to be the third one. The DGA proposal intends to exclude from its scope those providers that, whilst allowing users from two or more ends to use their services, only transact with the provider and do not enter transactions with the other user group.

[34] Article 9(1)(a) DGA proposal.
[35] Ibid., Article 9(1)(b).
[36] Ibid., Article 9(1)(c).

Whether or not the TRUSTS platform satisfies this criterion will depend on a case-by-case basis. However, from the use cases envisaged in the project it can already be argued that the TRUSTS platform would meet the criterion at least in some circumstances. This is because the users participating in the three UCs enter into (mostly smart contract-based) transactions between each other on top of transacting with the intermediary itself – i.e., the TRUSTS platform.

As to the data exchanges per se, the TRUSTS platform is designed to enable multiple types of activities related to the handling and sharing of data. Here as well it will be necessary to establish on a case-by-case basis whether each specific data-related activity can be considered a data exchange and whether the TRUSTS platform can be considered as enabling the parties to carry it out.

Below a list of possible future requirements stemming from the DGA and a preliminary approach to tackling them is provided.

Table 5: Potential requirements related to the DGA

Potential requirement / Question	**Explanation**
The TRUSTS platform needs to make the necessary arrangements to be able to send a notification as per Art. 10(1) DGA Proposal	Should the DGA Proposal enter into force as a legal act with the current text of Article 10(1), the TRUSTS platform will need to send a notification to be able to provide data intermediation services. No technical arrangements are assumed to be required to comply with this obligation. Upon this report's recommendation and its legal team's guidance, the legal entity managing the TRUSTS platform would send a notification as per Article 10(1).
The TRUSTS platform needs to comply with the obligation to not use the data for which to provide services for other purposes than to put them at the disposal of data users (Art. 11(1) DGA Proposal)	The TRUSTS platform will implement a policy requiring participating end-users to only use the data and metadata they access to for the purposes of the services provided within the TRUSTS framework. A draft subscription agreement has already been drafted detailing these requirements. Moreover, the TRUSTS Dataspace Connector (DSC) will ensure that operations on data will occur in a secure environment, by providing access control to local data assets and regulating the access rights to communicate and modify data assets.
The TRUSTS platform needs to comply with the obligation to only use metadata collected from the provision of the data sharing service may for the development of that service (Art. 11(2) DGA Proposal)	The TRUSTS policy mentioned in the above requirement applies also here. Moreover, the TRUSTS Dataspace Connector will ensure, amongst other things, secured communication of metadata between users and reinforce the technical architecture around the use of metadata.

The procedure for access to the TRUSTS platform services needs to be fair, transparent, and non-discriminatory for both data holders and data users, including as regards prices (Art. 11(3) DGA Proposal)	The smart contract system on which the TRUSTS platform relies will enable the platform to offer a high level of transparency and fairness to all end-users. Upon setting up the price for a given service and describing the service in detail in the associated smart contract, the execution of the transaction via smart contracts will ensure automatic and unbiased transfer of funds in exchange for services. For more details on how smart contracts are set to be used in TRUSTS, see Deliverable D3.3 "Smart Contracts".
The TRUSTS platform needs to put in place the necessary tools to enable exchanges of data in the same format in which data are received, and to enable interoperability when possible (Art. 11(4) DGA Proposal)	The architecture of the TRUSTS platform is already designed to accommodate these requirements. First, in terms of data formats, the TRUSTS platform requires data and metadata to be in a format compliant with the TRUSTS broker format. This means that, when possible, the format of the data and metadata received from end-users will be kept in the TRUSTS platform; in other cases, the format will be transformed in a compliant format without affecting the format of the initial data or metadata. This task will be accomplished by the Broker Format Mapper (see Deliverable D3.4 "Data Marketplaces with Interoperability Solutions I"). Second, the TRUSTS architecture puts interoperability at its core as it reuses components from existing data marketplaces platforms (IDS and DMA). These components are those that enable the interactions between the TRUSTS owner and the various actors (data providers and data buyers). TRUSTS envisages an interoperability component capable of providing the functionalities necessary for both providers and buyers (for more details, see Deliverable D3.4 "Data Marketplaces with Interoperability Solutions I".
The TRUSTS platform needs to put in place procedures to prevent fraudulent or abusive practices (Art. 11(5) DGA Proposal)	The trustworthy architecture of TRUSTS and the smart contracts-based system of transactions are assumed to be sufficient, at this stage, to prevent illegal behaviour concerning data exchanges. If the DGA Proposal enters into force with the current text of Article 11(5), the recommendation will be to study specific measures to prevent the practices referred to in that article.
The TRUSTS platform needs to put in place adequate measures to prevent transfer or access to non-personal data that is unlawful under EU law (Art. 11(7) DGA	The TRUSTS data processing architecture grounded on its FL model and the anonymisation services is set in such a way that the personal data input by participating organisations are not stored on the TRUSTS platform. TRUSTS components – the IDS Trusted Connector, the IDS Broker, the IDS Connector

Proposal)	Framework and the DMA Metadata mapper – are designed so as to allow transfers of data within the limits of the envisaged transactions. These safeguards also guarantee against any transfer of such data – whether in raw form or after being processed while still allowing for the identification of individuals – outside the platform and/or to unauthorised third parties that would qualify as unlawful under EU law.
The TRUSTS platform needs to put in place adequate measures to ensure a high level of security for the storage and transmission of non-personal data (Art. 11(8) DGA Proposal)	The TRUSTS FL model and components mentioned above also guarantee a level of storage security in line with the state of the art with regard to the non-personal data (both industrial and public data, and anonymised data) stored in the central FL model.

4.3 Competition law and commercial relationships between undertakings

Competition law is one fundamental cornerstone of EU economic law. For a few years by now data has been studied as a commodity capable of affecting the nature of competition on the market. More and more market realities depend on the value and use of data: different degrees of concentration of, and access to, data amongst companies can determine the extent to which a market is sufficiently open, and competition can thrive. For this reason, data-driven markets are being increasingly studied by academics and scrutinised by competition authorities in the EU to ensure the application of Articles 101 and 102 TFEU and of the relevant secondary legislation.

Article 101 TFEU prohibits anti-competitive agreements. Data-sharing agreements, such as of the kind envisaged in the TRUSTS experience, might be anti-competitive in either of the following cases:

- If they have the effect of denying or reducing access to data to competitors, for instance through less favourable terms and conditions that prevent competitors from using the data (exclusionary effect); or
- If they have the effect of imposing excessive prices for the use of data or unfair commercial conditions (exploitative effect); or
- If they have the effect of diminishing the degree of uncertainty and unpredictability of the market by allowing two or more competitors to exchange commercial information and therefore make it easier to collude at the expense of the other competitors (collusive effect).

As remarked in Deliverable D6.2,[37] the nature and extent of the data exchanged, the degree of concentration in the market and the market power of the companies involved are all factors that determine the extent to which a given agreement is likely to infringe EU competition law rules. In particular, the presence of personal data is important because, the more individualised and precise the

[37] See Deliverable D6.2, Chapter 7.

data exchanged are, the more likely – all things equal – the data exchange is to raise competitive concerns. In this vein, therefore, since the personal nature of data makes them more individualised, exchange of personal data needs to be carried out with great care with respect not only of personal data protection law, but also competition law. Data exchange agreements carried out in an environment managed by an intermediary, including an online intermediary, may also trigger its specific competition law responsibility. This is relevant to TRUSTS insofar as the TRUSTS platform brings together several participating organisations that will engage in data exchange agreements *specifically facilitated* by the platform.

These aspects are analysed in greater detail in Sections 5.2 and 5.3 below with reference to UC2 and UC3.

Another aspect of economic law deserves attention. Deliverable D6.2[38] presented national law provisions that – absent a comprehensive binding legal framework at EU level – are in principle applicable to the commercial relationships between undertakings, and particularly between an undertaking that possesses a large market power vis-à-vis smaller undertakings. Such provisions aim to prevent situations of legal and economic dependencies for the latter.[39]

In the context of TRUSTS this legislation is relevant to the commercial relationship between TRUSTS as a legal entity and the entities willing to participate in the data marketplace by way of selling and/or purchasing databases, applications, or services. It is important to notice that the undertakings expected to join the TRUSTS platform in the future are likely to present a very wide spectrum in terms of size and relative market power vis-à-vis the future TRUSTS legal entity. Therefore, the analysis as to whether the contractual relationships established between TRUSTS and the participating undertakings is problematic to the extent that it may trigger a violation of relevant national rules, will depend on a case-by-case assessment.

At this stage, however, it can be argued that the risk of creating legal and/or economic imbalances between TRUSTS and other undertakings is in theory very low. This stems from the analysis of the Draft TRUSTS Registration Agreement that is planned to be shared with future potential participants and that contains the set of rights and obligations of TRUSTS and the subscribing undertaking. The Draft Registration Agreement does not contain any clause resembling the terms found to be unfair and illegal by recent French[40] and Belgian law;[41] in particular, it does not contain any clause related to abrupt suspension or termination of the contractual relationship; economic advantages to be accrued by TRUSTS under certain conditions; unilateral modification of the contractual terms; etc.

Despite the ex-ante compliance of the Draft Registration Agreement with legal and ethical principles governing commercial relationship, compliance will need to be ensured continuously during the life cycle

[38] See Deliverable D6.2, Chapter 6.

[39] The deliverable looked specifically at the law of Germany, France, and Belgium.

[40] French Commercial Code, Articles L420-2, al. 2; L442-3, 442-1, II, L442-1, I, and L442-4,I. See also the landmark 2019 judgment of the Paris Commercial Court : Tribunal de commerce de Paris, 1ère ch., jugement du 2 septembre 2019, *M. Le Ministre de l'Economie et des Finances / Amazon*.

[41] *Loi du 4 Avril 2019 modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises*; Law of 4 April 2019, Art. 2, modifying the Code of Economic Law, Art. I.6; Law of 4 April 2019, Art. 4, creating a new Art. IV.2/1. in the Code of Economic Law.

of TRUSTS. The nature of draft contractual terms does not per se guarantee against abusive practices being committed in the future, such as, for instance, the refusal to allow participation in the data marketplace to a certain company, which, under certain circumstances, may qualify as 'refusal to deal' and be sanctioned.[42]

[42] See for instance Belgian Law, Law of 4 April 2019, Art. 4, creating a new Art. IV.2/1. in the Code of Economic Law.

5 Use Case Analysis

This section provides the legal and ethical assessment of the three UCs as they are envisaged to be deployed in real life, i.e., after project completion. The assessment of the pilots for each UC is provided separately in Chapter 7 because the pilots were conducted under different conditions than those characterising the intended real-life UCs.

5.1 Use Case 1: 'Smart big data sharing and analytics for Anti-Money Laundering compliance'

This section provides the legal and ethical assessment of the use of the UC1-based tools in real life, i.e., their intended use after the project completion. The table below summarises the main differences between the real-life scenario the workflow relied upon in the pilot.

Table 6: Differences between the pilot and real-life scenarios of UC1

Item	Pilot	Real-life
Data subjected to AI-based processing for AML purposes	Non-personal (anonymised) data	Personal data about bank customers and transactions
Organisational workflow	One entity (eBOS) responsible for anonymising the data and conducting the AI-based profiling	Different entities providing the personal data (financial institutions) and ingesting the data into the AI-enabled tool (eBOS)
Role of the TRUSTS platform	Hosting the application/service enabling UC1 – the testing organisations download the WiseBOS application on their premises	The TRUSTS platform provides the AML applications and service to the TRUSTS subscribers/interested parties who will still download applications on premises

As described in the table, the real-life service provided by TRUSTS is going to be the result of a different approach to data management and of different organisational arrangements compared to the pilot for UC1.

First, compared to the pilot, where anonymised data were the source material for the AML analysis, in the real-life scenario the WiseBOS application will use personal data of bank customers. This approach is likely to increase the utility and effectiveness of the processing but carries higher data protection risks and implications compared to the pilot approach.

Second, whereas in the pilot eBOS was the only entity involved in the workflow, the provision of AML analysis in real life is subject to source data being supplied by financial institutions and then injected into

the AI-enabled tools. In principle, this configuration complexifies the data protection assessment because it would add one data processing operation – i.e., the transfer of the data set between the supplying entities to eBOS.

Third, whereas the pilot did not rely on the TRUSTS platform, in the real-life scenario the platform is going to be the entry point for subscribers to use the AML services.

The Consortium has always been conscious of the data protection challenges entailed by such a complex architecture, complemented using AI technologies which call for even higher data protection safeguards. Therefore the Consortium has opted for a privacy-enhancing approach to the real-life provision of AML services that relies on **deep learning algorithms on distributed frameworks**.[43] This approach uses ML techniques that follow a privacy-by-design mentality. It allows multiple entities to carry out joint ML-based operations whereby, instead of transferring the source data between entities to make it closer to the algorithm – which would increase data protection risks and hence the need for safeguards – the algorithm used for the analysis is 'moved' closer to the data itself.

5.1.1 Description of the use case

UC1 aims to provide an AI-based functionality to process the data of customers of banks and other financial institutions for AML purposes. The idea behind is that the AI model deployed can analyse customer data faster and more efficiently than other IT tools or than humans, thus leading to a better detection rate of ML.

The initial setup of UC1 involved four key partners: eBOS, InBestMe, NOVA and TRUSTS. Each partner had a specific role in the data workflow:

- The role of eBOS was to provide the technology for ML detection, i.e., the actual AML service ('WiseBOS') through the TRUSTS platform. The WiseBOS tool would ingest Know-Your-Customer (KYC) data, transaction data and other customer data, cross-checks them against the lists mentioned above, and apply its parameters to give indications in the various phases of the assessment (i.e., screening, risk assessment, transaction monitoring).
- The role of InBestMe and NOVA was to provide the source data for the AML checks. Within the UC1 workflow, InBestMe could then use the WiseBOS service on the TRUSTS platform by logging in and entering a smart contract-based transaction.
- The role of TRUSTS was to host the services and applications enabling UC1.

The initial setup was amended during the project. As a result, instead of InBestMe and NOVA providing input data for the trial, the data sets were provided and processed by eBOS. Section 6.1 below takes this change into account in the legal and ethical assessment.

The workflow of UC1 is broken down into three main stages: AML screening; risk assessment; and transaction monitoring:

- *AML Screening*: this stage, performed via a service,[44] aims to identify the risk profile of the customer by screening their data against the database containing data about adverse media,

[43] Deliverable D4.2 includes a detailed description of the technology underpinning this approach.
[44] That is, by a functionality embedded in the TRUSTS platform and executed centrally.

sanctions and watchlists, PEPs and other focused datasets around risk themes, the Panama Papers, and marijuana-related businesses;
- *AML Risk assessment*: this stage, performed via an application,[45] aims to assign a risk level to the customer ('low'; 'medium'; or 'high') based on the analysis of the data concerning them; and
- *AML Transaction monitoring*: this stage aims to analyse the transactions of the customer based on the input data and to identify suspicious or anomalous transactions.

The results of UC1 are the data analysis reports performed by WiseBOS on the test data. In a real-world deployment perspective, the results of the analysis performed by WiseBOS can then be securely brokered to third parties that are bound by law to perform AML checks and that have an interest in consulting the results of the WiseBOS analysis.

5.1.2 Legal and ethical assessment

The data processing operations relevant to UC1 are envisaged to happen with personal data attributable to data subjects. With this in mind, the assessment is focused on the use of the TRUSTS FL-based modelling for data transfers and collaboration. The model applies across the three phases mentioned above, i.e., AML Screening; AML Risk assessment; and AML Transaction Monitoring. It is worth reminding that the data sets supposed to be used in UC1 are likely to contain personal data of bank customers.

The functioning of the FL-based modelling is assessed based on the following steps:

a. execution of the AML services/applications and local AI/ML training; and
b. data aggregation.

5.1.2.1 Step 1: Execution of AI/ML services and local AI/ML training

Description

This step occurs after the end-users (the organisation that have subscribed to the TRUSTS platform) have downloaded the AML applications/service provided by the platform.

The first service that is used is the AML Screening Service. To do so, the end-user, upon paying a subscription to use the package, downloads the AML Screening Service and can use it on a browser (not on its local premises as it is not an application). This means that the only data input the service needs from the end-user – i.e., the name of the entity/organisation that needs to be screened – is going to be provided to the service operating on a browser, and not shared with the TRUSTS platform itself.

Upon executing the AML Screening service, the data sets are again at the end-users' disposal and would typically go through the risk assessment process. The AML risk assessment (AML RiSC) application is downloaded locally and applies the pre-set parameters, the KYC input provided by the end-users, as well as the screening report in order to assign a risk score to the customers included in the data set. The RiSC application is based on AI/ML technology and the local execution also constitutes the local training of the AI/ML model supporting the AML RiSC application. The end-user can train the model by:

a) Using the internal data of the application;

[45] That is, by a functionality that can be downloaded from the TRUSTS platform by the user (e.g., a bank).

b) Using external data provided by another organisation through the TRUSTS platform; or
c) Using an external model provided by another organisation through the TRUSTS platform to replace the end-user's model.

After running the AML RiSC application, the data set typically goes through the AML Transaction Monitoring (AML TRM) process. For this, the end-user executes locally the AML TRM application previously downloaded on its premises. Relying on AI/ML, the application analyses the customer transactions, makes an evaluation of them, and spots those transactions that are potentially suspicious. As with the AML RiSC application, end-users can update and train their model with their own data as well as using external data and/or external models.

AssessmentBecause the AML Screening Service is set to run on a local browser and in any case there is no personal data to be input, this service does not give rise to any data protection or ethical implications.

As per the AML RiSC application and the AML TRM application, the execution occurred entirely locally on the end-user's premises. This is consistent with the description of the TRUSTS ensemble modelling provided in Section 4.1.2. This solution avoids all data exchanges – and hence, further processing – between organisations, that would result in higher risk of harm for the data subjects. In this UC1 scenario, each end-user runs its own data sets through the TRUSTS applications, and the processing operated by the AI/ML engine of the applications does not involve other actors than the individual end-user.

In terms of data protection responsibilities, this means that, if the end-user uses internal data of the applications, each end-user is the sole **data controller** responsible for the data processing. In this scenario, each end-user is indeed responsible for taking the decision as to the purpose of the data processing (performance of data analytics for better AML compliance) and as to its means. There is no instance of joint controllership because a) the TRUSTS platform administrator is not involved in the processing; and b) the processing of each individual end-user is shielded from the processing of other end-users, since each data set is not processed by more than the end-user having the rights to it.

How does the situation change if the end-user makes use of external data and/or external models provided through the TRUSTS platform?

In case of *external data*, the setup of data protection responsibilities is likely to remain unaltered because the data available through the TRUSTS platform, and that the end-user could rely on to enrich its model, are supposed to be non-personal data. This is because the TRUSTS platform is designed not to store any personal data originally belonging to the data sets of the participating organisations.

In case of *external models*, the data protection responsibilities are also likely to remain unaltered because the TRUSTS platform will only store ensemble models that have been built through the FL-based modelling combined with the cryptographic methods to preserve privacy. The TRUSTS platform will not store ensemble models that can lead to the identification of natural persons. Therefore, the use of external models by the end-users will not entail a new or different processing of personal data.

In terms of **legitimacy of data processing**, the processing entailed using the three UC1 assets mentioned above needs to be grounded in Article 6 GDPR. In theory, any of the grounds provided for in Articles 6(c), (e) and (f) – i.e., legal obligation; public interest task; and legitimate interests – could be relied upon by the end-users as controllers. Each of the three grounds entails a slightly different set

of standards and requirements that the controller needs to observe. Moreover, the presence of the AI/ML technology in the processing – via the FL-based modelling – needs to be accounted for with specific safeguards given its potential negative impact on the protection of personal data. The safeguards and measures already assessed in Section 4.1 are to be sufficient to this effect.

However, the processing of personal data by private organisations through AI/ML technology for AML purposes is a source of an ongoing legal debate and has not yet received sufficiently firm answers by the EU legislator nor the Court of Justice. Section 6.1 will delve into the main legal intricacies and issues left open by data processing in this context and will draw conclusions for the functioning of the TRUSTS platform.

5.1.2.2 Step 2: Data aggregation

Description

After all the three assets have run on the data set, the data set will typically be in either scenario:

a) it will have been analysed by the AI/ML technology embedded in the AML applications/services, and these applications/services will have been trained by the data set; or
b) on top of this, if the end-user chose to rely on external models, the AI/ML technology will have been trained more thoroughly thanks to these models.

In the latter case, the end-user ends up with an ensemble model that results from the synergies between the data analytics on its data sets and the analytics run on previous data sets that have refined and streamlined the model. The end-user's activity is another 'brick' in the training of the AML AI/ML-based model.

Assessment

The model trained by the end-user is therefore added to the ensemble model. This activity relies on the aggregation functionality of the TRUSTS FL-based model coupled with HE and MPC. Whenever a new end-user enriches the ensemble model, it uses its private key to encrypt its part of the data set that feeds the ensemble model; at the same time, that end-user can rely on the fact that all end-users that have contributed to the ensemble model in the past have all used their own private keys in accordance with the corresponding aggregated public key. This means that when our end-user uses the external model to augment the performance of its own model, it does not have access to the personal data originally used in the individual models by past end-users.

In terms of **legitimacy of the data processing** and legal base for processing, the considerations made above with regard to Step 1 apply also here. The reader is remanded to Chapter 6 for a more comprehensive discussion on the legitimacy of data processing in the AML context.

5.2 Use Case 2: The agile marketing through data correlation

This section provides the legal and ethical assessment of the use of the UC2-based tools in real life, i.e., their intended use after the project completion.

5.2.1 Description of the use case

The purpose of UC 2 is to verify that TRUSTS services can be used to advance current marketing activities towards enabling collaboration between different enterprises without processing personal data. The expected results are the following:

- From the business perspective, UC2 is expected to show that it is possible to exchange such data between the stakeholders through the data marketplace in a way that is meaningful for marketing purposes; and
- From the research perspective, UC2 is expected to demonstrate the role of TRUSTS platform as centre for the data exchange therein.

The data needed for UC2 is not open-source and it is provided by financial institutions and electronic communications service operators. However, such data was made subject to anonymisation techniques by the organisations holding the data before being processed for the purposes of TRUSTS. The section below analyses the anonymisation process applied. Because all data used for UC2 was anonymised, UC2 involved no direct marketing activities to be performed by the TRUSTS partners.

UC2 involves TRUSTS, FORTH, NOVA, KNOW and PB as main players:

- TRUSTS data marketplace operators (WP3 & WP4) which provide all the necessary functionalities;
- Application providers, i.e., KNOW provides the PSI and RSA provides the de-anonymisation risk analysis;
- NOVA provides anonymised CRM and application consumer data; FORTH provides big-data analytics and customer economic behaviour insights; PB provides financial data. All these data is anonymised by NOVA and FORTH on their premises via the functionalities provided by KNOW before being transferred to the TRUSTS platform.

5.2.2 Legal and ethical assessment

Since the data transfers relevant to UC2 are envisaged to happen with anonymised data, the assessment focuses on two main activities: the use of the TRUSTS anonymisation application by the data holders; and the use of the TRUSTS FL-based modelling for data transfers and collaboration.

5.2.2.1 Step 1: TRUSTS anonymisation in UC2

As mentioned in Section 4.1.3, the anonymisation of personal data qualifies as data processing within the meaning of Article 4(2) GDPR. The entities qualifying as data controllers are therefore required to comply with the relevant legal and ethical requirements.

The table below contains the assessment for the envisaged data anonymisation operations under UC2. The assessment covers one of the two business opportunities offered by the TRUSTS platform, i.e., the

use of ***applications*** on the participating entity's premise. This contrasts with the *services* provided by TRUSTS and used on the platform itself.

It is to be noted that this assessment is forward-looking, i.e., concerns activities envisaged to be carried out upon project completion based on the components and architecture of the TRUSTS platform.

Table 7: Anonymisation under UC2 – Requirements for the processing of personal data

Task	Assessment
Qualify the data set	The data sets likely to be at hand under this UC2 are of two types: First, **customer relationship management (CRM)** data held by telecommunication companies. Depending on the company, CRM data bases may include: - The personal details of the customers, such as: name, email address, telephone number, URLs, telecommunication (e.g., Skype) address, date of birth, age, title, etc.; - The purchase history of the customers, which would link the customer's identity with their purchase habits, type of telecommunication service, and monthly tarifs; and - Data concerning interactions between the customer service and the customers that may lead to identifying the latter; and - Geocode or postal data. Second, **financial data** held by organisations active in the financial and banking domain. Depending on the company, financial data may include: - The personal details of the customers, such as: name, email address, telephone number, Fax number, device identifier and serial number, license plate number, social security number, date of birth, age, title, etc. - Number of customers per requested areas identified by postal code; - Amount of deposit of customers, which are linked to the customer's identity; - Number of customers per transaction type; - Number of loans per transaction type; and - Credit card usage data per group of customers. Each of the two types of data set may therefore contain several entries that qualify as personal data, either because they directly identify the data subject or because they may contribute indirectly to their identification. Whereas insights into the data subjects' lives can be inferred already from within each data set separately, the cross-analysis of the two types of data sets is likely to lead to a very significant impact on data protection.
Define the controller and the processor	With regard to the anonymisation of the data sets, each organisation holding only one of the data sets would separately decide to anonymise its data set. Hence, each organisation would qualify as sole data controller, for the

	purposes of its data set, within the meaning of Article 4(7) GDPR. In practical terms, this would be the case where the telecommunication company holding the CRM data and/or the bank holding the financial data set would decide to anonymise their data sets in order to make it available to other organisations through the TRUSTS platform. Each organisation would qualify as sole controller because: 1. Each organisation would qualify as a *legal person* within the meaning of Article 4(7) GDPR; 2. Each organisation would *determine* decisive elements about the data processing operation. If the organisation wanted to anonymise its data set in order to make it available through TRUSTS in a second stage, this would obviously be the case; but the same would go if the organisation decided to anonymise the data to honour the terms of a contract with another organisation (e.g., a bank having a contract with a telecom operator). In this case it would still be each data holder that exerts the decisive influence and control over its data and would determine the key elements of the processing; 3. Each organisation would determine both the *purpose and means* of the processing. To take the example of the telecom company, it is this company that determines the specific purpose for the anonymisation of its data set taking into account the context of the processing and its goal; similarly, by downloading the anonymisation application from the TRUSTS platform, it is also the same organisation that determine the means for the processing. Because the processing does not take place on the TRUSTS platform itself – the application acts on the controller's premises – it is arguable that the entity managing the TRUSTS platform would not qualify as data processor. Moreover, the two or more entities that end up using each other's anonymised data base would not qualify as joint controllers;[46] 4. Each organisation would determine the purpose and means of the processing of personal data: several entries of typical CRM and financial databases qualify as personal, as noted above; For the above reasons, it can be argued that each of the two entities typically likely to participate in a data processing under UC2 would qualify as separate controllers.
Specify the purpose of the processing and identify a suitable	The purpose of the data processing operation would be to anonymise the data set to provide and consume data analysis services intended to provide business value to the participating entities. These purposes are likely to be

[46] Which would be likely to be the case if the two entities fed a TRUSTS-operated database with the data each of them held, and these data were only subsequently anonymised. This situation would be likely to give rise to a joint controllership for both the personal data exchange and the anonymisation.

lawful ground for the processing	different from the purposes for which the data held by each participating entity were initially collected. Therefore, the entities are unlikely to be able to claim that the anonymisation does not need a new legal base because it is compatible with the initial purpose. This means that a new legal base / lawful ground needs to be found. Because each entity would independently decide to anonymise their data set to make it available to other entities, the lawful ground likely to be relied upon would be Article 6(1)(f), i.e., a **legitimate interest** pursued by the controller. In this case, the legitimate interest would be the provision of services to other companies via the TRUSTS platform. The entity relying on this ground needs to conduct a balancing test to make sure that its legitimate interest does not run counter the interests of the data subject. The fact that this balancing needs to be made against "the interests or fundamental rights and freedoms of the data subject which require protection of personal data" makes it more likely that the legitimate interest ground is a suitable once for a data processing intended to anonymise the data, i.e., to better protect the identity of the data subjects. Alternatively, the entities may rely on Article 6(1)(a) and seek the **consent** of all data subjects. This would provide stronger data protection guarantees, but it would also likely entail a very heavy and time-consuming process.
Qualify the data processing operation	The data processing operation at issue would be the anonymisation of personal data (CRM and financial data).
Ensure data minimisation	Before conducting the data processing operation, each entity would need to carefully assess the nature of the data set and conclude that its size is adequate and does not go beyond what was necessary to extract value out of the contractual relationship with the other entity.
Ensure storage limitation	Each entity needs to make sure to keep their own data set on their premises during the whole anonymisation process and to not share the data sets with outside organisations, not even within the TRUSTS consortium in order to have stronger storage limitation guarantees. Each entity would be advised not to copy or store the data sets in multiple location either before or after the data processing operation.

The table below assesses the requirements related to **transparency and accountability**.

Table 8: Anonymisation under UC2 – Requirements related to transparency and accountability

Task	Assessment
Keep a record of data processing activities	All the organisations involved in the initial data processing (anonymisation) shall keep due record of their own processing, in particular detailing the rationale and the legal ground (Article 6 GDPR) behind the decision to process personal data.

	Since the processing occurs outside the reach of the TRUSTS platform, this responsibility sits within each end-user.
Comply with the accountability principle	All the organisations involved shall also keep documentation proving their compliance with data protection law, i.e., the rationale and legal ground (Article 6 GDPR) behind the processing, and, if necessary, any agreement between them concerning the sharing of personal data prior to the anonymisation.
Ensure respect for data subjects' rights	All the organisations involved shall also make sure to comply with the requirements set out in Article 13 and/or 14, depending on whether the personal data processed were or were not obtained from the data subjects; and in Article 15 regarding requests of access to their data by the data subjects.

5.2.2.2 Step 2: TRUSTS Federated Learning in UC2

This subsection assesses the legal and ethical implications of using the TRUSTS FL-based modelling in UC2.

Under UC2, the typical end-user, after anonymising the data as described in Step 1, will train the local model it has been provided with and subsequently update the central model.

After the local model downloaded by the end-user has been updated via the user's data set, the combination of PSI-based MPC and Homomorphic Encryption ensures that the new local model is transferred safely to the central model on the TRUSTS platform minimising to a great extent the risk of information about the data subjects being leaked during the transfer.

The safeguards provided by the FL-based model should also be evaluated in synergy with the de-anonymisation / re-identification risk assessment provided by the TRUSTS anonymisation application enables the end-user to reduce the re-identification risks upstream by selecting the most suitable degree and method of anonymisation. This will increase awareness and is likely to reduce the level of risk of data leaking to be dealt with during the transfer to the central model.

5.3 Use Case 3: The data acquisition to improve customer support services

This section provides the legal and ethical assessment of the use of the UC3-based tools in real life, i.e., their intended use after the project completion.

5.3.1 Description of the use case

UC3 aims to enable data-based debt management automation. The idea of UC3 is to create an out-of-the-box analytics solution to develop a chatbot that can act as an automated assistant for customers needing debt management advice. Automation is powered by enhanced analytics of big data, AI, and the

integration of bots, which make it possible to engage with a human customer without the need for human case workers.

UC3 involves three main players, i.e., TRUSTS, Alpha Bank and Relational Romania (REL):

- Alpha Bank provides financial data of customers, including data related to loan indebtedness;
- REL provides other customer data it has in-house and that it acquires via anonymised data transfers from third parties; and
- TRUSTS provides a series of services, i.e.: anonymisation services to anonymise customer data at Alpha Bank and REL (i.e., prior to data transfer onto the TRUSTS platform); data synchronisation; the application of big data analytics on the anonymised data; incorporation of results into an automated chatbot, to be used by customers; ready-to-market natural language and semantic components for the functioning of the service.

5.3.2 Legal and ethical assessment

The data needed for UC3 are not open-source data and are provided by financial institutions. However, similarly to UC2, since the data transfers relevant to UC3 are envisaged to happen with anonymised data, the assessment focuses on two main activities: the use of the TRUSTS anonymisation application by the data holders; and the use of the TRUSTS FL-based modelling for data transfers and collaboration.

5.3.2.1 Step 1: TRUSTS anonymisation in UC3

The table below contains the assessment for the envisaged data anonymisation operations under UC2. As for UC2, the assessment covers one of the two business opportunities offered by the TRUSTS platform, i.e., the use of ***applications*** on the participating entity's premise. This is in contrast to the *services* provided by TRUSTS and used on the platform itself.

As for UC2, it is to be noted that this assessment is forward-looking, i.e., concerns activities envisaged to be carried out upon project completion based on the components and architecture of the TRUSTS platform.

Table 9: Anonymisation under UC3 – Requirements for the processing of personal data

Task	Assessment
Qualify the data set	The following data sets are likely to be used in UC3: First, **Financial data regarding indebtedness**, such as: - Amount of indebtedness of customers, which are linked to the customer's identity; - Number of unpaid / paid loans per customer; and - Geocode and location data. Second, **customer** data, such as: - The personal details of the customers, such as: name, email address, telephone number, Fax number, device identifier and serial number, license plate number, social security number, date of birth, age, title,

	etc.; and - Number of customers per requested areas identified by postal code. Third, in particular for the training of the Next-Best-Action (NBA) model, **customer metadata**, obtained from the interaction of the customers with the financial institution (end-user).
Define the controller and the processor	Each organisation would qualify as sole controller because: - Each organisation would qualify as a *legal person* within the meaning of Article 4(7) GDPR;
Specify the purpose of the processing and identify a suitable lawful ground for the processing	Similarly to UC2, because the participating entities would be likely have collected the personal data, they hold for purposes other than to extract business value out of a TRUSTS-based data analysis, the entities are unlikely to be able to rely on the compatibility of anonymisation with a former purpose. This means that a new legal base / lawful ground needs to be found. Also, in this case the most suitable legal base appears to be Article 6(1)(f), i.e., the **legitimate interest** of the participating entities. The entities need to identify their legitimate interest so as it is sufficiently clear, lawful, and present (e.g., anonymise data for the purpose of accessing improved data analysis), and then carry out a balancing exercise between their legitimate interest and the rights of the data subjects. Because the processing is intended to protect the identities of the data subjects, the processing is likely to be found proportionate in light of a legitimate interest that is lawful, clear, and present. Alternatively, as for UC2, the entities may rely on Article 6(1)(a) and seek the **consent** of all data subjects. This would provide stronger data protection guarantees, but it would also likely entail a very heavy and time-consuming process.
Qualify the data processing operation	The data processing operation at issue would be the anonymisation of personal data (financial data on indebtedness, customer data, and metadata).
Ensure data minimisation	Before conducting the data processing operation, each entity would need to carefully assess the nature of the data set and conclude that its size is adequate and does not go beyond what was necessary to extract value out of the contractual relationship with the other entity.
Ensure storage limitation	Each entity needs to make sure to keep their own data set on their premises during the whole anonymisation process and to not share the data sets with outside organisations, not even within the TRUSTS consortium in order to have stronger storage limitation guarantees. Each entity would be advised not to copy or store the data sets in multiple location either before or after the data processing operation.

The table below assesses the requirements related to **transparency and accountability**.

Table 10: Anonymisation under UC3 – Requirements for transparency and accountability.

Task	Assessment
Keep a record of data processing activities	All the organisations involved in the initial data processing (anonymisation) shall keep due record of their own processing, in particular detailing the rationale and the legal ground (Article 6 GDPR) behind the decision to process personal data. Since the processing occurs outside the reach of the TRUSTS platform, this responsibility sits within each end-user.
Comply with the accountability principle	All the organisations involved shall also keep documentation proving their compliance with data protection law, i.e., the rationale and legal ground (Article 6 GDPR) behind the processing, and, if necessary, any agreement between them concerning the sharing of personal data prior to the anonymisation.
Ensure respect for data subjects' rights	All the organisations involved shall also make sure to comply with the requirements set out in Article 13 and/or 14, depending on whether the personal data processed were or were not obtained from the data subjects; and in Article 15 regarding requests of access to their data by the data subjects.

5.3.2.2 Step 2: TRUSTS Federated Learning in UC3

The functioning of the TRUSTS FL-based model in UC3 follows a similar pattern to UC2. As in UC2, the end-user will typically use its anonymised data sets to train its local two models, the ChatBot and the Next-Best-Action (NBA) respectively.

If the end-user intends to train both applications, a similar process is set to occur twice, once for the ChatBot and once for the NBA.

As for the ChatBot model, the end-user uses its anonymised dialogues data set to enrich the model downloaded locally from the TRUSTS platform (where it was provided by another user and possibly already trained by other users). This represents a local training of the ChatBot model. Subsequently, and similarly to UC2, the end-user pushes the locally trained model on to the TRUSTS platform by relying on the TRUSTS FL-based mechanism, which in this case will ensure that the data added to the local model – and transferred to the central node – do not leak any information regarding the data subject.

As for the NBA model, the process is very similar. Instead of the dialogues data sets, which are designed to improve the ChatBot's ability to reply to the customer's questions, here the process mainly concerns metadata that are going to enable the algorithm to establish whether the customer should be granted or denied a loan. The metadata are obtained from the relationships between the end-user (a financial institution) and its customers. Also here, once the NBA model is trained locally by the end-user, the FL-based mechanisms of TRUSTS enable the end-user to push the model to the central node and protect the information.

6 Outstanding legal and ethical aspects

The legal and ethical assessment conducted in the previous chapters has highlighted some areas where the legislation and case law are still evolving and/or do not yet permit to reach reasonably stable conclusions. This Chapter delves into some of these areas and lays the groundwork for the recommendations that will be provided in Deliverable D6.4.

6.1 Legal and ethical aspects regarding UC1

In this subsection an elaboration is offered on the challenges raised in the legal and ethical assessment of UC1. The legal issues surrounding the application of the legal framework to UC1 are explored, with a view to providing research patterns and to issuing recommendations in Deliverable D6.4.

The tools and processes envisaged in UC1 fall within the range of technologies that banks and financial institutions are starting to equip themselves with in order to comply with AML obligations stemming from EU law.[47] Processing customers' personal data is a strategy for achieving more effectively the objectives of AML laws, but it may not always lead to a straightforward and smooth relationship with the objectives of EU fundamental rights law, in particular the protection of personal data.[48]

The use of AI-and ML-enabled analytics tool, while still posing coherence questions about data protection law, adds yet another challenge which relates to the compatibility of AI/ML-enabled systems with the restrictions and safeguards found in EU law to the processing of personal data.[49]

In short, the use of AI/ML-enabled systems for AML purposes leads to the intersection of three legal corpuses that, while being studied by the literature, is not yet being accompanied by clear and easy-to-apply regulatory guidelines that are likely to prevent instances of non-compliance. The three corpuses are the following:

a) first, the EU legislation on AML with its policy objectives related to the fight against money laundering and terrorist financing, its obligations towards targeted entities to carry out checks on their customers, and the national law implementing the Anti-Money Laundering Directive (AMLD);

b) next, the EU legal corpus on data protection, comprising of the EU Charter of Fundamental Rights – in particular Article 8 –, the GDPR, and the case law of the European Court of Justice on the application of the Charter and the GDPR; and

c) finally, the legislative proposal and ethical guidance concerning the use of AI/ML-enabled systems. Aside from the fact that the absence of well-established rules for the use of AI in EU law does not help solving the uncertainty surrounding the EU legal framework, the application of current law to the use of such systems is in and of itself by no means uncontroversial.

[47] Bertrand, Maxwell, Vamparys, *Do AI-based anti-money laundering (AML) systems violate European fundamental rights?,* International Data Privacy Law, 2021, Vol. 11, No. 3, p. 276-277.
[48] D6.2 tension GDPR / AML
[49] Musketeer deliverables generally on AI/ML and GDPR + sources in there

Depending on the analysis carried out in Deliverable D6.2 and expanding on it by analysing specifically the challenges raised by the use of the systems envisaged in UC1 by delving into the practical implications of this relationship in the light of the opportunities provided by EU AML law.

6.1.1 Reconciling data protection and AML: Introduction

Law enforcement relies heavily on data. AML is no exception, and its predictive function cannot do without through analysis of financial and transaction data to identify patterns and suspicious behaviour.[50] It is therefore not surprising that, thanks to their enhanced data analysis capabilities, AI/ML-based tools are increasingly used to support AML policies. Considering EU AML legislation, many such actors have naturally made recourse to AI/ML-based tools to perform AML checks.[51] Due to technical and legal hurdles, AI/ML is not yet massively used in the banking and financial industry,[52] but as UC1 in TRUSTS demonstrates there is a clear case for a more intense recourse to these technologies.

AI/ML-enabled tools can help the industry players throughout their AML compliance steps.[53] In particular, AI/ML can speed up and enhance data analysis in all AML phases, namely for the purpose of name screening, transaction screening, and transaction monitoring; being better than humans at recognising patterns and locating deviations, AI/ML can prove more effective than humans and current IT AML systems to spot suspicious transactions.[54] Generally, AI/ML tools can be broken down into two main categories with respect to the underlying technology and functioning: tools using 'supervised training' and tools using 'unsupervised learning and reinforcement approaches'.

In essence, tools based on *supervised training* get better as they are fed with historical data they can interpret and analyse. For AML purposes, such tools use historical data to calculate a series of parameters to then categorise a given transaction as suspicious or regular. In the current AML context, such tools suffer from a limitation related to data quality. Since banks are not informed of whether transactions previously flagged as 'suspicious' to the authorities were indeed instances of money laundering, inevitably incorporate a margin of error in the data they can feed AI/ML tools with.[55] Tools based on *unsupervised training* present the advantage that they do not need large amount of training data (which is one of the drawbacks of the former type in the current AML context). However, such tools can only detect new, unusual behaviour – which is, to be sure, highly important – and not refine the 'routine' detection of usual behaviour.[56]

[50] See for instance Raaijmakers, *Artificial Intelligence for Law Enforcement: Challenges and Opportunities*, IEEE Security & Privacy, Volume 17 Issue 5, 2019.
[51] The following subsection also hints at the unusual nature of EU AML laws related to entrusting private actors with public interest tasks such as monitoring transactions to fight money laundering.
[52] See Bertrand et al., Maxwell, Vamparys, cited supra, note 47, p. 286: "A shared observation from AML/CFT practitioners is that banks are still very cautious in using ML and that adoption is still slow. ML projects are generally in experimental phase only, due to regulatory uncertainties and operational complexities".
[53] For an overview of AI/ML methods available for AML purposes and the proposition of a new framework, see Han et al., *Artificial intelligence for anti-money laundering: a review and extension*, Digital Finance 2 (2020), 211–239.
[54] Bertrand, Maxwell, Vamparys, cited supra, note 47, p. 276-277.
[55] Ibid., p. 285.
[56] Ibid.

The heavy reliance of AI/ML tools on data inevitably raises the question of their compatibility with data protection law in the various settings in which they are used, including AML. Whilst being purpose-driven, laws generally attempt to be technology-agnostic, i.e., to achieve policy goals without placing undue burden on a given technology. At the same time, like different principles and policy interests are sometimes conflicting with one another, certain technologies have features that appear to line up against or in favour of a given policy goal enshrined in the law. The relationship between AI/ML and data protection is one such example. AI/ML include a series of technologies designed to increase the data processing capabilities available to society, and that are constantly being improved on to process higher amounts of data to extract higher amounts of information. In that, it is easy to see how AI/ML-based tools can help achieving the EU policy objectives in relation to the free flow of data and the digital economy.[57] These objectives, however, coexist with other fundamental objectives of 'constitutional' nature such as the one to protect the personal data of individuals, enshrined in the EU Charter of Fundamental Rights.[58] Such a configuration is well-known in legal theory. Whenever in a legal situation two or more principles cannot be fully made coherent with one another, a balancing exercise becomes necessary to lead to an outcome that preserves the essence of each principle. Now, because of the inherent features of AI/ML technologies, it may not always be straightforward how to encourage their use while preserving with principles of EU data protection law.[59] Some authors have gone as far as argue that the use of AI/ML based on 'big data' is fundamentally incompatible with such principles.[60]

It is not within the scope of this chapter to contribute to this debate. However, the use of AI/ML in the AML domain provides a case study to gauge the extent to which AI/ML can help attaining certain policy goals whilst still respecting the core of data protection principles.[61] The next subsection provides an *in concreto* analysis of how specific AI/ML-enabled tools for AML, such as the one envisaged in UC1 of TRUSTS, can be deployed in compliance with EU data protection law.

6.1.2 GDPR and AML I: Compatibility of AI/ML systems with EU fundamental rights law

The analysis starts by looking at the main features of EU AML legislation. The reader is remanded to Deliverable D6.2 for an introduction to the main provisions of such legislation;[62] this subsection focuses on the crucial provisions for our analysis considering the EU Charter and the GDPR.

At the outset, it must be highlighted that EU AML legislation is special at least for two reasons. First, it includes direct obligations for banks and other financial institutions to carry out activities that amount to pre-emptive law enforcement activities. Such entities are required to monitor customers and their

[57] This stance is also visible in the White Paper on Artificial Intelligence – A European approach to excellence and trust by the European Commission. COM(2020) 65 final.
[58] In particular Articles 7 and 8 of the Charter.
[59] See more in detail below. See also Rossello, Díaz Morales, Muñoz-González, *Data protection by design in AI? The case of federated learning*, Computerrecht 2021/116, 2021.
[60] See e.g.: Center for Information Policy Leadership, *First Report: Artificial Intelligence and Data Protection in Tension*, 2018; Zarsky, *Incompatible: the GDPR in the age of big data*, Seton Hall Law Review 47, 995-1020, 2017.
[61] The term 'whilst' is chosen because EU data protection law and EU AML law do not share the same objectives and hence lead to the need for balancing exercises in practice. See Deliverable D6.2, p. 108 and next subsection of this deliverable.
[62] Deliverable D6.2, Chapter 8, pp. 100 and seq.

transactions with a view to detecting unusual or suspicious behaviour.[63] In this sense, EU AML law shifts the responsibility for such activities from public authorities to private entities, in practice delegating to the latter tasks normally carried out by public powers.[64] Second, targeted entities are also obliged to report the outcome of these tasks to the authorities (Financial Intelligence Units – FIUs[65]) without disclosing it to customers whose data were processed to that effect.[66] These are two uncommon elements in isolation, let alone if combined. Both have significant consequences for the data protection assessment of AI/ML-enabled tools implemented to give effect to AML legislation.

One obvious consequence of the obligations provided for in AML law is that the targeted entities are required to process large amounts of personal data. Targeted entities need first to identify each customer for the purposes of AML checks, which entails processing data that reveal their identity; then they need to keep under scrutiny customers' transactions, hence having access to and processing financial and transaction data.[67] The processing of these data could in theory be used to infer a lot of information about a customer's financial stability, employment history and conditions, social security benefits, and potentially their location, movements, health, political opinions, religious beliefs, etc.[68] The degree of intrusion into customers' lives that can be obtained via AML checks is therefore very high, especially considering that, because of how uncertain the process is and because of the fines foreseen by AML law for non-compliance, targeted entities are incentivised to engage in 'gold-plating', i.e. surf on the 'safe' side and privilege over-scrutiny rather than under-scrutiny.[69]

When asking targeted entities to collect and process personal data, EU AML law (unsurprisingly) does recognise the need to do so in full compliance with fundamental rights, in particular the right to protection of personal data, and with the GDPR.[70] Incidentally, the GDPR would apply regardless of it being mentioned in the various AMLDs, insofar as its legal outreach unquestionably covers the data processing activities carried out by targeted entities under EU AML law.[71] The question is therefore how to balance the objectives of the two frameworks whenever they (seem to) clash, especially in light of the recourse to AI/ML-enabled tools. This is even more crucial given that private actors are called upon to strike such balance in practice when they deploy their IT tools for AML checks, including AI/ML-enabled systems. There is the risk that the AML policy benefits linked to scrutiny being made by the entities with more data on potential launderers (i.e. targeted entities) are offset by undue interferences with fundamental rights when such entities are called upon to strike the balance.[72] It is worth noting that EU

[63] Bertrand, Maxwell, Vamparys, cited supra, note 47, pp. 276-277.
[64] Maxwell, *The GDPR and private sector measures to detect criminal activity*, Law European & Affairs, Bruylant, 2021, p. 3; Milaj, Kaiser, *Retention of data in the new Anti-money Laundering Directive—'need to know' versus 'nice to know'*, International Data Privacy Law, 2017, Vol. 7, No. 2, p. 118.
[65] Articles 30, 31, 32, 32a, 32b, of the 5th AMLD.
[66] Bertrand, Maxwell, Vamparys, cited supra, note 47, p. 283: "AML/CFT laws are unusual because they require private sector actors actively to look for suspicious activity by their customers and report the activity to FIUs without informing their customers".
[67] Milaj, Kaiser, cited supra, note 64, p. 118.
[68] Ibid., p. 118-119; Bertrand, Maxwell, Vamparys, cited supra, note 47.
[69] Bertrand, Maxwell, Vamparys, cited supra, note 47, p. 287-288. Maxwell, cited supra, note 64, p. 3.
[70] See in particular 5th AMLD, Chapter V on Data Protection, Record Retention and Statistical Data.
[71] See in general Bertrand, Maxwell, Vamparys, cited supra, note 47.
[72] Maxwell, cited supra, note 64, p. 3: "In theory this should lead to more targeted, proportionate, and effective solutions. In practice, the risk-based approach puts the burden on private entities to strike the right balance

AML legislation, in its rather principles-based approach to the obligations for targeted entities, neither specifically authorises nor prohibits AI/ML in the context of AML checks, and much less provides guidelines on the proportionality of such technologies. When transposing the AMLD into national law, the Member State legislators may include specific provisions authorising recourse to AI/ML-enabled systems. Explicit mentioning in the law is an essential factor in light of the criteria developed by the case law of the CJEU to assess the compatibility of AI/ML-enabled systems, albeit in different domains than AML.[73]

Against this backdrop, EU fundamental rights law imposes restrictions on the government ability to authorise limitations of individual fundamental rights. The two relevant provisions are Article 52(1) of the EU Charter of Fundamental Rights (hereinafter: EUCFR) and Article 23 GDPR, which articulates the same basic principle. The literature has so far mainly addressed the question of compatibility of AML AI/ML-enabled systems with data protection and fundamental rights by applying a general proportionality test based on these two provisions, somewhat including in this analysis also the assessment of the specific tools deployed by targeted entities.[74]

However, it can be argued that two perspectives need to be distinguished:

a. on the one hand, the compatibility of *legislative measures* authorising restrictions of the right to data protection by means of AI/ML-enabled systems. This compatibility would be assessed on a case-by-case basis under the purview of Articles 52(1) EUCFR and Article 23 GDPR, which are directed at public measures;
b. on the other hand, the compatibility of *specific AI/ML-enabled systems* deployed by targeted entities. This compatibility would be also assessed on a case-by-case basis, but the framework of analysis is different: it includes the law authorising the systems at hand (assuming that the law itself is compatible with EU fundamental rights law as per the analysis referred to in the first point), and the GDPR provisions on lawful grounds for processing.

This is due to a legal and a practical reason: from a legal point of view, the deployment of AI/ML-enabled tools by a bank or another entity would lead to processing of personal data and would need to be justified based on Article 6 GDPR, hence requiring an assessment on its own merits; from a practical point of view, then, however specific and detailed the law authorising such tools may be, its assessment could obviously never account for any possible contextual and technological feature of individual systems. In this vein, the European Data Protection Supervisor (EDPS) has stated that the necessity tests involved in the two analyses[75] are two different concepts.[76]

---

between interference with privacy and the protection of public security. This displacement of the proportionality analysis conflicts with the philosophy of the GDPR and fundamental rights case law, which require that the necessity and proportionality balance be struck by lawmakers and government, not by private entities."

[73]

[74] See in general Bertrand, Maxwell, Vamparys, cited supra, note 47.

[75] See further in the following subsections.

[76] EDPS, *Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights*, Background paper, 2016, p. 4. Quoted by González, De Hert, *Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles*, ERA Forum 19, 597–621 (2019), p. 600.

Now it is time to turn to both analyses. The following subsection looks at the criteria developed by the CJEU based on Article 52(1) EUCFR and Article 23 GDPR and that would be applicable to authorising laws; the subsection immediately after then turns to assessing the compatibility of the specific system envisaged under UC1 of TRUSTS considering the restrictions and opportunities offered by Article 6 GDPR.

Proportionality of AI-based AML tools I: Compatibility of national laws

Article 52(1) EUCFR comes after the enumeration of rights and freedoms. It states that: "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*." The article in essence puts forward five requirements' limitations of fundamental rights need to abide by.[77] In particular, limitations must:

i. Be provided in law;
ii. Respect the essence of the rights and freedoms they intend to limit;
iii. Be intended to meet EU objectives of general interest or the need to protect the rights and freedoms of others;
iv. Be proportionate vis-à-vis the rights and freedoms limited; and
v. Be necessary to achieve the objectives referred to in point iii.

All five requirements entail a substantive test (even the first one). The fourth and fifth requirements point to a proportionality and a necessity test, which both require careful and possibly complex analysis of the measure at issue.[78] The CJEU has scrutinised several – and cleared some – legislative measures created to combat criminal activities on the grounds of Article 52(1).[79]

In its core provision Article 23 GDPR states: "*Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard […]*" one of the objectives of general interest listed in that article. Article 23(2) then lists a series of elements that the legislative measure shall contain in order to be as detailed as possible with regard to the envisaged processing of personal data.

In a critique of typical legislative measures authorising risk-based monitoring by private entities, Maxwell argues that Article 23 places upon the legislator, and not the private entity, the task of striking the balance between the general interest objective and the right to data protection.[80] In doing so, he argues that the risk-based approach introduced in EU AML law sits at odds with the GDPR's philosophy

[77] See also Bertrand, Maxwell, Vamparys, cited supra, note 47, p. 280.
[78] Ibid.: "It will come as no surprise that requirements 4 (necessity) and 5 (proportionality) are the most complex, requiring a concrete analysis of the impact of the measure, its utility and necessity in achieving the public interest objective, and the safeguards provided for in the law to ensure that the adverse effects on fundamental rights are minimized."
[79] Maxwell, cited supra, note 64, p. 21.
[80] Ibid., pp. 3, 21.

grounded on having public powers determine the proportionality of privacy invasive measures.[81] While this is true, it can be argued that this only concerns *part* of the overall ex-ante proportionality assessment, i.e. the crucial step where lawmakers are called to circumscribe the recourse to a given type (or typology) data processing to a degree that does not excessively interfere with the interests protected by the GDPR, and at the same time allows the addressees of the measure to contribute to the general interest objective. However, private entities will still be called on to self-assess whether the data processing they are about to initiate by deploying a *specific* system is proportionate and necessary having regard of the criteria of Article 6, while also having to abide by the criteria set out in the authorising law. In other words, it is right to point out, as does Maxwell, that current AML laws may not be precise enough to satisfy the criteria of Article 52(1) EUCFR and Article 23 GDPR; however, even if the authorising laws were to be irreproachable on those accounts, private entities would still be required to do a balancing exercise depending on the lawful ground chosen under Article 6 GDPR.

Whereas the Article 6 tests are therefore relevant on their own,[82] the question arises as to what the relationship between Article 52(1) EUCFR and Article 23 GDPR is. It is arguable that, although Article 52(1) EUCFR has constitutional value has Article 23 GDPR does not, the question should not really be phrased in terms of what rule prevails, as Article 23 GDPR fully translates the spirit of the Charter provision into EU data protection law. In this vein, the CJEU stated in its *Quadrature du Net* decision[83] that Article 23 GDPR should be applied when relevant on its own merits and should be read considering Article 52(1) EUCFR.[84]

Concerning the requirements that AI/ML-based AML systems would need to comply with, it is helpful to analyse the CJEU case law concerning automated systems to process data in order to fight crime and terrorism in various domains.[85] This analysis allows one to construct a set of features that laws authorising AI/ML-based systems for AML purposes should arguably have. The analysis has been broken down based on the five requirements of Article 52(1) of the Charter, also to reflect the typical Court's line of argumentation when assessing whether a measure that interferes with fundamental rights can nonetheless be justified.

I. Limitation provided in the law

The requirement of 'limitation provided in the law' is one of the most straightforward to address, and at times the Court does not even need to specifically tackle it as the measure at issue is evidently provided for in a legal act.[86] The key substantive condition is that the act that provides for the measure needs to

[81] Ibid., p. 21: "This reveals the major conflict between risk-based approaches and the GDPR. Risk-based approaches have a tendency to outsource the question of necessity and proportionality, including the question of safeguards, to the private sector. The GDPR, and the case law of the CJEU and the ECtHR, require on the contrary that necessity and proportionality be dealt with in the law itself."

[82] See next subsection.

[83] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net et al. v Premier Ministre et al*., judgment of 6 October 2020, ECLI:EU:C:2020:791.

[84] Ibid., para. 202.

[85] For a comprehensive analysis see Bertrand, Maxwell, Vamparys, cited supra, note 47.

[86] See e.g. CJEU judgments in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, judgment of 8 April 2014, ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige v Post- och telestyrelsen, and*

be legally binding in the legal order in which it produces its effects.[87] As long as the use of AI-based AML systems is provided for by EU law or by national laws or regulations (i.e. not soft law instruments), this requirement should be easy to address.

II. Respect the essence of the rights and freedoms

Assessing whether a measure respects the essence of the rights and freedoms it is limiting, specifically the right to private life and to data protection, may prove less straightforward, especially because this appears to be a very versatile requirement in the case law of the Court.[88] The Court has so far taken a fairly liberal approach to this assessment. It has conceded that even particularly restrictive measures would not infringe the essence of these rights: for instance, in *Digital Rights Ireland*, the Court found that the particular serious interference with fundamental rights did not affect the essence of those rights because the providers involved would at least not have access to the actual content of the data they were going to be allowed to retain, and because the providers would still be obliged, under that particularly serious interference, to observe certain data protection principles.[89]

It appears therefore that so long as the interference does not preclude the application of general data protection principles (which might nonetheless not be sufficient to shield it from a negative result under the proportionality and necessity test), the Court is likely to be ready to consider that the essence of the rights at issue has been respected. The Court is in particular ready to consider that this is the case when the disclosure of information regarding personal identifiers and/or the private life of the data subjects is either prevented[90] or only concerns a limited set of aspects. On the latter point the example of the Canadian-EU PNR Opinion is illustrative. As regards the right to private life, the Court found that the PNR system would, to be sure, reveal very specific information about the data subjects' private life, but those aspects were very circumscribed (they only concerned EU-Canada trade); as regards the right to data protection, the Court found it sufficient that the purposes to use the data at issue were strongly limited, and that the legislation laid down rules to ensure security, confidentiality and integrity of the data and to prevent unlawful access and processing.[91]

It appears, therefore, that as long as EU and national AML legislation can ensure that these minimum requirements are observed, it is likely to pass the essence of rights test.

III. Meeting EU objectives of general interest

The *raison d'être* of this requirement is that the limitation of a fundamental right needs to be based on the aim to pursue an interest that is considered as important by society, i.e., an objective of general interest in the EU context. In the cases *Digital Rights Ireland*, *Tele2 Sverige*, *Ministerio Fiscal*, *Quadrature du Net*, and in the *EU-Canada PNR Opinion*[92] the CJEU has recognised various goals as objectives of general interest, such as: fight against crime; safeguard of public security; fight against international

Secretary of State v Watson, judgment of 21 December 2016, ECLI:EU:C:2016:970; and Case C-207/16, *Ministerio Fiscal*, judgment of 2 October 2018, ECLI:EU:C:2018:788.

[87] *Quadrature du Net* judgment, para. 132.

[88] See e.g. Scarcello, *Preserving the 'Essence' of Fundamental Rights under Article 52(1) of the Charter: A Sisyphean Task?*, European Constitutional Law Review , Volume 16 , Issue 4 , December 2020 , pp. 647 – 668.

[89] *Digital Rights Ireland*, paras. 39-40.

[90] See also *Tele2 Sverige*, para. 101.

[91] *Canadian-EU PNR Opinion*, para. 150.

[92] Case Opinion 1/15, Opinion of the Court (Grand Chamber) of 26 July 2017.

terrorism in order to maintain peace and security. In the AML context the objective of general interest pursued would be the fight against serious crime and terrorist financing.

IV. Proportionality test[93]

In general terms, the proportionality test is about making sure that legislative acts do not exceed the limits of what is appropriate and necessary to achieve a general interest objective.[94]

In the realm of security and fight against crime the Court of Justice has developed a hierarchy between objectives of general interest, distributing them across what can be defined as 'seriousness spectrum' that has a bearing on the degree of seriousness of justifiable limitations of rights and freedoms.[95] In essence, the degree of seriousness of the limitation cannot be higher than the degree of seriousness of the crime that the measure is intended to fight.[96] The CJEU did this in an attempt to avoid restrictions of rights and freedoms that are disproportionate to the objective pursued. In this sense, the general interest objectives can be divided into the following categories, in an increasing order of seriousness: 'combating crime in general'; 'combating serious crime and terrorism' and 'safeguarding public security' (these two on equal terms); and 'safeguarding national security'.[97] The Court, taking into account the features of each specific restriction, then determines how serious is the limitation on rights and freedoms that measure entails, and compares it against the category the objective at hand falls within. In this vein, in *Tele2 Sverige* the Court found that the measure at hand, whilst constituting a serious "interference in the fundamental rights concerned", could be justified by the objective of combating serious crime.[98] This was confirmed in the *Canada-EU PNR* Opinion, where it was held that the fight against terrorism "is capable of justifying even serious interferences with the fundamental rights".[99]

Laws authorising the use of AI-enabled AML tools are therefore going to be scrutinised with a view to establishing whether the seriousness of the objective of general interest pursued by that law is at least equal, if not superior, to the seriousness of the limitation of rights and freedoms generated by the law. The qualification of the objective of fighting money laundering and terrorist financing is therefore important considering the data protection impact by AML legislation. Based on the recent case law, because of the connection between money laundering and terrorist financing, this objective is likely to

[93] Proportionality is discussed before necessity (next paragraph) consciously, given that the Court has often done so in its judgment despite the 2019 EDPS Guidelines on Proportionality recommending to address necessity first and proportionality right after.

[94] See, amongst others, judgments of the Court in cases Case C-343/09 *Afton Chemical* EU:C:2010:419, para. 45; Cases C-581/10 and C-629/10 *Nelson and Others* EU:C:2012:657, para. 71; Case C-283/11 *Sky Österreich* EU:C:2013:28, para. 50; and Case C-101/12 *Schaible* EU:C:2013:661, para. 29.

[95] See in particular the paragraph 'proportionality test' below.

[96] See *Quadrature du Net*, para. 131. *Ministerio Fiscal*, para. 57: "In accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'. By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally".

[97] On the last point see *Quadrature du Net*, para. 136: "The importance of the objective of safeguarding national security… goes beyond that of the other objective […] inter alia combating crime in general, even serious crime, and of safeguarding public security".

[98] *Tele2 Sverige* judgment, para. 102.

[99] *Canadian-EU PNR* Opinion, paras. 108-109.

be qualified as 'fighting serious crime and terrorism',[100] i.e., a high category in the 'seriousness spectrum', but not quite the highest. It is actually worth examining what this may entail in terms of proportionality by looking at how the Court treats interferences generated in the name of the highest category of objectives, i.e. safeguard of national security.[101] In *Quadrature du Net*, after acknowledging that safeguarding national security could – in light of its higher importance than that of any other objective, even fighting serious crime – potentially justify very intrusive restrictions of fundamental freedoms, the Court analysed the measure at issue. The Court held that the monitoring of traffic and location data of – at least in principle – any individual creates a 'particularly serious' interference with fundamental rights by reason of its indiscriminate nature.[102] In that connection, it also held that, as long as a threat to national security is genuine and foreseeable, measures that entail collection, analysis and/or retention of personal data of virtually any data subject, even indiscriminately, i.e. without a connection between the data subject and the threat, can in principle be justified.[103] However, the Court also held that even the indiscriminate processing of data needs to be limited in time – including if it is renewed – to what is strictly necessary, subject to strict safeguards, and cannot be systematic in nature.[104] This line of interpretation confirms the Court's previous reasoning. Based on the *Digital Rights Ireland* and the *Tele2 Sverige* judgments, it can be argued that if the law were to authorise indiscriminate processing of all customer transaction data, this might be illegal insofar as there would be no objective link between the set of data subjects and the money laundering risks of that set of customers.[105]

Two crucial conclusions can be drawn from the reading of *Quadrature du Net* considering previous case law in this respect: firstly, the Court is ready to justify indiscriminate processing of personal data *only* if they serve the purpose of pursuing the most important objective (safeguard of national security). In all other cases, as illustrated further in the same judgment as well as in *Digital Rights Ireland* and *Tele2 Sverige*,[106] the Court has held that measures entailing collection of personal data need to establish a link, even an indirect one, between the data subjects and the threat tackled by the measure. Secondly, even when justifying indiscriminate data processing, the Court does not authorise limitless restrictions of fundamental freedoms. These two conclusions have an impact on AML legislation because, first, although the objective of combating money laundering and terrorist financing is a serious one, it will not be equated to the seriousness of safeguarding national security; and second, because private entities conduct AML checks, they are likely – as they do now[107] – to have to probe into their entire customer dataset, which is likely to amount to an indiscriminate data processing and which, as was just pointed out, may only be justified against an objective equal to the safeguard of national security.

[100] This would arguably be the case even though definition of 'serious crime' depends on national law.
[101] The type of argumentation that follows falls within the necessity assessment in some of the Court's judgments. It is however discussed under proportionality because they relate to the fair balance between the intensity of the measure and the core of the objective of general interest pursued.
[102] Ibid., p. 282. *Quadrature du Net* judgment, paras 146, 174, 177 and 187.
[103] *Quadrature du Net* judgment, para. 137.
[104] Ibid., para. 138.
[105] This is the conclusion proposed by Bertrand, Maxwell, Vamparys, cited supra, note 47: "This wording [in *Tele2 Sverige*] suggests that wholesale analysis of all customer transaction data by banks for AML/CFT purposes would be excessive, and that there would have to be some objective link between the population whose data is being analysed and relevant money laundering risks", p. 281.
[106] See *Digital Rights Ireland*, paras. 56-68 and *Tele2 Sverige*, paras. 110-111.
[107] Milaj, Kaiser, cited supra, note 64, p. 118; Bertrand, Maxwell, Vamparys, cited supra, note 47, p. 286.

Therefore, AML legislation will probably have to strike a balance between the reach of the data processing operations it authorises and its ambitions in combating money laundering. An escape route could be to insert as many safeguards and limitations as possible to the processing, i.e. acting on the other parameters the Court examines in the proportionality assessment, such as: the parameters used for risk profiling; whether or not the processing allows to draw significant conclusions about the data subjects' private lives; access control measures; redress mechanisms available to data subjects; prompt information of data subjects as soon as compatible with any ongoing investigations.[108] It must however be noted that the presence of very strong safeguards in this regard is already something the Court might require by default and all the more so as personal data would be subject to processing prompted by AI-enabled tools, and the Court already held that '[t]he need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing'.[109] Therefore, such safeguards may not be regarded by the Court as something sufficient to clear highly intrusive AML laws but rather as minimum requirements given the potential intrusiveness of AI-enabled tools.

Finally, the judgment of a Dutch district court in *SyRI*[110] may shed some light on the compatibility of AI/ML-based systems with the GDPR principles of transparency and accountability. First, the decision highlights that algorithms need to be 'explainable' to guarantee adequate rights to data subjects and allow courts to review the functioning of the systems;[111] second, it also highlights that explainability cannot be merely replaced by human review of algorithmic decisions, since the two relate to two different concepts, i.e. the transparency of the algorithm itself (which needs to be guaranteed) and the automated nature of the decision as a whole, which is an entirely different matter.[112] It is arguable that this line of reasoning may be shared also by the Court of Justice.[113]

V. Necessity test

The necessity test looks at whether a measure is not just proportionate, but also necessary to pursue the envisaged objective. Measures limiting fundamental rights and freedoms might be: necessary and proportionate; necessary but not proportionate; or proportionate but not necessary. The Court addresses the two requirements in varying order depending on the logic of the argumentation, so that sometimes, depending on which test is applied first, if the measure at hand does not pass it, it is not even needed to address the second.

[108] See Bertrand, Maxwell, Vamparys, cited supra, note 47, p. 280-281, drawing on the *Tele2 Sverige* judgment, para. 121, where the Court held that competent authorities need to inform the data subjects concerned of the processing as soon as informing them does not jeopardise the ongoing investigation.

[109] *Digital Rights Ireland* judgment, para. 55. To be noted that this is independent from and without prejudice to the question as to whether the automatic processing constitutes automated decision-making within the meaning of Article 22 GDPR.

[110] The Hague District Court (Rechtbank Den Haag), *Systeem Risico Indicatie (SyRI)*, judgment of 5 February 2020.

[111] Bertrand, Maxwell, Vamparys, cited supra, note 47, p. 283. It has been highlighted that explainability is often not easy to achieve, and that algorithms are often difficult to be truly understood even to architects. See e.g.: Nišević, *Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR*, Global Privacy Law Review, Volume I, Issue 2, 2020, p. 106: "Depending on what kind of algorithms is used for profiling, and how they are trained, it can be difficult for the designers of a given system to understand how or why an individual has been profiled or why the system has made a decision."

[112] On the latter concept see in particular Subsection 6.1.3.2 on the automated decision-making.

[113] Bertrand, Maxwell, Vamparys, cited supra, note 47.

In *Digital Rights Ireland* the Court recalled that limitations to the protection of personal data can only apply insofar as strictly necessary to the objective at hand.[114] Looking at the Court's case law, the following elements are likely to be relevant in the necessity test:

a) Precision and clarity of the rules at hand;
b) the effectiveness of the measure; and
c) the existence of alternative options (leading to the 'less intrusive means' analysis).

As recalled in *Digital Rights Ireland* and in its *Canada-EU PNR* Opinion, the Court examines whether the measure's rules are precise and clear because the less the measure is precise as to the amount and nature of data to be processed (scope), the higher the chance that data not explicitly mentioned may fall into the measure's net and widen the interference with data subjects' rights, i.e. the lower the chance that the measure will stick to an interference that is strictly necessary. In its *Canadian-EU PNR* Opinion, for instance, the Court found that the list of data points to be processed by Canadian authorities was not defined with sufficient precision.[115] Drafters of AML laws need to be extremely careful with this requirement and to clearly enumerate the data points envisaged to be processed during AML checks.

Then, two key benchmarks used in the necessity test, often in succession, are effectiveness and alternative options. Both benchmarks have a link with the objective the measure attempts to achieve. The analysis looks at effectiveness to establish to what degree the measure at hand is likely to achieve the objective, i.e., how useful the measure is. Of course, the analysis does not content itself with usefulness (which would resemble appropriateness), and here is when the alternative options come into play: the measure at hand does not qualify as necessary if, having regard to the degree to which the measure can achieve the objective, there exist alternative measures that could achieve it to a comparable degree while restricting the right to data protection and privacy to a lesser extent. This is what is referred to as the 'less intrusive means' analysis. Demonstrating effectiveness to the required degree is likely to be a non-negligible challenge for legislators willing to authorise AI-enabled tools, also for reasons alien to the quality of the law itself and having to do with the downstream outcomes of AML flagging.[116]

Assuming that the legislator had all the necessary information to demonstrate the effectiveness of AI-enabled AML tools, the effectiveness would need to be gauged in light of the Court's requirements developed in the *Canada-EU PNR* Opinion and in *Quadrature du Net*, i.e. that the algorithm of the AI-enabled tools should be based on "models and criteria that are specific and reliable, making it possible […] to arrive at results targeting individuals who might be under a 'reasonable suspicion' of participation" in the criminal activity pursued by the measure.[117] From a theoretical standpoint this requirement hits two birds with one stone in the sense that the interest of lawmakers and targeted entities deploying the tools – i.e. catch actual launderers with high precision – coincides with the interest protected by the

[114] *Digital Rights Ireland* judgment, para. 52.
[115] *Canadian-EU PNR* Opinion, para. 155-163.
[116] For instance, as also mentioned above, the generalised lack of reliable feedback from law enforcement authorities on the degree of precision of AML flagging. See on this Bertrand, Maxwell, Vamparys, cited supra, note 47, pp. 277-278; 288-292. Moreover, proof of effectiveness in this context is without prejudice to the need for targeted entities to prove that the AI-enabled tools they intend to deploy are also effective to a sufficient degree in the context of the necessity test under Article 6 GDPR (see below).
[117] *Canadian-EU PNR* Opinion, para. 172 and, to the same effect, *Quadrature du Net* judgment, para. 180.

Court – i.e. ensure that the processing has as little negative spill over effects as possible for data subjects who are not involved in money laundering activities. However, things may not be straightforward in practice. Apart from the context-dependent obstacles mentioned above, there is a key legal question: what does exactly mean to be an individual "who *might* be under a *reasonable* suspicion of participation in [money laundering activities]"? While the intent of the Court is clear – i.e. to ensure that the results of the processing narrow down the scope to individuals likely to be launderers – the actual workings of this requirement may be ambiguous: does the Court refer to individuals who, account being taken of their situation, it would be reasonable to suspect of money laundering? Or is it individuals who the targeted entity is entitled to presume that they might *already* be under suspicion by law enforcement authorities? Neither approach appears convincing. Also, the criterion of reasonableness adds to the uncertainty as it highly depends on the judicial authority's appreciation. This requirement, while going in a clear direction, does not seem to provide a sufficiently reliable discriminating factor between the community of data subjects and the subset of data subjects the measure should focus on how to get closer to being strictly necessary.

Even having established that the measure at hand is effective, it needs to be proven that there are no other means available to attain the objectives that are less intrusive for data subjects' rights. As noted in the literature, this subtest also suffers from the same objective shortcomings plaguing the effectiveness assessment in the first place, i.e. if there is a high uncertainty on how to measure the effectiveness of one approach to doing AML checks, it will also be difficult to compare that and other approaches in terms of effectiveness.[118] This is likely to be a hurdle for AI-enabled systems that, because of their intrusiveness, would benefit from evidence that they can guarantee better results than less intrusive means. At the same time, since even today AML checks are very comprehensive and intrusive, it is debatable whether, if the extent and nature of the data processed, the safeguards in place and the retention periods remain equal, AI-enabled AML tools as such would present a higher level of intrusiveness, apart from the automated nature of the processing.

Having analysed the main challenges lawmakers need to pay attention to when drafting laws authorising the use of AI-based AML tools, the discussion now turns to the actual deployment of such tools. This needs to be following the GDPR provisions on lawful processing.

Proportionality of AI-based AML tools II: Compatibility of private AI tools

Lawful grounds for processing. The legal test for judging the lawfulness of laws authorising AI-based AML tools and the test for judging the lawfulness of the tools to be deployed are two different tests. The difference is motivated by the fact that, while the laws set out the criteria tools should abide by and have general effects, the deployment of one such tool is always a much more specific operation and concerns a technology that, while having to comply with the law, is merely one of the possible implementations of what the law in principles allows.

Moreover, the deployment and use of such a tool constitute processing of personal data within the meaning of Article 4 GDPR, while laws do not in themselves. This requires the targeted entity to carry out an analysis to determine the most suitable lawful ground – amongst those listed in Article 6 GDPR – that

[118] Bertrand, Maxwell, Vamparys, cited supra, note 47, p. 289.

authorises it to carry out the processing through the tool.[119] This analysis is crucial because not every ground has the same legal consequences for the entity and the data subjects.[120] The table below zooms in on the grounds enumerated in Article 6. The conclusion will be that, because consent is unsuitable as a ground, targeted entities must turn to other grounds that prompt a legal test that could be challenging to satisfy entirely. It is also worth noting that the guidance by the Article 29 Working Party and the EDPS on which lawful grounds are recommended has not been crystal-clear and coherent throughout the years.[121] Some authors also argue that the possibility granted to targeted entities to develop their own AML tools is a source of legal uncertainty.[122]

Table 11: Analysis of GDPR lawful grounds for AML data processing by obliged entities

GDPR lawful ground	Analysis
Consent (Article 6(1)(a) GDPR)	Consent is normally the most widely used legal basis whenever data processing operations are envisaged because it also provides the most extensive guarantees to data subjects. However, consent is unlikely to be suitable in the AML contexts: if data subjects knew about the occurrence and details of data processing operations looking for suspicious transactions, actual launderers amongst the targeted entity's customers would be alerted and could try to dodge the checks and evade authorities. For this reason, targeted entities are likely to have to turn to other lawful grounds.
Compliance with a legal obligation (Article 6(1)(c) GDPR)	Targeted entities relying on this ground would claim the fact that AML legislation imposes on them to carry out checks to detect money laundering activities, and that the data processing they enact is necessary to comply with this obligation. It is worth noting that such legislation obliges targeted entities to carry out AML checks but does not oblige them to achieve results that could only be achieved via AI-enabled tools. This is likely to have a bearing on the necessity assessment. The GDPR provides that, in order for the data controller to be able to rely on this ground, the processing needs to be *necessary* to comply with the legal obligation. See further below this table on the necessity test involved in this respect.
Performance of a task	This ground has in common with the previous one the fact that there is an

[119] Article 29 Working Party, Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, 13 June 2011, p. 3: "[…] measures that are imposed as obligations to prevent money laundering and terrorist financing should always have a clear legal basis and remain necessary and proportionate to the nature of the data."

[120] See González, de Hert, *Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles*, Academy of European Law (ERA) Forum, 2019, p. 599.

[121] See on this issue Maxwell, cited supra, note 64, p. 13.

[122] See e.g., Bertrand, Maxwell, Vamparys, cited supra, note 47, p. 279.

carried out in the public interest (Article 6(1)(e) GDPR)	element related to an objective of general interest that informs the targeted entity's behaviour and data processing activity. The difference is that this ground implies the existence of not merely an obligation between legislation and targeted entities, but also of some sort of derogation or deference by the public powers towards private entities. These would carry out an activity not merely because obliged to, but more specifically in order to support the authorities in pursuing a public interest – the fight against money laundering. This scheme conforms rather well to the relationships between actors tasked with fighting money laundering, as recognised also by the 4th AML Directive.[123] Again, the GDPR provides that the controller needs to show that the processing is *necessary* to perform this task. See further below.
Legitimate interests (Article 6(1)(f) GDPR)	Legitimate interest refers to a value or intention the controller seeks to achieve and that complies with the relevant legal framework. As highlighted in Deliverable D6.2, the legitimate interest must also be real, present, and sufficiently so as to allow the balancing test to be carried out.[124] As suggested by the Article 29 WP, targeted entities may claim to have the legitimate interest of verifying the identity of their customers and detect suspicious transactions that might indicate money laundering.[125] It is worth noting that in relying on such ground targeted entities would refer to an interest that goes hand in hand with the objective of general interest pursued by the AML legislation – i.e. it would not be a legitimate interest merely pertaining to the targeted entity's business. Also in this case, the controller needs to show that the envisaged processing is *necessary* for the purpose of its legitimate interests. See further below.

As was just pointed out, three of the four lawful grounds in principle available to targeted entities require the entity to show that the processing to be carried out with an AI-based tool is *necessary* to the purpose at hand. It is worth noting that the necessity test thereby triggered is logically similar but fundamentally different to the necessity test that authorising laws need to pass.[126] The logic is similar in that also this necessity test entails assessing whether the data processing at hand could be replaced by

[123] 4th AML Directive, Article 43: The processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under Regulation (EU) 2016/679 of the European Parliament and of the Council.
[124] Deliverable D6.2, p. 28.
[125] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014, p. 61.
[126] See EDPS, 2016 Toolkit on Necessity: ""Necessity" is also a recurrent condition in almost all the requirements on the lawfulness of the processing of personal data stemming from EU secondary law3. However, necessity of processing operations in EU secondary law and necessity of the limitations on the exercise of fundamental rights refer to different concepts.", p. 4.

an alternative, less intrusive data processing activity. How does this test apply to the three grounds at hand? Each of the three grounds is examined separately.

Compliance with a legal obligation. Here the question to be answered is: "*Are there less intrusive means that can make the controller comply with the legal obligation to the same extent?*" As mentioned in the table above, the fact that the obligation concerns carrying out data processing to detect money laundering and does not aim at results only achievable via with AI-enable tools, is not negligible. If the opposite were true, it would be way easier to comply with the necessity test as it would only be necessary to show that the AI-enabled tool provides sufficient safeguards for the fundamental rights of data subjects. Though, the controller is not shielded by non-AI data processing activities and needs to rely on two elements to prove its case:

a) demonstrate that the processing with AI is not, in and of itself, more intrusive than a more traditional processing; and/or
b) demonstrate that the processing with AI would enable it to achieve the objective to a greater degree than any other traditional processing would, i.e., be better and more accurate at detecting suspicious activities and transactions.

As will be pointed out below, on top of being difficult to prove, this latter element might not be decisive.

Performance of a task in the public interest. Here the question to be answered is: "*Are there less intrusive means that can make the controller perform that task in the public interest to the same extent?*" It can be said that the public interest ground gives somewhat more weight to the latter element mentioned in the paragraph above, i.e., the higher accuracy. Due to the way the legal obligation is formulated in AML legislation, compliance with this legal obligation might be interpreted more strictly, possibly leading to a scenario whereby – failing to demonstrate that AI-based processing is as intrusive as non-AI processing – the higher performance guaranteed by AI might not be a decisive factor in the overall assessment. Conversely, the concept of 'performing a task in the public interest' is hardly a binary concept; in other words, one does not simply perform or not perform a task: it may also perform the task to varying degrees. In this sense, therefore, the possibly higher accuracy of AI-enabled tools might have a larger bearing on the assessment under this ground, since the public interest task at hand – fight money laundering – can be performed increasingly better.

Legitimate interest. Here the question to be answered is: "*Are there less intrusive means that can make the controller achieve its legitimate interest to the same extent?*" The analysis here requires a balancing test in which the controller's legitimate interest is weighted against the interests of the data subject regarding their personal data. The Article 29 WP lists the prevention of money laundering amongst the purposes that may qualify as legitimate interests.[127] However, despite this guidance and even though in the AML case the controller's legitimate interest is in line with the public interest pursued by the authorities, the balancing test is generally harder to meet, and a private legitimate interest is likely to weigh less than an objective of general interest in the overall assessment.

According to the above, it can be argued that the most promising lawful ground for targeted entities may be Article 6(1)(e) GDPR, i.e., performance of a task in the public interest. This is because of the following:

[127] Article 29 Working Party, cited supra, note 125, p. 25.

First, it appears riskier for targeted entities to rely on legitimate interest than it is on the other two grounds. Although the Article 29 WP considers that targeted entities may, "alternatively [to legitimate interest]", explore compliance to a legal obligation as a lawful ground, it appears that the latter provides more assurances than the former, as the purpose is specified in law. Also, the legitimate interest ground is usually relied to when the controller cannot rely on a legal obligation – for instance because the obligation is not enshrined in EU or Member State law, or because the law merely recommends an action to the controller, or the controller has a wide range of discretion. But when the law specifically obliges targeted entities to carry out processing of data and clearly indicates the types of data needed, it appears more straightforward to rely on such obligation than on legitimate interest.

Second, however, as hinted at above, the flexibility with which a public interest can be appreciated vis-à-vis the rigidity of a legal obligation may suggest that Article 6(1)(e) is all things considered more suitable. A controller willing to rely on Article 6(1)(c) to use an AI-enabled AML tool might run the risk that, if it does not demonstrate that the tool would not be less intrusive than non-AI data processing, it might not be able to rely on the higher effectiveness of the tool depending on the legal obligation at hand and on the interpretation that is chosen:

- In some EU Member States AML legislation obliges targeted entities to merely check the identity of bank customers and to report transactions that are deemed suspicious according to given parameters.[128] As long as the obliged entities have systems in place that allow them to do so, for the purposes of the necessity test it may be irrelevant how *effective* the systems are at catching *actual* instances of money laundering. Such type of legislation may therefore impose an obligation that does not give to the effectiveness of the processing sufficient weight for it to be playing a key role in the assessment.
- Conversely, in other EU Member States AML legislation obliges the entities not to report transactions when they are suspicious, but only when the entity believes there is an instance of money laundering or terrorist financing.[129] In these cases, the parameter relating to the effectiveness of the AI-enabled tool might be more relevant: the more effective the entity proves its tool to be, the more likely the entity is to honour the core of its legal obligation.

In terms of choice of lawful ground, some authors suggest that the difference between compliance with legal obligation and performance of a task in the public interest is *in concreto* quite limited insofar as both grounds rely on an authorising law that, in and of itself, needs to abide by the principles of proportionality and necessity.[130] In this sense, a much more meaningful choice would be the one between, on the one hand, either of these two legal grounds, and the legitimate interests ground on the other hand.[131]

[128] This is the case, amongst others, of The Netherlands.

[129] This is the case, amongst others, of Germany.

[130] See e.g., Maxwell, cited supra, note 64, p. 14: "The real debate is not so much between legal obligation and public interest, since both approaches require a basis in law, and the law must contain clear and precise rules which respect the principles of necessity and proportionality. Going down the "legal obligation" path or the "public interest" path leads to the same destination, the requirement of a clear and precise law with appropriate safeguards."

[131] Ibid.: "The real debate is whether legitimate interest can be an acceptable legal basis for risk-based law enforcement cooperation measures".

Necessity test. Whichever of the legal grounds discussed above – other than consent – is chosen, the obliged entities need to demonstrate the necessity of the processing. The logic of this test is similar to the necessity test applying to legislative measures but needs to be circumscribed to the specific features of the processing at hand taking into account the context in which the processing is to be taking place. According to the literature, obliged entities may not have sufficient legal certainty to carry out this exercise with confidence. Depending on the degree of detail in the law, the entities may be left with significant discretion when it comes to determining how to strike a balance between an approach that makes them comply with the obligations while not going beyond what is necessary to do so.[132]

The pillars of the necessity test can nonetheless provide some guidance. The section focuses on the two main ones, i.e.: a) the non-indispensability; and b) the 'no less intrusive means'.

Non-indispensability. This pillar can plead in favour of AI-enabled tools. This is because the pillar suggests that, for a certain data processing approach to satisfy the necessity criterion, it need not be absolutely indispensable to achieve the objective. There is therefore a difference between the legal concept of 'necessary' and that of 'indispensable', the latter being more restrictive. This exempts the targeted entities from having to demonstrate that the recourse to the AI-enable tool is the only possible way to comply with the AML legal obligations. There is another side to this pillar: the fact that if an alternative to a given processing exists but would require disproportionate efforts, then it would not represent an effective alternative to the processing at hand, which could then be deemed 'necessary'.[133] This argument is handful because, as it turns out, the manual data processing for AML purposes is very time- and resource-consuming for the obliged entities.[134]

'No less intrusive means'. This pillar may be more problematic taking into account the particularly worrisome nature of AI and machine learning applied to personal data processing. Manual processing normally allows for fewer insights and inferences than AI-based processing does. To say that, if less intrusive processing were available that allowed the controller to achieve the purpose to the same degree as the processing envisaged, in practice means that it is not sufficient to show that AI tools are as effective as other AML methods – such as non-AI analytics or human analysis – that are by their nature likely to cause intrusions of lower significance into the personal data processed. It is not sufficient because, being presented with equally effective tools, the controller must choose the least intrusive one, which would not be an AI-enabled tool. This argumentation might represent a challenge if this pillar were to be interpreted strictly against a threshold of effectiveness that was given once and for all. However, understanding the notion of 'effectiveness' and varying degrees of effectiveness may help overcome this challenge.

In a scenario whereby the effectiveness threshold was fixed once and for all, the effectiveness factor would be immutable in the necessity equation; the changing factor would only be 'intrusiveness', and non-AI methods would likely always turn out to be preferrable.[135] It follows that for AI-enabled tools to be lawfully used based on GDPR grounds other than consent, they need to be shown more effective than

[132] Bertrand et al, cited supra, note 47, p. 287. See also Maxwell, cited supra, note 64, p. 22. In his opinion, some AML laws are so vague that the public powers basically shift to the obliged entities the burden of finding the right middle ground between efficacy of processing and respect for data protection.
[133] See e.g., González, de Hert, cited supra, note 120, p. 606.
[134] See e.g., Data Analytics - A anti-money laundering weapon in the UAE (nrdoshi.ae).
[135] See for such a logic González, de Hert, cited supra, note 120, p. 600.

other methods. This would amount to raising the 'effectiveness bar' as well as the bar for achieving the purpose at hand.

Let us use a fictional example to illustrate the logic: if a bank shows that it can catch 20% of money laundering situations by using non-AI analytics tools, it could not claim, for instance, that processing of data based on an AI-enabled tool is necessary if such tool also catches around 20% of money laundering situations (any other parameter, such as resource-intensiveness, speed, etc. assumed to be equal). Conversely, if the bank could show that the success rate of the AI tool is, say, 30%, it could be argued that, whilst the non-AI AML methods can still be considered effective and appropriate to achieving the objectives, the AI tool would increase the effectiveness rate compared to past tools, and would allow the controller to achieve the same objectives to a higher degree.

With this in mind, it can be argued argue that it would not be reasonable to not clear the use of the AI tool as non-necessary on grounds that, albeit to a lesser extent, the non-AI tools can still be considered as effective. Such a perspective would risk discouraging technological development and likely condemn the success rate of analysis tools to a sub-optimal level for a very long time. Even if this constraint is overcome, however, the obliged entities still face two challenges: first, they need to be confident that the specific AI tool they envisage to apply is indeed more effective than other available methods; and second, they need to be able to show the higher effectiveness in order to have a chance to pass the necessity requirement.

These two questions are going to be crucial in the Data Protection Impact Assessment (DPIA) that the obliged entities, including those using the TRUSTS platform for AML checks, would need to conduct considering Article 35(1) GDPR.[136] Both questions open up a whole realm of research that needs to start from the status quo when it comes to assessing the effectiveness of AML detection by the obliged entities. The obliged entities are generally aware the average AML checks are quite inefficient, with a low detection ratio. However, because of how the workflow with the FIUs is designed, the entities lack a complete picture of how the suspicious transactions reported are classified and whether they are investigated. There is little to no feedback loop allowing the entities to identify patterns in the transactions that were not actual instances of ML/FT, hence they have little room to improve their detection methods according to such patterns.[137]

It is beyond this report's objectives to investigate in depth the circumstances in which targeted entities can improve their awareness on the effectiveness of AML tools. However, there is one strategy that could enable them to at least have solid knowledge of how effective an AI-enabled tool is before deployment: *training*. Below it is argued that allowing more data processing for the purpose of training AI-enable tools might, especially in a context where FL is used, be justified by the need to deploy a tool that is more effective and efficient – hence that presents a better privacy/utility trade-off – than current AML detection methods.

6.1.2.1 Data processing to train AI-based AML tools

As was pointed out above, the main endeavour in complying with the necessity criterion is to show that the processing envisaged, while not necessarily being absolutely indispensable to the purpose at hand, is however needed because any other form of processing that may be less intrusive for personal data

[136] See also Bertrand et al, cited supra, note 47, p. 289.
[137] Cfr. ibidem for a discussion of the problem and possible solutions.

would not enable the controller to achieve its purpose. In relation to AI-enabled AML systems, the question comes down to determining whether the processing envisaged with the specific tool at hand can be considered as necessary, account being taken of the nature of the processing and the data involved.

The first challenge is a fundamental one and is likely to affect the second one too. Because it is impossible to know how effective an AI will be in the real world before deployment, organisations willing to use AI need to 'train' it beforehand. To train an AI means making it run the same processes as in the post-deployment scenario, but in a controlled environment and using 'training' data that allow the tool to develop its analytical capabilities based on the adopted algorithm. The amount, quality, variability and representativeness of data are amongst the most crucial variables conducive to a good training and to being able to deploy the best AI tool possible given the technology at hand. In other words, the more numerous and better the data, the more likely it is that the AI tool will be sufficiently well-trained to reach the expected effectiveness rate and the more likely it is to pass the necessity test. A key difference in that regard is between data that have been pseudo- or anonymised and 'plain' personal data: normally, the more PII and attributes the training data have, the more effective they will be to train the AI tool. Data that have not been made subject to pseudo- or anonymisation contain more information than pseudo- or anonymised data, to the extent that, in certain circumstances and depending on the level of granularity desired in the analysis, an AI tool might never be fully trained as effectively with personal data as with anonymised data. In those situations where this is true, organisations such as banks that have used – as is common practice – anonymised data to train the AI tool, at the time of deployment would rely on a tool that is less effective than it would be where it trained with real-life data – i.e. data that it is about to ingest and analyse after deployment.

Hence the crucial question: how can organisations such as obliged entities be expected to satisfy the necessity test of Articles 6(1)(c), (e) and (f), by demonstrating higher effectiveness of AI tools compared to traditional, non-AI analysis methods, if they are strongly encouraged to anonymise training data? In other words, there may be a potential tension between the methodology of the necessity test and the restrictions to process personal data. In order to lawfully use an AI tool without relying on consent, an obliged entity needs the tool to pass the necessity test (i.e., show that it is the least intrusive tool capable of reaching a given level of effectiveness). But to do this the entity needs to have observed the tool in action before deployment in real-life situations and be certain of its level of effectiveness. However, the entity is unlikely to be able to do so without training the tool with non-anonymised data, because the tool would miss out on key information for its training. In short: obliged entities may be prevented from using AI-enabled tools in compliance with GDPR rules on legal grounds for processing precisely because of the restrictions posed by those same rules on earlier processing (for AI training)

This challenge affects the second challenge mainly in terms of time. In an ideal world, i.e., where an obliged entity could deploy the AI tool after training it with 'real-life' data and therefore being confident of its level of effectiveness, the necessity test could be complied with right at the time of deployment. This is because at that point in time it could already be proven that the AI tool is better than previous methods at catching ML and FT. However, because of the first hurdle described above, an obliged entity may never be able to deploy its AI tool with this level of confidence. Hence, the result would be that the entity would deploy and use such a tool, attempt to justify the processing involved based on one of the three legal grounds mentioned above, but would do so surrounded by a mist of legal uncertainty as to whether the tool would pass the necessity test at the time of deployment. The entity could obtain sufficient confidence in that regard only once the tool has worked long enough with personal data in the

real world and has improved its analytical capabilities to the extent that it outmatches those of concurrent methods.

One normative question that arises is, therefore: should the prospects of AI in terms of effectiveness across a broad spectrum of domains (including, but not limited to, AML) encourage us to ease the requirements for processing 'training' data for the purposes of deploying AI-enabled tools that could increase the utility of processing (i.e., in the AML case: increase the success rate in identifying ML and fraudulent situations)? Deliverable D6.4 will provide recommendations in this regard.

6.1.3 AML and GDPR II: Automated individual decision-making

The sections above have focused on the limitations imposed by the GDPR grounds for processing on the operations carried out with AI-enabled tools for AML purposes, specifically focusing on UC1 of the TRUSTS project. The GDPR contains however another limitation targeting AI-enabled data processing: Article 22 provides that "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[138] This rules does not apply when:

a) the processing is necessary for a contract between the data subject and the controller;
b) the processing is authorised by EU or national law that contains adequate safeguards; and
c) the data subject agrees to the processing through their explicit consent.[139]

The subsections below elaborate on the implications of this provision and on whether or not it is likely to apply to the processing envisaged in the real-life scenario of UC1 in TRUSTS.

6.1.3.1 Concepts of automated processing *and* profiling

Amongst the keywords of Article 22(1) there is 'solely': only if the decision at hand is based *solely* on automated processing – which includes profiling – is the decision to be regarded as falling within the purview of Article 22. For now, however, let us focus on the concepts of 'automated processing' and 'profiling'.

Automated processing. This term refers to processing of personal data that is executed – at least partly – by machines (computers). Processing executed by machine learning and AI-enabled tools, such as that envisaged in UC1 of TRUSTS, falls within the concept of 'automated processing'.

Profiling. For the purposes of this provision, the GDPR defines this term as a subset of automated processing.[140] More specifically, it means 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation,

[138] Article 22(1) GDPR.
[139] Article 22(2) GDPR.
[140] It should be noted that the term 'profiling' is not, per se, only a subset of the concept of 'automated processing'. This would mean that profiling must imply data processing executed by computers, which is not the case. Instances of non-automated data processing may also constitute profiling so long as the criteria of the definition under Article 4(4) are fulfilled.

health, personal preferences, interests, reliability, behaviour, location or movements'.[141] The processing envisaged in TRUSTS UC1, in the real-life scenario, is likely to amount to profiling. This is because the processing is carried out on personal data and is intended to categorise the data subjects based on the nature, amount, and circumstances of their transactions. This intent can be said to fall within the concept of 'evaluate certain personal aspects relating to a natural person'. The Article 29 WP indirectly confirm this reading by referring to the profiling carried out by obliged entities subject to a legal obligation for AML purposes.[142]

6.1.3.2 Concept of decisions based solely *on automated processing*

As was established that the processing envisaged in TRUSTS UC1 is likely to qualify as automated processing, and specifically profiling, it must now be determined how likely it is that the outcome of this processing falls within Article 22 GDPR. The purview of Article 22 has been the subject of abundant legal literature given the many possible interpretations of the various concepts contained in the provision.[143] The next paragraphs discuss the meaning of three concepts that are key to determining if Article 22 applies to the TRUSTS UC1 processing: 'solely'; 'decision'; and 'legal effects' for or 'similarly significantly affects' the data subject.

Based solely *on automated processing*. One major point of interest is the term 'solely'. The logic behind the term is to distinguish decisions produced by humans from decision produced by machines, the latter being the subject of Article 22. In a black-and-white world whereby, decisions were made either only by humans or only by machines, there would not be much contention on the breadth of the term 'solely'. In this sense, the 29WP states in its Guidelines that decisions based solely on automated processing imply that "there is no human involvement in the decision process".[144] This statement should not, however, be read in the most restrictive manner as it would mean that as soon as a human element appears in the processing the application of Article 22 is ruled out. Real-life scenarios are often blurred: decisions can be the result of several contributions from humans and machines, sometimes occurring in different

[141] Article 4(4) GDPR.

[142] WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, p. 13.

[143] For instance: Tosoni, *The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation*, International Data Privacy Law, 2021, Vol. 11, No. 2, in which the author tackles the nature of the provision and argues that, contrary to most literature and guidance documents, it should not be seen as an outright prohibition 'in disguise' but rather – as the text of Article 22 suggests – as a right to be exercised by the data subject; Hawath, *Regulating Automated Decision-Making: An Analysis of Control over Processing and Additional Safeguards in Article 22 of the GDPR*, (2021) 7 European Data Protection Law Review (EDPL) 161, proposing a philosophical and theoretical analysis of the background of the GDPR and its implications for the regulation of automated processing; Nišević, *Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR*, Global Privacy Law Review, Vol. I, Issue 2, 2020 Kluwer Law International BV, The Netherlands, focusing on various readings of the term 'profiling' and analysing the 'blind spots' of Article 22 through the application of big data analytics to profiling of consumers; Binns, Veale, *Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR*, International Data Privacy Law, 2021, Vol. 11, No. 4, focusing on the key characteristics of multi-stage decision-making processing that may or may not make that processing fall within the purview of Article 22, account being taken of the terms 'solely', and 'legal or otherwise significant effects'.

[144] WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, p. 20.

stages and with various dependencies. The Article 29 Working Party indeed goes on the specify that the concept of 'human involvement' implies meaningful interventions by humans that are entitled to and capable of overseeing the process effectively and of affecting the results of the automated processing.[145]

Decision. The other key concept to analyse is that of 'decision'. The notion refers to an act whereby the machine or the human allows something to happen, or a situation to change, that will affect the data subject. In this respect, Tosoni rightly observes that the decision should not be confused with the data processing that leads to it.[146] This distinction is essential to allow for the existence of automated data processing operations whose outcome is not a decision for the purposes of Article 22.

Legal or similarly significant effects. This notion indicates that, in order for a decision to fall within Article 22, it does not need to affect the legal situation of the data subject. The scope of decisions caught by Article 22 is broader: it also concerns decisions that affect them 'similarly significantly', i.e., that produce a type of effect by nature different from legal effects, but substantially still very significant. The extent of the notion is debated in the literature.[147] For the purposes of our discussion, there appears to be consensus on the fact that the typical consequences of detecting a suspicion financial transaction – such as: asset freezing; closing of the bank account; etc. – are likely to be similarly significant effects.[148] Binns and Veale debate whether the significance of such effects is to be judged with reference to a *potential* outcome, or to an *actual* outcome, and conclude that if the former interpretation succeeds, then Article 22 may apply to the entire AML detection process.[149] This specific discussion is key to making generally applicable legal policy choices with regard to AML processing by obliged entities; however, it is argued that this question does not even need to be asked in the context of TRUSTS UC1 because the UC does not lead, in the first place, to a decision, as is shown below.

It can be argued that the processing envisaged in the real-life scenario of TRUSTS UC1 does not trigger the application of Article 22 GDPR. This is because when automated processing does indeed take place with no meaningful human intervention, that processing does not lead to decisions having legal or significant effects for the data subjects. The assessment is provided in the table below.

Table 12: Assessment of TRUSTS UC1 vis-à-vis Article 22 GDPR

Step	Assessment
AML Screening	In the first step of the processing, data analytics functionalities are deployed to run the data of the customers against various databases (sanctions lists,

[145] See also Binns and Veale, cited supra, note 143, for a discussion of this concept through the lens of various decision-making models. In particular, they refer to examples – such as the 'triaging' system and the decommissioned UK immigration screening tool – whose logic resembles that of TRUSTS UC1 deployed in real life.
[146] Tosoni, cited supra, note 143, p. 153: "[…] it should be noted that, although a decision adopted under Article 22 is based on automated processing, the decision constitutes the outcome of a processing operation, but does not qualify in itself as processing within the meaning of Article 4(2) GDPR."
[147] Ibid.; see also González, de Hert, cited supra, note 120.
[148] Recital 71 of the GDPR mentions: automatic refusal of an online credit application or e-recruiting practices without any human intervention, as examples of legal or similarly significant effects. These appear to be very similar in nature to the automatic annulment of the bank account contract in an AML context. All the more so, automatic reporting of suspicious transaction to FIUs, which could lead to very significant effects from a criminal law perspective, qualifies as legal or similarly significant effect.
[149] Binns and Veale, cited supra, note 143, p. 326.

	Political Exposed Persons, etc.) in order to extract the **risk factors of each customer**. In this step the processing is completely automated, but it can be argued that it does not lead to a) a decision that b) significantly affects the data subject. It is not a decision because the data analysis merely provides a report of the risk factors attached to each individual based on a series of pre-established parameters and does not proactively take a decision that modifies the legal sphere of the data subject.
AML RiSC	In the second step of the processing, an AI-enabled tool **assigns a risk profile** to each customer (low/medium/high) based on the analysis conducted in the first step. Also in this step, there is no decision significantly affecting the data subjects. The processing is automated and based on AI. However, the AI-enabled tool does not decide to trigger restrictions or reporting of an individual customer's situation. It merely limits itself to scoring the customers across a risk matrix based on parameters.
AML Transaction monitoring	In the third step of the processing, the AI-enabled functionality applies the **continuous monitoring** required by law analysing the data related to the customers' transactions. It is a merely analytical step in which no decisions are made by the tool. If the tool detects a transaction that drifts away from the parameters indicating ordinary and non-suspicious transactions, the tool does not automatically report the transaction, nor does it take decisions affecting the customers (such as freezing their assets or closing their bank accounts): the tool will provide **recommendations** for next steps and the transaction will be looked up by a human caseworker. Based on the analysis and scoring carried out in the first two steps and on the monitoring conducted in the third step, if a potentially suspicious transaction is detected, it is **investigated by the caseworker** who, in accordance with applicable law, has discretion on whether to confirm the recommendations of the AI-enabled tool. This last paragraph might lead to another problem. The fact that the human caseworker is entitled and able to overturn or modify the recommendations of the machine is a necessary but not sufficient condition for the processing to escape Article 22 GDPR. This is because from the entitlement and ability to influence the recommendations it does not follow automatically that the caseworker will, in actuality, do so. Caseworkers may in fact creep into 'autonomous bias':[150] It may be the case that caseworkers end up following blindly the recommendations of the AI-enabled system, progressively turning

[150] See Maxwell, cited supra, note 64, p. 19: The existence of meaningful human involvement may also require asking whether human analysts are really making autonomous decisions, or whether they are simply following algorithmic recommendations, a phenomenon known as automation bias.

	their own role into a 'rubber stamping' or a 'token gesture' to echo the 29WP Guidelines.[151] This potential issue concerns the practice of the data processing workflow more than its design. However, it is also a design-related question concerning the implementation of the functionality by obliged entities. This is because the workflow should have **safeguards** in place to ensure that human caseworkers do make full use of their entitlement and capability to review and influence automatic recommendations, and only follow them after assessing that the recommendations correspond to the result of supplementary human analysis.

6.1.3.3 Article 22 GDPR: Conclusions

The previous assessment shows that, as far as the design of the TRUSTS architecture for UC1 goes, the data processing envisaged to occur in the UC1 real-life scenario are unlikely to be subject to the purview of Article 22 GDPR. This is because the AI-enabled tool is not designed to make decisions that may produce legal effects or similarly significant effects for the data subjects. However, obliged entities relying on the TRUSTS applications for AML purposes shall ensure to have sufficient administrative and procedural safeguards in place to avoid the 'automation bias' that might occur if the caseworkers started to 'blindly' follow the automatic recommendations.

In this respect, to the extent that obliged entities give in to this automation bias and give rise to situations where Article 22 would indeed apply, it would be important to clarify the nature of the provision in terms of rights and obligations. This would amount to determine whether Article 22 is an outright prohibition on data controllers or rather confers a right that data subjects can exercise vis-à-vis data controllers that have already conducted the processing at hand. This determination is key as either interpretation of the provision entails different consequences and duties for data controllers.

In connection with the results of this determination, the provision of Article 22(2)(b) warrants a brief note, as it is the only exception that might be invoked by data controllers should Article 22 be found to apply. The provision mirrors somewhat Article 6(1)(c) – processing necessary to fulfil a legal obligation to which the controller is subject – although it does not entail a necessity test and is framed in terms of a law 'authorising' the processing by the controller. For controllers to rely on this provision, there should be a law in the EU or national legal system that specifically authorises and/or (much more unlikely) mandates the use of automated means for AML purposes. To our knowledge, no such laws are in force in the EU as of yet.

Deliverable D6.4 will provide more detailed recommendations on these aspects, namely on the nature of Article 22 (obligation, or right?) and on the use of the Article 22(2)(b) defence.

[151] WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, p. 21.

6.2 Legal and ethical aspects regarding UC2 and UC3

This section examines the legal challenges raised by UC2 and UC3 starting from the legal framework applying to these use cases. On top of the legal framework governing data anonymisation – dealt with in Chapter 4 – the section focuses on competition law and consumer protection law. The first body of law is triggered by the envisaged data exchange agreements between organisations participating in the TRUSTS platform as well as by the role of the platform itself. The second body of law is triggered by the ultimate effect of these agreements, i.e., the possibility for banks and other financial institutions to carry out more targeted marketing activities thanks to the analytics services performed by TRUSTS.

Each area is covered separately below.

6.2.1 Competition law

UC2 and UC3 envisage the participation of: organisations holding CRM data; organisations holding financial data; and the TRUSTS platform. The exchange of data between these organisations might trigger the application of EU and national competition rules governing agreements between companies (Article 101 TFEU and corresponding national provisions) and the abuse of market power (dominant position) by one or more organisations jointly (Article 102 TFEU and corresponding national provisions).

6.2.1.1 Article 101 TFEU: anti-competitive agreements

As far as Article 101 is concerned, it is argued that two distinct situations may arise: **agreements between non-competing undertakings; and agreements between competing undertakings**. Each scenario is tackled separately.

Agreements between non-competing undertakings. These are agreements that are concluded between two or more organisations that do not compete in the same relevant (geographic and product) market.[152] In light of the model and architecture behind the TRUSTS platform and ecosystem, it is argued that this type of agreements is likely to be the most common one in TRUSTS. This is because, as also described in Section 5.2.1, UC2 and UC3 mainly envisage the participation of two organisations active in totally different markets, one of which (for instance active in the telecommunications sector) holds CRM data including geo-location data, and the other one, usually active in the banking sector, holds financial data and wants to cross-analyse them with the CRM data held by the other organisations (or, in a more mature scenario, add the data to an existing model). Should the two companies arrange to exchange the data within the boundaries of the TRUSTS Federate Learning model, the data exchange arrangement would occur between two non-competitors.

This type of agreements is generally less likely to be harmful to competition because the potential colluding element of the agreement would not concern two or more entities that are supposed to

[152] For a definition and overall description of the concept of 'relevant market' in EU competition law, see e.g.: Robertson, *The relevant market in competition law: a legal concept*, Journal of Antitrust Enforcement, Volume 7, Issue 2, July 2019, Pages 158–176; Mandrescu, *Applying (EU) Competition Law to Online Platforms: Reflections on the Definition of the Relevant Market(s)*, World Competition Volume 41, Issue 3 (2018) pp. 453 – 483; Eben, Robertson, *The Relevant Market Concept in Competition Law and Its Application to Digital Markets: A Comparative Analysis of the EU, US, and Brazil*, Journal of European Competition Law and Economics 2021.

genuinely compete; in other words, the restriction of the market uncertainty stemming from the data exchange would not diminish competition in the relevant market of the two companies.

Agreements between competing undertakings. These are agreements that are concluded between two or more organisations that *do* compete in the same relevant market. Two or more banks / financial institutions would very likely be considered as competing in the same market for financial and banking services; similarly, two telecom companies would be considered as competing in the market for telecommunication services. These agreements are generally known as *horizontal agreements*, but only if the organisations involved in the agreement compete both on the same relevant product and geographic market.[153] Compared to the former type of agreement, horizontal agreements are generally considered, per se, more likely to have harmful effects on competition because they can place two undertakings at an undue advantage vis-à-vis the rest of the competition. However, this is not to say that horizontal agreements are in principle regarded as illegal by EU law. Quite to the contrary, the law has recognised that horizontal agreements can in certain cases foster cooperation between companies with beneficial effects on the market and on consumers.[154]

It is argued that horizontal agreements are likely to be less common in the TRUSTS ecosystem than the former. This is because the principal structure of cooperation between companies under TRUSTS is likely to be closer to the former type of agreement and involve non-competitors exchanging data sets in a secure and privacy-preserving way to improve their respective services. However, it can also be argued that horizontal agreements, whilst less often, could also be concluded around TRUSTS. This would for instance occur every time two or more banks decide to use the TRUSTS services to improve their marketing capabilities by injecting their data sets into a pre-existing model that can be downloaded from the TRUSTS platform. In such a case, and insofar as the two banks jointly decide to both contribute to the model with their data, they would be performing a coordinated exchange of data through the TRUSTS FL-based model.

The EU Guidelines on Horizontal Agreements are helpful in assessing the risks and limitations of these agreements. First off, it needs to be established if behaviours such as that described in the above paragraph really entails an 'exchange of data'. Indeed, the exchange would not materialise itself as a direct transfer, as the data would be exchanged via the TRUSTS FL-based model reinforced by cryptographic methods. A reading of the Guidelines appears however to suggest that the data exchange that would take place via the TRUSTS platform could very well amount to a data exchange. Indeed, in the section devoted to 'information exchange',[155] it is said that "data can be shared indirectly". It could be argued that, even though the two competitors would not come as far as access the actual pieces of information of each other's data sets, their joint and concerted behaviour would nonetheless lead to the provision of a service that takes full advantage of each other's resources and assets in terms of data and information. Even absent an agreement within the meaning of this term in EU competition law, such a behaviour could still be caught by Article 101 TFEU if some form of coordination or reciprocally aware action occurred: the behaviour would therefore amount to a concerted practice.[156]

[153] See European Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements (hereinafter: EU Guidelines on Horizontal Agreements), 2011, para. 1.
[154] Ibid., para. 2; see also paras. 95-103 with regard to information exchange agreements.
[155] Ibid., paras. 55 et seq.
[156] Article 101 TFEU; EU Guidelines on Horizontal Agreements, paras. 60-63.

The competitive assessment of horizontal agreements aims to determine whether the agreement (or concerted practice) is such as to restrict competition by object[157] or by effect.[158] The very wide variability of horizontal concerted behaviour conceivable under TRUSTS, as well as the potentially different relevant markets involved, makes it impossible to formulate a one-size-fits-all assessment. The Guidelines do however remark that the most worrying agreements and concerted practices in terms of potential competitive harm are likely to occur in very transparent markets, with only a handful of players, where market power is highly concentrated and hence gives more incentives to collude. The EU banking and financial sector, while having been affected by a slight degree in competition after the 2011 financial crisis, appears to maintain a sufficient level of competition so as to make collusion infrequent and unlikely.[159]

This is however not to say that anti-competitive horizontal agreements cannot occur in the TRUSTS ecosystem. This might well be especially if the organisations concerned are large undertakings that the data sets covered by the exchange contain strategic and/or individualised data.[160] Amongst the examples of strategic data the Guidelines mention customer lists,[161] whose potential to be strategic also depends on the degree of aggregation / individualisation.

The example of the customer lists is key to TRUSTS insofar as the main working scenario of UC2 is cooperation around customer lists to carve out the common subset and improve marketing services. To be sure, as often recalled, under the TRUSTS scheme two competitors would not have direct access to each other's customer lists. The TRUSTS FL-based model is designed to prevent disclosure of personal data to participants which do not already hold the data beforehand. However, what the TRUSTS model does *not* prevent (and in fact tries to achieve) is the determination of the common share of customers and its communication to both participants. It is argued that, insofar as the participants are competitors, such a result would reduce somewhat the degree of competitive uncertainty between the two: compared to a scenario whereby neither company knows which customers the other company serves, the after-TRUSTS scenario would enable both companies to know, out of their own share of customers, which are those served by the other company. Each company is therefore given more knowledge about its competitor than it had before. Competition is therefore likely to be reduced to a degree, though arguably much less than if each company had a) direct access to b) the full list of customers of the other. It is recommended that the TRUSTS entity and the companies willing to rely on the platform conduct a competitive assessment of the envisaged practice to rule out anti-competitive effects.

It needs to be noticed that, if the two participating organisations are potential competitors on the same product market – e.g., they are both banks – but are active on different geographies to the extent that their businesses do not affect the same subset of consumers, then the agreement will not be considered a horizontal agreement. This scenario may well occur in the TRUSTS ecosystem when, for instance, two banks involved in an agreement or concerted practice such as the type described above are established in two Member States and not compete in the same relevant product market. The TRUSTS platform

[157] EU Guidelines on Horizontal Agreements, paras. 24-25.
[158] Ibid., paras. 26-31.
[159] See e.g.: Apergis, Fafaliou, Polemis, New evidence on assessing the level of competition in the European Union banking sector: A panel data approach, International Business Review, Volume 25, Issue 1, Part B, February 2016, Pages 395-407.
[160] EU Guidelines on Horizontal Agreements, paras. 86-89.
[161] Ibid., para. 86.

being open also to non-EU undertakings, this scenario may also materialise with a non-EU player concerting with an EU player.

Both scenarios outlined at the beginning of the subsection – i.e., horizontal, and non-horizontal agreements – would be affected by the **role of the TRUSTS platform as an intermediary**. On the one hand, by acting as an intermediary to an agreement or concerted practice that is deemed anti-competitive, the TRUSTS entity may fall afoul of Article 101 TFEU for facilitating the anti-competitive conduct. In certain circumstances, as recognised by the Court of Justice explicitly in the *AC-Treuhand*[162] case, the undertaking acting as intermediary and/or facilitator between the colluders might also be punished under competition law. It is disputable whether the conditions found to be conducive to the infringement in *AC-Treuhand* may materialise in the context of TRUSTS: in that judgment, the Court found that AC-Treuhand a) directly helped such members; and b) played an essential role in connecting the cartel members. It is argued that the TRUSTS architecture makes it difficult to find both conditions. First, from an architecture and workflow point of view, the TRUSTS entity would not manage the relationships between participating companies, nor would it actively connect them and hold a continuous relationship with them. Participating companies would autonomously approach the TRUSTS platform and, if they accept the terms and conditions, rely on it and use the provided services. It would therefore be very difficult for the TRUSTS entity to even be aware of whether two companies willing to use the services have concerted to use the TRUSTS platform to an anti-competitive object or effect. Second, it is very unlikely that the TRUSTS entity could ever satisfy the requirement of playing an *essential* role in connecting two or more competitors in such a scenario. If the competitors are concerting their behaviour, this likely means that they could coordinate *already* before approaching the TRUSTS platform, and hence the role of the TRUSTS entity would be far from required to make the concertation possible.

On the other hand, however, precisely by enabling data sharing agreements and concerted practices between competitors, the TRUSTS platform may be the vehicle of efficiency gains and pro-competitive effects of such cooperation. Indeed, to the extent that the amount, nature, and frequency of the data shared through the TRUSTS FL-based model do not make the agreement anti-competitive, the cost savings in procurement, transactions, information asymmetries, etc. might even make this conduct pro-competitive because it would enable the participating undertakings to improve their services at a far lower cost than if they had to reach the result without the cooperation.

The pro-competitive effect could also be a reason to exempt, under Article 101(3) TFEU, an arrangement that has been found to violate in principle Article 101(1), i.e., the prohibition of anti-competitive agreements. However, the recommendation is to strive to make arrangements that run the least possible risk of infringing Article 101(1) in the first place. This is essentially because it is very hard to prove legally that an anti-competitive agreement satisfies all the conditions required by Article 101(3).

6.2.1.2 Article 102 TFEU: abuse of dominant position

Article 102 TFEU and corresponding national provisions target behaviours of those companies which, starting from a particularly strong market position, restrict or stifle competition by making it more difficult for other organisations to compete with them. Abuses can typically be exclusionary, i.e., the dominant undertaking's practices have the effect of preventing competitors and other undertakings from operating on the market or making it more difficult for them to do so; and exploitative, i.e., the

[162] Case C-194/14, *AC-Treuhand AG v European Commission*, judgment of 22 October 2015, ECLI:EU:C:2015:717.

practices do not per se prevent competitors from operating but render competition ineffective as the dominant undertaking is able to charge unduly high prices or conditions on its customers.

In the context of the TRUSTS platform, given that TRUSTS is envisaged to serve as a major hub bringing together several undertakings willing to do business with one another through data exchange and analytics, the TRUSTS entity might be the sort of actor that, through its architecture and the management of its smart contracts policy, might cause exclusionary practices at the expense of certain undertakings willing to participate in the platform.

It is important to notice, however, that EU competition law only attaches the scrutiny of abusive practices to undertakings that possess an economic power on the relevant market that confers them a 'dominant position'. This is a legal concept determined through economic analysis of various aspects such as the nature of the goods/services at hand, market shares, their trend, the degree of innovation in the market, the nature and extent of competition, etc. Therefore, to the extent that an undertaking engages in exclusionary and/or exploitative behaviour without holding a dominant position, such behaviour cannot be sanctioned by EU competition law, unless in connection with an anti-competitive agreement. From a merely **legal point of view**, this has consequences for TRUSTS: unless the European market for digital marketplaces evolves in a very specific way, it is highly unlikely that the TRUSTS platform will accrue such economic power to be regarded as a dominant undertaking on that market.[163] It appears therefore far-fetched to envisage that TRUSTS may engage in behaviours that would qualify as abusive under Article 102 TFEU.

Whilst this is true from a merely legal standpoint, nonetheless, abusive practices such as those caught by Article 102 when committed by a dominant undertaking might still be reprehensible from an **ethical point of view**. The TRUSTS endeavour is grounded on the search for greater transparency, fairness, and trust in the market for data. Therefore, it is imperative that the TRUSTS platform does the greatest possible effort to avoid unethical behaviours regardless of whether such behaviour might be legally punishable under current laws.

In that regard, one first concern is to make sure that the architectural design of the TRUSTS platform enhances inclusion of any interested organisation and does not have any components or workflows that might be conducive to exclusionary or discriminatory effects. As far as this point is concerned, there is no feature of the proposed TRUSTS architecture that might have the effect of discriminating against participating entities based on their market characteristics: for instance, no 'privileged APIs' (Application Programming Interfaces) are foreseen that could, depending on their design, leave out certain categories of organisations.

Subsequently, it is also important that the prices for the proposed services are not exclusionary and are set in a transparent manner. The TRUSTS smart contracts-based system will be able to ensure the latter element, as the price for each transaction will always be shown in advance before contract signature and accompanied by relevant information and details concerning the service at hand.

[163] This would in any case require defining the relevant market for the TRUSTS platform. Relevant markets in the digital space are typically very fluid, and more so when involving entities – such as TRUSTS – envisaged to provide a wide range of services potentially of interest for any sector. To get more insights on the definition of the relevant market for online platforms and marketplaces, see Podszun, Bongartz, *Competition rules for B2B platforms and marketplaces – guidance from Germany*, European Competition Law Review, E.C.L.R. 2021, 42(5), 247-255.

6.2.2 Consumer protection law

UC2 aims to provide companies with better insights on consumer preferences to carry out more targeted marketing activities and provide more targeted services. On top of the data protection implications assessed in Chapter 4, the use of advanced analytics, including AI-based tools, on personal and non-personal data for marketing purposes can have consumer protection implications.

6.2.2.1 Risks posed by AI and data analytics to consumers

Legal literature bridging consumer protection law and AI & analytics has long studied the potential perverse effects of increased automation and customisation on the principles of consumer protection.[164] It needs to be reminded that the TRUSTS platform would not, in and of itself, be a vehicle through which companies can directly provide marketing services to consumers after making use of the AI-based and data analytics services. In that regard, therefore, each TRUSTS partner should, upon use of the TRUSTS services, conduct its business in full compliance with applicable consumer protection law. However, by providing essentially the technology and the hub for data analytics services, the TRUSTS platform can steer upstream – i.e., facilitate or hamper – such compliance in practice.

The risk posed by AI and data analytics to consumer protection are essentially the following. First, depending on how the algorithm behind the autonomous decision-making process is designed and updated, an AI-based system might arrive at decisions that unduly discriminate against a subset of consumers.[165] This may occur because the parameters under which the algorithm is working tend to attach negative consequences to the existence of a given number of characteristics. Second, AI and analytics may unduly expose consumer vulnerabilities, more than it is currently done with traditional tools. The insights companies can obtain through AI might go as far as exploit the vulnerable traits of their customers by way of profiling and targeting.[166] Third, the complexification of algorithmic decision may also increase the information asymmetry between consumers and businesses, with consumers being increasingly less able to understand the logic behind business decisions and therefore having fewer resources to make fully informed decisions.[167] Fourth, these novel technologies may even undermine the sense of control and autonomy of consumers.[168] The EU consumer protection legal framework is evolving to cope with the rise of AI-based services, but there is currently no law with specific rules to prevent and correct the negative effects of AI and data analytics applied to contractual relationships with consumers.[169] The Unfair Commercial Practices Directive (UCPD),[170] as well as the recent Digital Content

[164] See, e.g.: Ebers, *Liability for Artificial Intelligence And EU Consumer Law*, Journal of Intellectual Property, Information Technology and E-Commerce Law, 2021; Hacker, *Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law*, European Law Journal, 2021; André et al., *Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data*, Customer Needs and Solutions (2018) 5:28-37; Goetghebuer, *AI and Creditworthiness Assessments: the Tale of Credit Scoring and Consumer Protection. A Story with a Happy Ending?*, in De Bruyne, Vanleenhove, *Artificial Intelligence and the Law*, Intersentia, 2021, pp. 429-460.

[165] See, e.g., in the insurance sector: *The European Consumer Organisation (BEUC), The use of big data and artificial intelligence in insurance*, 2020, available at: beuc-x-2020-039_beuc_position_paper_big_data_and_ai_in_insurances.pdf, p. 3.

[166] Ebers, cited supra, note 164, p. 208.

[167] Ibid.

[168] André et al., cited supra, note 164.

[169] Ibid.

and Services Directive[171] and the Sale of Goods Directive,[172] being based on the principle of technological neutrality, do not take specific account of these novel technologies.

The EU Artificial Intelligence Act Proposal[173] is the first legal instrument that explicitly recognises the risks posed by AI to the full spectrum of consumer rights, focusing on preventing not just economic harm, but also emotional and mental harm that may be caused by AI-driven systems. The proposed AI Act has a three-tiered approach to preventing emotional and mental harm:

- First, the AI Act aims to forbid the marketing and use of certain AI-enabled systems that deploy "subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm".[174] This prohibition is welcome but appears quite limited in scope as it targets systems whose primary feature is to deploy such manipulative techniques. Recital 16 reinforces this idea referring to systems "*intended* to distort human behaviour" (emphasis added). The reason why this ban cannot the primary answer to preventing emotional and mental harm caused by AI is that it the ban is based on the notion of 'intent' whereas several ordinary AI-driven systems are capable of distorting consumer choice via more subtle means while not being specifically designed to do so;
- Second, the AI Act proposes a vetting process for those AI systems deemed 'high-risk' systems, which are subject to a continuous risk management system and adequate data governance and management practices; need to be accompanied by technical documentation; to be equipped with record-keeping capabilities; and to be designed in a transparent and understandable manner; have to be designed so as human can oversee their functioning; and are subject to specific accuracy, robustness and cybersecurity requirements.[175] These requirements provide a convincing safety threshold. However, the AI systems falling within this category are either those fall under existing product safety regulations, or other systems – listed in Annex III to the AI Act – that however focus more on social risks;[176]
- Third, and coupling the approach of the proposed Digital Services Act in that regard, the AI Act would introduce transparency and information obligations applying to all AI systems – even those not falling within the 'high-risk' definition – that are intended to interact with natural

[170] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council.

[171] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

[172] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC.

[173] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final.

[174] Article 5(1)(a) of the proposed AI Act.

[175] Articles 9-15 of the proposed AI Act.

[176] See also Vranckaert, *My brain hurts! Can the AI Act adequately protect cognitive and/or mental harm by AI software?* Parts 1 and 2, Blog of the Katholieke Universiteit Leuven (KUL) Centre for IP and IT law (CiTiP), 2021.

persons, or use emotion recognition systems, or biometric categorisaton systems.[177] The transparency information obligations, however, do not seem to be particularly restrictive, as they entail making sure the persons exposed are informed of the operation of the AI system. There is not ex-ante requirement on the inner workings of the algorithms unless the systems fall within the second category above ('high-risk').

Having presented the legal requirements existing and envisaged in EU law to prevent risks concerning manipulation of consumers by AI-driven systems, it is worth looking more closely at how these general risks might materialise in the TRUSTS context under UC2 and UC3. Each use case is covered separately.

UC2: Agile Marketing. The services provided by the TRUSTS platform are of the kind that might present instances of illegal profiling and might be (mis)used by companies to engage in manipulative targeted marketing, including for example instances where companies exert undue influence[178] on customers. If the data analysis system that extracts information from the available data and metadata does place too much weight on certain human biases or characteristics, and if there are no sufficient safeguards to mitigate this patterned behaviour, the resulting recommendations to business users might induce the latter to engage in discriminatory and/or manipulative behaviour on consumers.[179] This is especially the case as the tools provided by the UCPD to fight this type of practices do not appear to be up-to-date:[180] Article 8 UCPD places significant weight on 'aggressive commercial practices', which however require the presence of pressure (not necessarily physical), or harassment, or coercion; the criteria to determine whether any of these took place in a transaction, however, are quite restrictive and seem to not include the cases where AI and data analytics technologies are able to exploit general consumer vulnerabilities that are not linked to any particular "specific misfortune or circumstance of such gravity as to impair the consumer's judgement":[181] the UCPD appears still concerned with traditional commercial practices rather than with innovative behaviour enabled by invasive AI.

The data analysis system (brokerage system in TRUSTS) therefore needs to have the necessary design features to be transparent and provide the necessary safeguards to avoid subsequent exploitative action by companies.

UC3: Customer support services. Contrary to UC2, the services provided under UC3 are straight out meant to improve the customer experience by offering them a better, more articulated and customised guidance services via an AI-enabled ChatBot. However, the inherent pro-consumer goal of the services does not per se rule out potential detrimental effects for consumer rights. Indeed, first of all, all depends on the actual content of the recommendations given by the ChatBot to the consumer – i.e., the data analysis system may be set in such a way as to provide unnecessary and actually harmful recommendations to consumers; second, even with the aim to provide a service that is as customised as

[177] Article 52 of the proposed AI Act.
[178] Pursuant to Article 2(j) UCPD, 'undue influence' means "exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision". This concept is therefore closely linked to the need for consumers to maintain their sense of control and choice with regard to the products and services they consume.
[179] Ebers, cited supra, note 164, p. 212.
[180] Ibid., pp. 209-210.
[181] Article 9(c) UCDP.

possible, the recommendations of the ChatBot might be based on an unduly invasive insight into the consumer's data and emotional response, which may trigger a trespassing of the consumer's private sphere;[182] third, a similar issue to UC2 may also materialise here, namely the ChatBot may be set to carry out profiling activities that turn out to be discriminatory as to the resulting categories of consumers and the corresponding subsequent support strategies in the debt management lifecycle.

6.2.2.2 TRUSTS solutions to prevent risks for consumers: the TRUSTS Recommender System

The TRUSTS platform comprises a brokerage system architecture that contains the main technology behind the capabilities of the services provided to participating organisations. The brokerage system includes a Scalable Recommender System (ScaR) Framework (hereinafter: TRUSTS Recommender System) whose tasks are the following:

- To provide datasets and services recommendations to its users pertaining to their profile and needs;
- To employ matchmaking mechanisms through which hosted datasets are matched with hosted services (e.g., suitable for their analysis) and vice versa; and
- To identify and match related datasets so as to provide combined and enriched data.

The data and metadata contained in the data sets referred in the list above are the ones processed via the TRUSTS Federated Learning model to deliver business value under UC2 and UC3 (as described in Sections 5.1.2 and 5.2.2). The TRUSTS ScaR Framework and Recommender System are developments based on the initial framework used in the DMA marketplace.

As shown in the list above, the TRUSTS Recommender System is designed to make matches between three elements: the users, the services, and the data sets. In the TRUSTS project this has generated six possible combinations where the system would be active:

a) recommending data sets to users;
b) recommending services to users;
c) recommending data sets to services;
d) recommending services to data sets;
e) matching two data sets; and
f) matching two services.[183]

A key feature of the TRUSTS Recommender System is that it has a built-in algorithm which is designed to make recommendations between two categories of items (users / data sets / services) based on the available data. The algorithm, which sits in the Recommender Engine (RE), is also designed to be trained, and one of the key elements of the training is that it is carried out from data and metadata resulting from the interaction between users and services on the TRUSTS platform. This means that the TRUSTS Recommender System is guaranteed not to collect any additional data outside these interactions to refine and target its algorithm. Therefore, the level of interference attainable by the Recommender

[182] See Hacker, cited supra, note 164, p. 2: "Offers can be targeted, that is, made exclusively to specific subgroups of consumers which the trader believes will be particularly receptive because they share certain characteristics.7Hence, consumers do not self-select, but are pre-selected by the trader.8That strategy therefore presupposes knowledge, by the trader, of subgroup membership. Such information is increasingly provided by data collection and algorithmic modelling".

[183] For more details about these combinations please refer to Deliverable D3.12 "Profiles and Brokerage".

System is limited to what it can extract from analysing data resulting from transactions that have already been cleared on the TRUSTS platform, which – as it is useful to remind – is only set to store anonymised data or non-personal data. No personal or non-personal data collection from the data subjects that may be listed in the initial data sets used by the participating companies is envisaged to carry out the Recommender System operations. These safeguards are key to evaluating the ethical dimension of the TRUSTS Recommender System. By only relying on sub-products of TRUSTS-based interactions, the Recommender System only allows for better – algorithm-based – matchmaking of available data and is therefore going to be less invasive than a recommender system that would, on top of applying AI-enabled data analytics, also rely on additional external data. Not only would such data trigger the existence of additional data processing operations, thereby increasing the data protection risks for the data subjects; even in full compliance with data protection law, but reliance on additional data would also increase the degree to which the recommender system would enable participating companies to gather potentially invasive insights into the data subjects' lives.

7 TRUSTS Use Case Pilots: Legal and Ethical Assessment

This Chapter provides the legal and ethical assessment of the pilot activities carried out to test the three use cases of the TRUSTS project. It should be noted that this assessment applies to the carrying out of the use cases for the purposes of the TRUSTS project and does not cover the use of the TRUSTS platform in real-life scenario by organisations willing to rely on the services provided by the TRUSTS platform. Chapter 5 provides the assessment of the three use cases as they are envisaged to be deployed in real life, i.e., after the deployment of the TRUSTS platform.

7.1 UC1 Pilot: Smart big data sharing and analytics for Anti-Money Laundering (AML) compliance

This section provides the legal and ethical assessment of the pilot activities carried out in the TRUSTS project under UC1: AML.

It is worth noting that the workflow related to UC1 assessed in this paragraph does not entail any data – personal or not – being transferred to the TRUSTS platform for further use. For the purposes of the pilot activities, the data used by the WiseBOS two applications and one service that is downloaded and used on-premises by the testing organisations.

It is appropriate to break down the workflow related to UC1 into two main steps:

1. The processing (anonymisation) of the initial data set composed of personal data; and
2. The use of the resulting anonymised data set in the delivery of UC1.

7.1.1 Processing of the initial data set

Although the first step is not formally included in UC1, it includes the activities necessary to obtaining a data set that could be used in the use case trials. The first step is the one that directly concerns the application of the EU data protection legal framework, insofar as the source data are personal data that are subsequently anonymised. This step therefore requires investigating: the nature of the personal data; the definition of the data controller; the lawful ground and purpose for the processing; the actual data processing conducted on the data, including the safeguards applied; and compliance with the transparency and accountability principles.

The tables below provide the substance of the assessment by looking at two main sets of requirements:

1. Requirements for the processing of personal data (Table 13); and
2. Requirements related to transparency and accountability (Table 14).

The table below illustrate the compliance with the requirements for the **processing of personal data**.

Table 13: Legal and ethical assessment UC1 (step 1) – Requirements for the processing of personal data

Task	Assessment
Qualify the data set	The initial data set used by eBOS included the following data input: - Names and other identification data of companies; - Names and other identification data of bank customers; - Number of transactions; - Amount and value of transactions. The data set therefore included data qualifying as personal data within the meaning of Article 4 GDPR. The data set did not include data qualifying as sensitive data for the purposes of Article 9 GDPR.
Define the controller and the processor	With regard to the data processing operation performed on the initial data set, i.e., the anonymisation of the data, eBOS qualifies as data controller within the meaning of Article 4(7) GDPR. This is because: a) First, eBOS, having access to the initial data set, has made the decision to process the personal data contained in that data set and has determined the purpose to do so; and b) Second, eBOS has also determined the means through which the processing was to be carried out. It has decided to apply an anonymisation method. For the above reasons, eBOS is to be regarded as data controller in the first step of the workflow under UC1. eBOS did not rely on any processor when anonymising the original data set for the purposes of UC1. It is therefore not necessary to define the processor(s).
Specify the purpose of the processing and identify a suitable lawful ground for the processing	The purpose of the data processing operation is scientific research. This is compliant with the notion of 'scientific research' spelled out in the GDPR, which includes "technological development and demonstration and […] applied research.[184] Horizon Europe projects, such as the one in which the pilot activities have been carried out, provide a research environment subjected to rigorous ethical review, as confirmed by the EDPS.[185] It is argued that the purpose of conducting scientific research is compatible with the original purpose of the collection of the personal data.
Qualify the data processing operation	eBOS has qualified the data processing operation as anonymisation of personal data. It should be noted that eBOS did not delete the original data set. According to an absolute interpretation of personal data such as the one seemingly provided by the Article 29 WP in 2014, it could be argued that such data is

[184] Recital 159 GDPR.
[185] EDPS, A preliminary Opinion on data protection and scientific research, p. 26, 2020.

	still personal to eBOS. However, the following factors suggest that the data resulting from the operation are anonymous and hence not subject to the GDPR: - First, the use of the data is appropriate and made to achieve a legitimate purpose (i.e., testing of a digital platform to enhance business-to-business relationships); - Second, the individuals entrusted with handling the anonymised data are all employees of eBOS and all bound by contractual and ethical obligations in the framework of the Horizon Europe project; - Third, the eBOS employees delivering the pilot for UC1 were not granted any form of (physical or logical) access to the original data set where the personal data are stored; - Fourth, the statistical results of the processing operations performed on the anonymised data are likely to be non-disclosive; - Fifth, the risk of re-identification from the anonymised data is rated as low. The data anonymisation operation therefore allowed eBOS to pursue its goal of feeding the WiseBOS application with training data while applying the most reliable safeguards to the protection of personal data, i.e., removing the identifiable information. This ensured the lowest possible impact on the data subjects while ensuring the fulfilment of the pilot activities.
Ensure data minimisation	Before conducting the data processing operation, eBOS has carefully assessed the nature of the data set and concluded that its size was adequate and not beyond what was necessary to perform the pilot activities within the TRUSTS project. The size of the data set was deemed to be the minimum required in order to perform data analysis through the WiseBOS application and provide workable results in terms of anomaly detection.
Ensure storage limitation	The personal data set was kept on eBOS' premises during the whole anonymisation process and was not shared with outside organisations, not even within the TRUSTS consortium. It was not copied and stored in multiple location either before or after the data processing operation. The anonymised data resulting from the processing operation were kept on eBOS' premises as well, available to the WiseBOS application for data analysis. The data were not uploaded to the TRUSTS platform nor made available to other organisations.

The table below assesses the requirements related to **transparency and accountability**.

Table 14: Legal and ethical assessment UC1 (step 1) – Requirements related to transparency and accountability

Task	Assessment
Keep a record of data processing activities	Through its Data Protection Officer (DPO), eBOS duly documented the life-cycle of the data processing operation consisting of the anonymisation of the initial data set, in particular:

	- The decision to use on a specific data set; - The selection of the data within the data set to be anonymised; and - The use of the data anonymisation application, including selecting and recording the re-identification risk provided by the application.
Comply with the accountability principle	Through its DPO, eBOS keeps records of the data processing operation and the legal ground chosen for it. It therefore can be argued that eBOS is able to demonstrate compliance with Article 6 GDPR as far as the data anonymisation is concerned; hence, it complies with the accountability principle.
Ensure respect for data subjects' rights	In light of the legal ground chosen for the processing, eBOS has provided, through its DPO, the data subjects with the information referred to in Article 14 GDPR. eBOS has remained available to provide access to the data subjects to their data in accordance with Article 15 GDPR.

7.1.2 Delivery of the UC1 pilot

The initial data set was no longer used for the purpose of delivering UC1. The delivery of UC1 after anonymisation did not involve processing of those or any other personal data.

The anonymised data were ingested by the WiseBOS application to perform simulations in the three consecutive steps envisaged in the UC:

a) AML Screening service;
b) AML RiSC application; and
c) AML TRM application.

The screening activities and the risk assessment were based on profiling by the AI-based component of WiseBOS. The profiling was conducted on anonymised data, and hence it did not need to be surrounded by the guarantees and safeguards necessary for profiling on personal data – in particular the need for the data subjects' explicit consent.[186] The use of anonymisation techniques made the profiling operations fully in line with the 29WP's 2017 Guidelines on Guidelines on Automated individual decision-making and Profiling, in which anonymisation techniques are suggested as a good practice for controllers engaging in profiling and automated decision-making activities on data.

Despite the above, the use of AI-enabled tools to conduct profiling on anonymised data does not guarantee that the operation is harmless to the rights of the data subjects. The literature has been studying the data protection risks of relying on anonymised data, in particular re-identification risks. Therefore, it is necessary to assess the profiling activities carried out in the delivery of UC1 to account for the risk of re-identifying the data subjects that the initial data set refers to.

[186] Pursuant to Article 22(1)(c) GDPR.

7.2 UC2 Pilot: The agile marketing through data correlation

This section provides the legal and ethical assessment of the pilot activities carried out in the TRUSTS project under UC2: Agile marketing through data correlation.

Similarly to UC1, it is appropriate to break down the workflow related to UC2 into two main steps:

1. The processing (anonymisation) of the initial data set composed of personal data; and
2. The use of the resulting anonymised data set in the delivery of UC2.

7.2.1 Processing of the initial data sets

In the UC2 pilot two organisations were involved: NOVA and PB. At the start, both organisations held their own data sets containing CRM data. As seen in Chapter 5, CRM data is likely to contain several personal data.

Therefore, in a first step and before initiating their collaboration over the data sets, NOVA and PB used the anonymisation application provided by the TRUSTS platform to independently anonymise their data sets locally. The anonymisation process

The table below illustrate the compliance with the requirements for the **processing of personal data**.

Table 15: Legal and ethical assessment UC2 (step 1) – Requirements for the processing of personal data

Task	Assessment
Qualify the data set	The initial data set used by NOVA and PB included CRM data, which contained data similar to those listed in Section 5.2.2.1. The data set therefore included data qualifying as personal data within the meaning of Article 4 GDPR. The data set did not include data qualifying as sensitive data for the purposes of Article 9 GDPR.
Define the controller and the processor	With regard to the data processing operation performed on the initial data set, i.e., the anonymisation of the data, it is argued that NOVA and PB qualified as joint controllers within the meaning of Articles 4(7) and 26 GDPR. This is because: c) First, both NOVA and PB carried out their data processing upon agreeing to subsequently share the anonymised data for the purpose of testing the functionalities of the TRUSTS platform. This means that NOVA and PB jointly determined the purpose of the data processing operations. They also jointly determined the means of the operation as they agreed to use the anonymisation application provided by TRUSTS; d) Second, it is irrelevant that NOVA did and could not access PB's data set and vice-versa. According to the recent case law of the CJEU,[187]

[187] See case C-210/16, *Wirtschaftsakademie*, judgment of 5 June 2018, ECLI:EU:C:2018:388.

	the fact that one of the entities involved does not access the data that are processed is not per se a condition that rules out joint controllership. For the above reasons, NOVA and PB are to be regarded as joint controllers in the first step of the workflow under UC2. Neither NOVA nor PB relied on any processor when anonymising the original data set for the purposes of UC2. It is therefore not necessary to define the processor(s).
Specify the purpose of the processing and identify a suitable lawful ground for the processing	Similarly to UC1, the purpose of the data processing operation is scientific research. It is argued that the purpose of conducting scientific research is compatible with the original purpose of the collection of the personal data.
Qualify the data processing operation	NOVA and PB have qualified the data processing operation as anonymisation of personal data. NOVA and PB did not delete the original data sets. However, the following factors suggest that the data resulting from the operation are anonymous and hence not subject to the GDPR: - First, the use of the data is appropriate and made to achieve a legitimate purpose (i.e., testing of a digital platform to enhance business-to-business relationships); - Second, the individuals entrusted with handling the anonymised data are all employees of NOVA and PB and all bound by contractual and ethical obligations in the framework of the Horizon Europe project; - Third, the NOVA and PB employees delivering the pilot for UC2 were not granted any form of (physical or logical) access to the original data set where the personal data are stored; - Fourth, the statistical results of the processing operations performed on the anonymised data are likely to be non-disclosive; - Fifth, the risk of re-identification from the anonymised data is rated as low.
Ensure data minimisation	Before conducting the data processing operation, NOVA and PB have carefully assessed the nature of their data sets and concluded that their size was adequate and not beyond what was necessary to perform the pilot activities within the TRUSTS project. The size of the data set was deemed to be the minimum required in order to perform data analysis through for the purposes of UC2 and provide workable results.
Ensure storage limitation	The personal data set was kept on NOVA's and PB's premises during the whole anonymisation process and was not shared with outside organisations, not even within the TRUSTS consortium. It was not copied and stored in multiple location either before or after the data processing operation.

	The anonymised data resulting from the processing operation were kept on NOVA's and PB's premises as well. The data were not uploaded to the TRUSTS platform nor made available to other organisations.

The table below assesses the requirements related to **transparency and accountability**.

Table 16: Legal and ethical assessment UC2 (step 1) – Requirements related to transparency and accountability

Task	Assessment
Keep a record of data processing activities	Through their DPOs, NOVA and PB duly documented the life-cycle of the data processing operation consisting of the anonymisation of the initial data set, in particular: - The decision to use on a specific data set; - The selection of the data within the data set to be anonymised; and - The use of the data anonymisation application, including selecting and recording the re-identification risk provided by the application.
Comply with the accountability principle	Through their DPOs, NOVA and PB keep records of the two data processing operations and the legal ground chosen for them. It therefore can be argued that NOVA and PB are able to demonstrate compliance with Article 6 GDPR as far as the data anonymisation is concerned; hence, they comply with the accountability principle.
Ensure respect for data subjects' rights	Considering the legal ground chosen for the processing, NOVA and PB have provided, through their DPOs, the data subjects with the information referred to in Article 14 GDPR. NOVA and PB have remained available to provide access to the data subjects to their data in accordance with Article 15 GDPR.

7.2.2 Delivery of the UC2 pilot

The initial data sets were no longer used for the purpose of delivering UC2. The delivery of UC2 after anonymisation did not involve processing of those or any other personal data.

Upon the anonymisation, both NOVA and PB declared which data they were going to share with each other for the purpose of the pilot. Subsequently, they both used the MPC functionality provided by the TRUSTS platform to initiate the data analytics phase. The MPC functionality in question is based on the Private Set Intersection (PSI) allowing the collaborating entities to find out the common parts of their data sets without the rest being disclosed to each entity. Thanks to the PSI-based MPC functionality, NOVA and PB benefitted from a match-making process linking the common entries across the two data sets.

7.3 UC3 Pilot: The data acquisition to improve customer support services

This section provides the legal and ethical assessment of the pilot activities carried out in the TRUSTS project under UC3: Data acquisition to improve customer support services.

Similarly to the two previous use cases, it is appropriate to break down the workflow related to UC2 into two main steps:

1. The processing (anonymisation) of the initial data set composed of personal data; and
2. The use of the resulting anonymised data set in the delivery of UC2.

7.3.1 Processing of the initial data sets

In the UC3 pilot two organisations were involved: REL and ALPHA Bank Group. REL provided the main infrastructure and the tools to run the pilot, in particular the environment to import, train and export the ChatBot model – which is designed to guide the real-life customer through their questions – and the NBA model – which is designed to help the real-life operator take a decision based on the customer's situation.

ALPHA Bank Group took the role of the organisation dealing with its customers and provided data sets to train the ChatBot and NBA models. ALPHA Bank Group held a data set largely comparable to the data sets envisaged to be used by financial institutions and banks in real-life deliveries of UC3. As seen in section 5.3.2.1, these data sets typically contain financial and personal data.

The table below summarises the assessment regarding the processing of personal data for the UC3 pilot.

Table 17: Legal and ethical assessment UC3 (step 1) – Requirements for the processing of personal data

Task	Assessment
Qualify the data set	The initial data set used by ALPHA Bank Group included financial and customer data, which contained data similar to those listed in Section 5.3.2.1. The data set therefore included data qualifying as personal data within the meaning of Article 4 GDPR. The data set did not include data qualifying as sensitive data for the purposes of Article 9 GDPR.
Define the controller and the processor	With regard to the data processing operation performed on the initial data set, i.e., the anonymisation of the data, ALPHA Bank Group qualifies as data controller within the meaning of Article 4(7) GDPR. This is because: e) First, ALPHA Bank Group, having access to the initial data set, has made the decision to process the personal data contained in that data set and has determined the purpose to do so; and - Second, ALPHA Bank Group has also determined the means through which the processing was to be carried out. It has decided to apply

	an anonymisation method. For the above reasons, ALPHA Bank Group is to be regarded as data controller in the first step of the workflow under UC1. ALPHA Bank Group did not rely on any processor when anonymising the original data set for the purposes of UC1. It is therefore not necessary to define the processor(s).
Specify the purpose of the processing and identify a suitable lawful ground for the processing	Similarly to the previous use cases, the purpose of the data processing operation is scientific research. It is argued that the purpose of conducting scientific research is compatible with the original purpose of the collection of the personal data.
Qualify the data processing operation	ALPHA Bank Group has qualified the data processing operation as anonymisation of personal data. ALPHA Bank Group did not delete the original data set. However, the following factors suggest that the data resulting from the operation are anonymous and hence not subject to the GDPR: - First, the use of the data is appropriate and made to achieve a legitimate purpose (i.e., testing of a digital platform to enhance business-to-business relationships); - Second, the individuals entrusted with handling the anonymised data are all employees of ALPHA Bank Group and all bound by contractual and ethical obligations in the framework of the Horizon Europe project; - Third, the ALPHA Bank Group employees delivering the pilot for UC3 were not granted any form of (physical or logical) access to the original data set where the personal data are stored; - Fourth, the statistical results of the processing operations performed on the anonymised data are likely to be non-disclosive; - Fifth, the risk of re-identification from the anonymised data is rated as low.
Ensure data minimisation	Before conducting the data processing operation, ALPHA Bank Group has carefully assessed the nature of its data set and concluded that its size was adequate and not beyond what was necessary to perform the pilot activities within the TRUSTS project. The size of the data set was deemed to be the minimum required in order to perform data analysis through for the purposes of UC3 and provide workable results.
Ensure storage limitation	The personal data set was kept on ALPHA Bank Group's premises during the whole anonymisation process and was not shared with outside organisations, not even within the TRUSTS consortium. It was not copied and stored in multiple location either before or after the data processing operation. The anonymised data resulting from the processing operation were kept on

	ALPHA Group's premises as well. The data were not uploaded to the TRUSTS platform nor made available to other organisations.

The table below assesses the requirements related to **transparency and accountability**.

Table 18: Legal and ethical assessment UC3 (step 1) – Requirements related to transparency and accountability

Task	Assessment
Keep a record of data processing activities	Through its Data Protection Officer (DPO), ALPHA Bank Group duly documented the life-cycle of the data processing operation consisting of the anonymisation of the initial data set, in particular: - The decision to use on a specific data set; - The selection of the data within the data set to be anonymised; and The use of the data anonymisation application, including selecting and recording the re-identification risk provided by the application.
Comply with the accountability principle	Through its DPO, ALPHA Bank Group keeps records of the data processing operation and the legal ground chosen for it. It therefore can be argued that ALPHA Bank Group is able to demonstrate compliance with Article 6 GDPR as far as the data anonymisation is concerned; hence, it complies with the accountability principle.
Ensure respect for data subjects' rights	In light of the legal ground chosen for the processing, ALPHA Bank Group has provided, through its DPO, the data subjects with the information referred to in Article 14 GDPR. ALPHA Bank Group has remained available to provide access to the data subjects to their data in accordance with Article 15 GDPR.

7.3.2 Delivery of the UC3 pilot

The initial data sets were no longer used for the purpose of delivering UC2. The delivery of UC2 after anonymisation did not involve processing of those or any other personal data.

Upon the anonymisation, ALPHA Bank Group declared which data they it was going to use for the purpose of the pilot. Subsequently, ALPHA Bank Group used the MPC functionality provided by the TRUSTS platform to initiate the data analytics phase. As for UC2, the MPC functionality in question is based on the PSI allowing the collaborating entities to find out the common parts of their data sets without the rest being disclosed to each entity. Thanks to the PSI-based MPC functionality, ALPHA Bank Group triggered a match-making process linking the common entries across the two data sets provided by that company, thereby simulating a match-making process between two data sets shared by two different organisations in real life.

8 Conclusions and Next Actions

This deliverable provides the legal and ethical assessment of the TRUSTS platform, including its core architecture and components (the FL model and anonymisation services) responsible for data transfers and cooperation on data and metadata; the assessment of this architecture has shown that TRUSTS has implemented a state-of-the-art mix of technological solutions to strike a compromise between data utility stemming from advanced analytics-based cooperation and the protection of personal data and privacy. In particular, the cryptographic methods used to strengthen the FL model are likely to prevent data leakage and potential threats to data protection, thereby increasing the already high privacy-preserving capabilities of the model itself.

The deliverable has also assessed the extent to which current and proposed EU legislation that regulates online, and digital services applies to the TRUSTS platform; and the extent to which the TRUSTS platform has the necessary features to comply with it.

Based on the assessment carried out on the core TRUSTS components and technologies for privacy-preserving data cooperation, the deliverable has then assessed the legal and ethical implications of the three basic use cases envisaged in the real-life deployment of the TRUSTS platform, i.e.: data analytics for AML; data analytics for agile marketing; and data analytics to improve customer support. The assessment has shown that the three UCs are meant to rely on the TRUSTS' core architecture and privacy-preserving services and that this is likely to prevent or reduce to a minimum the risks for data protection. However, the data processing inherent to UC1 (AML) and the legal and ethical implications on consumers and competition of UC2 and UC3 have sparked the need for a more thorough legal analysis of the outstanding legal issues concerning the three UCs.

In this regard, the deliverable has delved into an analysis of the legal and ethical requirements coming from AML law, combined with data protection law, regarding UC1, and argued that the TRUSTS platform operations to facilitate AML processes are unlikely to be characterised as interferences that would infringe the proportionality and necessity test applied by the Court vis-à-vis EU fundamental rights law. In regard to UC2 and UC3, the assessment has concluded that the potential to infringe competition law is very limited and mainly concerns one specific type of agreements, to be monitored by the interested parties; the assessment has also concluded that the TRUSTS Recommender System has sufficient safeguards to prevent manipulatory behaviours by the beneficiaries.

Finally, the deliverable provides the legal and ethical assessment of the operations conducted by TRUSTS Consortium partners in the delivery of the use case pilots, i.e., the testing of the use cases as they are envisaged to be deployed in real-life scenarios.

The work of the legal and ethical WP6 will continue based on this assessment and will lead to the elaboration of legal and policy recommendations for stakeholders and policymakers. The deliverable has identified areas of the current legal frameworks that might not provide stakeholders with the necessary degree of legal certainty, either because of legislative proposals whose text is currently evolving, or because of an ongoing process of legal clarification carried out through case law. The next deliverable (D6.4) will address policymakers with a number of recommendations based on the analysis done in this deliverable that might increase legal certainty while legislative proposals and case law evolve over time. The same deliverable will include recommendations to TRUSTS consortium members and other interested stakeholders on how to improve compliance of the TRUSTS platform and of the operations

envisaged to be conducted therein, as well as recommendations on how to get ready for the upcoming legislative developments in the area of data protection and data law as a whole, as well as regulation of artificial intelligence (Data Governance Act, Digital Services Act, Data Act, Artificial Intelligence Act). Deliverable D6.4 is foreseen to be released in M36.

Annex I: Legal and Ethical Checklist

This annex presents the Legal and Ethical Checklist used to collect input from the TRUSTS Consortium Partners for the legal and ethical assessment.

Table 19: Legal and Ethical Checklist

#	Legal base	Requirement	Applicability	Notes and comments by partners
Part I: Data protection				
Requirements related to lawfulness of data processing *The first seven requirements below relate to the six lawful grounds of processing as per Art. 5 GDPR. Data processing is lawful provided that it complies with at least one lawful ground.* *The other requirements relate to the lawful grounds of processing of special categories of personal data (i.e. sensitive data). Such data are unlikely to be part of the data sets processed within TRUSTS, but the requirements are provided nonetheless for the sake of completeness.*				
Personal data				
1.	Art. 6(1)(a) GDPR	The data subjects have given consent to the processing of his/her personal data for one or more specific purposes.		
2.	Art. 6(1)(b) GDPR	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.		
3.	Art. 6(1)(c) GDPR	Processing is necessary for compliance with a legal obligation to which the controller is		

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

		subject.		
4.	Art. 6(1)(d) GDPR	Processing is necessary in order to protect the vital interest of the data subject or of another natural person.		
5.	Art. 6(1)(e) GDPR	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of judicial authority vested in the controller.		
6.	Art. 6(1)(f) GDPR	Processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.		
7.	Art. 6(4) GDPR	The consortium shall ensure that, when the data collected are intended to be processed for a purpose other than the initial one, for which no consent was obtained and which is not explicitly provided for in EU or MS law, the new processing is compatible with the initial purpose. The consortium shall in particular evaluate the links between the two purposes, the context of the processing, the nature of the data involved, the possible consequences of the new processing for the data subjects, and the application of safeguards,		

		such as encryption, anonymisation and pseudonymisation.		
Special categories of personal data *(i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation)*				
8.	Art. 9(2)(a) GDPR	The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.		
9.	Art. 9(2)(b) GDPR	Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.		
10.	Art. 9(2)(c) GDPR	Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.		
11.	Art. 9(2)(d)	Processing is carried out in the course of its legitimate activities with appropriate		

	GDPR	safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.		
12.	Art. 9(2)(e) GDPR	Processing relates to personal data which are manifestly made public by the data subject.		
13.	Art. 9(2)(f) GDPR	Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.		
14.	Art. 9(2)(g) GDPR	Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.		
15.	Art. 9(2)(h) GDPR	Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or		

		treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.		
16.	Art. 9(2)(i) GDPR	Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.		
17.	Art. 9(2)(j) GDPR	Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.		
Requirements related to data protection principles				
18.	Art. 25(1)	The TRUSTS platform shall implement the **data protection by design principle**, i.e.		

	GDPR	include measures to enhance protection of personal data in the design and deployment of TRUSTS technologies and systems.		
19.	Art. 25(1) GDPR	The TRUSTS consortium shall use engineering privacy to embed privacy by default and by design in the platform.		
20.	Art. 5(1)(b) GDPR	The TRUSTS platform shall implement the **purpose limitation principle**, i.e. ensure that the data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.		
21.	Art. 5(1)(b) GDPR	Whenever the TRUSTS consortium intended to collect and process personal data, the consortium has previously defined one or more legitimate purposes for the collection and the processing, and clearly and unambiguously expressed such purpose(s) to the data subjects concerned.		
22.	Art. 5(1)(b) GDPR	Whenever the initially collected personal data were intended to be used for another purpose than the one(s) chosen for the initial processing (i.e. further processing), the TRUSTS consortium made sure that the new purpose(s) were compatible with the initial one(s).		
23.	Art. 5(1)(c) GDPR	The TRUSTS platform shall implement the **data minimisation principle**, i.e. ensure that the data processed are adequate,		

		relevant and limited to what is necessary in relation to the purposes for which they are processed.		
24.	Art. 5(1)(c) GDPR	The TRUSTS consortium has conducted assessments to ascertain whether certain intended results (e.g. from data analysis) could be obtained by using pseudo- or anonymised data sets instead of data sets composed of personal data. In those instances where a positive conclusion was drawn, the TRUSTS consortium has made use of psuedonymisation and anonymisation techniques enabling them to reduce the amount of data qualifying as 'personal data'.		
25.	Art. 5(1)(c) GDPR	For the personal data not already anonymised before being processed by TRUSTS, the TRUSTS consortium has made use of state-of-the-art anonymisation techniques that were applied according to recognised best practices and standards.		
26.	Art. 5(1)(c) GDPR	The consortium makes use of encryption, pseudonymisation and other PETs enabling them to reduce the amount of data qualifying as 'personal data'.		
27.	Art. 5(1)(f) GDPR	The TRUSTS platform shall implement the **integrity and confidentiality principle**, i.e. ensure that the data are processed in a manner that ensures appropriate security		

		of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.		
28.	Art. 5(1)(f) GDPR	The TRUSTS platform shall make use of Privacy-Enhancing Technologies (PETs) such as anonymisation and pseudonymisation whenever processing of anonymised or pseudonymised data is sufficient to achieve the intended purpose.		
29.	Art. 5(1)(f) GDPR	The TRUSTS platform shall have procedures, including technical safeguards such as access control mechanisms, in place to ensure that only authorised personnel that forms part of the project teams has access to personal data.		
30.	Art. 5(1)(f) GDPR	The TRUSTS platform shall implement all available state of the art security and safety measures to prevent any unauthorised access or alteration, and to restore the availability and access to data and system processes		
31.	Art. 5(1)(d) GDPR	The TRUSTS platform shall implement the **data accuracy principle**, i.e. ensure that the data processed are accurate and, where necessary, kept up to date.		
32.	Art. 5(1)(d) GDPR	The TRUSTS platform has functionalities enabling it to erase or rectify personal data that are inaccurate and/or procedures in		

		place to ensure erasure and rectification from the third party that provides the source data.		
33.	Art. 5(1)(e) GDPR	The TRUSTS platform shall implement the **storage limitation principle**, i.e. ensure that the data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.		
34.	Art. 5(1)(e) GDPR	The TRUSTS platform has functionalities enabling the automated deletion of data upon the expiration of a pre-set retention period.		
35.	Art. 5(1)(e) GDPR	The TRUSTS platform is set to erase all personal data upon the completion of the processing for which they were collected.		
36.	Art. 5(1)(e) GDPR	The TRUSTS platform is set to erase all anonymised data upon the completion of the project activities.		
37.	Art. 5(1)(a) GDPR	The TRUSTS platform shall implement the **fairness and transparency principle**, i.e. ensure that the data are collected and processed in a fair and transparent manner.		
38.	Art. 5(2) GDPR	The TRUSTS platform shall implement the **accountability principle**, i.e. have measures and/or processes to ensure that the data controller(s) be able to		

		demonstrate compliance with the above data protection principles.		
Requirements related to responsibilities with regard to data protection				
39.	Art. 4(7) GDPR	The consortium shall identify the legal entity(ies) that qualify as data controller(s), i.e. as "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".		
40.	Art. 26 GDPR	The consortium shall identify whether, according to the role of more than one entity in TRUSTS, there is joint controllership shared by two or more legal entities, i.e. a situation whereby two or more entities share the controller's responsibility with regard to a specific data processing operation. If there is joint controllership, data controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under GDPR, in particular as regards the exercising of the rights of the data subject, by means of an arrangement between them.		
41.	Art. 26 GDPR	In case of joint controllership, joint controllers shall make arrangements that duly reflect the respective roles and relationships of the joint controllers vis-à-		

		vis the data subjects and its "essence" shall be made available to the data subjects.		
42.	Art. 4(8) GDPR	The consortium shall identify the legal entity(ies) qualifying as data processor(s), i.e. natural or legal persons, public authorities, agencies or other bodies which processes personal data on behalf of the controller(s).		
43.	Art. 28(3) GDPR	The relationship between the controller(s) and the processor(s) shall be governed by contracts or other acts that are binding on the processor with regard to the controller and that set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller		
44.	Art. 4(9) GDPR	The consortium shall identify the entities qualifying as data recipients, i.e. natural or legal persons, public authorities, agencies or another bodies, to which the personal data are disclosed, whether a third party or not.		
45.	Art. 13-14 GDPR	Data controller(s) shall provide data subjects with the identification of recipients or categories of recipients.		
46.	Art. 4(10) GDPR	The consortium shall identify the entities qualifying as third parties, i.e. natural or legal persons, public authorities, agencies		

		or bodies other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.		
47.	GDPR and applicable national data protection law	Data sharing agreements performed in the context of TRUSTS for the provision of personal data sets fully comply with the provisions of GDPR and, when such transfers are made between two EU Member States, fully comply with data protection legislation of those Member States.		
48.	Art. 7 GDPR	The consortium shall have procedures in place to ensure that, if the data subject withdraws their consent, the data controller is required to return the data to the data subject or/and delete the data and terminate data processing activities.		
Requirements related to data subjects' rights				
49.	Art. 12-13 GDPR	The TRUSTS platform shall display a message informing the user of the privacy policy adopted and informing him/her of how their personal data – if any – will be treated.		
50.	Art. 12-13 GDPR	Data subjects that gave their consent to the data processing were given all relevant information related to the controller and the processing, and were informed in a timely manner of the processing of their		

		personal data.		
51.	Art. 12 and 14 GDPR	Data subjects were informed in a timely manner of the processing of their personal data, in cases where their consent was not obtained, and in compliance with other obligations (e.g. obligation to not inform data subjects of processing for anti-money laundering purposes).		
52.	Art. 15 GDPR	The TRUSTS platform is designed to enable access to their personal data to data subjects upon their request.		
53.	Art. 16-17 GDPR	The TRUSTS platform is designed to make it possible to rectify and erase data subjects' personal data upon their request.		
54.	Art. 18 GDPR	The TRUSTS platform is designed to make it possible for the data subject to object to the processing in the cases provided for in the law.		
55.	Art. 20 GDPR	The TRUSTS platform is designed in such a way as to enable data subjects to obtain the data they supplied the platform with (right to data portability).		
56.	Art. 46 GDPR	The TRUSTS platform includes specific safeguards for transfer of personal data outside the EU.		
Part II: Smart contracts				

57.	Principle of good faith in contracting	The TRUSTS platform shall enable a third party to understand the terms of each smart contract proposed on the platform, and to understand the legal consequences of accepting that contract.		
58.	Principle of good faith in contracting	It is recommended that the TRUSTS platform provides a natural language equivalent of each smart contract proposed on the platform.		
Part III: Competition law				
59.	Art. 101 TFEU	Data sharing agreements between TRUSTS and other partners shall not lead to the undue exclusion of, or discrimination against, other undertakings with regard to access to data.		
60.	Art. 101 TFEU	Data sharing agreements shall not include commercially sensitive information to the extent that the agreements may become anti-competitive.		
61.	Art. 101 TFEU	The TRUSTS platform shall ensure that, in its intermediary role between commercial partners, it does not act as a facilitator of anti-competitive behaviour, such as agreements, between these partners.		
62.	Art. 101-102 TFEU	The data sharing arrangements proposed by the TRUSTS platform to users shall not be exploitative and shall not be proposed under unfair prices.		

Part IV: Ethical requirements				
63.	Art. 22 GDPR	The TRUSTS AI-enabled technologies shall not lead to decisions based solely on automated means of processing of personal data. A decision shall be made by a human operator based, amongst other things, on the guidance provided by the analysis generated by the AI.		
64.	EU White Paper on AI; AI Act proposal	The TRUSTS technologies based on artificial intelligence shall ensure that the data are processed with safeguards to prevent discrimination of data subjects. In particular, automated profiling generated by AI-enabled tools shall not result in undue biases or in discriminatory results.		
65.	EU White Paper on AI; AI Act proposal	Designed and implemented algorithms of the TRUSTS platform should not contain any inequality or discrimination by design. This should be observed during the design, training and validation of the system.		
66.	EU White Paper on AI; AI Act proposal	The workings and decision-making of the TRUSTS technologies and systems are frequently reviewed and assessed on their accuracy, fairness and lack of unintended outcomes.		