TRUSTS

Trusted Secure Data Sharing Space

D6.4 Legal and Policy Recommendations

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

Contributors: **Valcke Peggy (CiTiP & imec – KU Leuven)**

December 2022

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

TRUSTS Trusted Secure Data Sharing Space

D6.4 Legal and Policy Recommendations

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	D6.4 “Legal and policy recommendations”		
Work Package	WP6		
Contractual due date	M36	Actual submission date	13 December 2022
Nature	Report	Dissemination Level	Public
Lead Beneficiary	KUL		
Responsible Author	Gugliotta, Lorenzo (KUL)		
Contributions from	Valcke, Peggy (KUL)		

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete[1]	Changes	Contributor(s)
V0.1	03/11/2022	5%	Initial Deliverable Structure	Lorenzo Gugliotta (KUL)
V0.2	17/11/2022	40%	First Draft	Lorenzo Gugliotta (KUL), Peggy Valcke (KUL)
V0.3	29/11/2022	90%	Final Draft	Lorenzo Gugliotta (KUL), Peggy Valcke (KUL)
V0.4	12/12/2022	95%	Final Draft	Andreas Trügler (KNOW), Dominik Kowald (KNOW), Samuel Sousa (KNOW)
V1	15/12/2022	100%	Submission	Alexandra Garatzogianni (LUH), Gerrit Rosam (LUH), Michael Fribus (LUH)

Disclaimer

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

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

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

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

[1] According to TRUSTS Quality Assurance Process:

1. to be declared

Copyright message

Table of Contents

Glossary of terms and abbreviations used

Abbreviation / Term	Description
AI	Artificial Intelligence
AML	Anti-money laundering
29WP	Article 29 Working Party
CFT	Counter financing of terrorism
CJEU	Court of Justice of the European Union
DGA	Data Governance Act
DIS	Data Intermediation Service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSS	Data sharing service
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
FIU	Financial Intelligence Unit
FRAND	Fair, Reasonable, And Non-Discriminatory
FT	Financing of terrorism
GA	Grant Agreement
GDPR	General Data Protection Regulation
GPSD	General Product Safety Directive
HLEG	High-Level Expert Group
IoT	Internet of Things
IP	Intellectual Property

IPR	Intellectual Property Right
ML/FT	Money laundering and terrorist financing
PEP	Politically exposed person
PII	Personal identifiable information
SME	Small and Medium Enterprise
TRUSTS	Trusted Secure Data Sharing Space
UCPD	Unfair Commercial Practices Directive

1 Executive Summary

Deliverable D6.3 is the third legal deliverable in TRUSTS, which follows up on the work performed in D6.1 and D6.2 as well as WP9 relating to ethics and legal requirements of the project. The present deliverable focuses on lessons learned and gaps identified during the project and provides recommendations to both stakeholders in the digital space and policymakers to overcome them. The deliverable provides recommendations in the following areas: (i) the EU data protection legal framework; (ii) the EU legal framework on data, including data governance; and (iii) the EU consumer protection framework.

With regard to *data protection*, the first focus is on the relationship between rules on the protection of personal data and rules regulating the data processing for anti-money laundering (AML) and counter terrorist financing (CFT) purposes. The AML/CFT monitoring being one of the key TRUSTS use cases, it was found that the relationship between these regimes is still a potential source of legal uncertainty, especially as to the lawful grounds for data processing by private entities ('obliged entities') and to the use of AI monitoring system that may make the analysis more precise but also more intrusive for data subjects. The AML/CFT case is also instructive as to another challenge, that concerns the legal regime for processing personal data used to train AI systems before deployment: the need to comply with the data minimisation principle and with the necessity test as per Article 6 GDPR possibly gives rise to a tension that private data controllers (obliged entities) may not find easy to unbundle. Finally, it is shown that the data marketplaces can give rise to complex networks of interactions between various actors (the platform and the participating organisations) that unveil some uncertainties as to the application of the notions of 'controllership' and 'joint controllership'.

With regard to the *EU regulation of data*, the deliverable exposes the need for clarification on the scope of application of the Regulation on data governance (Data Governance Act – DGA) to data marketplaces, focusing also on the grounds of exclusion of the definition of data intermediation services (DIS) providers. It is also shown that the meaning and breadth of some of the conditions and obligations placed upon DIS providers would benefit from more clarifications and guidance, especially the principle of 'neutrality'; and that some others, i.e., the regime on international transfers of/access to data, may place undue decision-making burdens upon DIS providers. It is also shown that the EU regulation on data may give a more prominent role to DIS providers to leverage synergies between the DGA and the Data Act Proposal, especially regarding the role DIS providers can play to bring together data holders and data users under Chapter II of the Data Act Proposal. Finally, still under Data Act Proposal, it is shown that the interaction between the rules on statutory obligations to share data and the fairness rules for data sharing may need further clarification and/or reformulation to enhance legal certainty.

With regard to the EU consumer protection framework, the focus of the analysis is on the risks for consumers stemming from the capability of AI systems to cause cognitive and/or mental harm. AI systems are used by the TRUSTS platform and some of its applications and are likely to be embedded in the services of several other data marketplace platforms participating in the EU data space. It is argued that, in general, the risk of causing cognitive and/or mental harm can negatively affect natural persons both as human beings – hence from a fundamental rights perspective – and as consumers. These risks therefore require sensible regulation, and the AI Act may be a suitable instrument to introduce safeguards from a product safety perspective.

2 Introduction

This document is **Deliverable D6.4 of the TRUSTS project, "Legal and Policy Recommendations"**. It is the fourth and final deliverable within Task 6 of the project. Its goal is to formulate recommendations related to the legal and ethical framework surrounding the TRUSTS experience with a particular emphasis on the real-life deployment of the platform. The recommendations take stock of lessons learned and research conducted in three key areas: (i) EU data protection law, which is key to TRUSTS and similar data marketplaces because the data sets exchanged may contain personal data and hence be handled with extreme care for the rights of the data subjects concerned; (ii) EU law on data governance, which is being enriched and aims to create a comprehensive legal framework for data flows in the digital environment at EU level. This framework places significant responsibilities on entities responsible for intermediation services and digital platforms and is hence of crucial importance to TRUSTS; and (iii) EU law on consumer protection, which is relevant insofar as the data-enriching practices enabled by TRUSTS can have knock-on effects on consumers, in particular via the use of AI-enabled technologies for analysis and value creation to the benefit of commercial actors.

This deliverable provides two types of recommendations: (i) recommendations addressed to relevant stakeholders in the data marketplace ecosystem, such as companies, trade organisations, entities managing data marketplaces and data exchange platforms, and association of digital rights, on how maximise the effectiveness of TRUSTS in compliance with the applicable legal and ethical framework; and (ii) recommendations addressed to policymakers, mainly the European Commission, on how to clarify and/or improve parts of the legal and ethical frameworks applying to TRUSTS and overcome barriers exposed during the project, with a view to unlocking the full potential of EU data marketplaces while complying with the fundamental principles underpinning the EU legal order.

2.1 Mapping Projects' Outputs

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

Table 1: Adherence to TRUSTS GA Deliverable & Tasks Descriptions

TRUSTS Task		Respective Document Chapter(s)	Justification
T6.4 Recommendations	*Point out the potential legal gaps and barriers identified and the lessons learned in the course of the project*	*Chapters 3, 4 and 5*	*Each section within these chapter contains the description of the open point and/or challenge at hand, which may point to a legal gap or barrier, and/or to a lesson learned along with project partners.*

Lead to tailor made recommendations regarding the employment of the platform in compliance with the established legal rules and ethical principles	*Chapters 3, 4 and 5*	*Each section, after the discussion of the open point/challenge, leads to recommendations. It includes recommendations (light green boxes) aimed to encourage compliant behaviour by stakeholders and to advise on how to handle possible legal gaps or uncertainties.*
Develop recommendations for relevant stakeholders and policy makers, based on the identified legal gaps identified and lessons learned	*Chapters 3, 4 and 5*	*On top of recommendations for stakeholders, each section contains a set of recommendations for policymakers (dark green boxes). They include suggestions to increase their awareness of the challenge discussed, and to take policy initiatives to tackle the challenge (e.g., by improving legal certainty).*

2.2 Deliverable Overview and Report Structure

D6.4 relies on the following TRUSTS Deliverables:

- D9.1 to D9.10 on the EC Ethics and Legal Requirements, which set out the initial understanding of the legal and ethical elements relevant to TRUSTS;
- D6.2 “Legal and ethical requirements”, which sets out and explains the legislation applicable to TRUSTS and its stakeholders, and elicits requirements to be taken into account during project design and implementation;
- D6.3 “Legal and ethical assessment”, which, based on the requirements of D6.2, analyses the project results and identifies gaps and lessons learned that are the basis for the recommendations issued in D6.4; and

This Deliverable is structured as follows:

- Chapter 3 discusses open points and challenges that emerged under the EU legal framework on data protection and formulates recommendations in that regard;

- Chapter 4 discusses open points and challenges that emerged under the current and envisaged EU legal framework on data as a whole – including data governance – and formulates recommendations in that regard;
- Chapter 5 discusses open points and challenges that emerged under the EU consumer protection legal framework and formulates recommendations in that regard; and
- Chapter 6 presents concluding remarks.

3 Recommendations in the data protection framework

Below we focus on challenges, open points and lessons learned that have emerged with regard to the EU data protection legal and ethical framework. We present each point and, depending on which group is affected, provide recommendations to stakeholders and/or policymakers. We focus on the following points:

- The relationship between data protection and Anti-Money Laundering (AML) law;
- The processing of training data for AI systems;
- The notion of 'controllership' and its configuration in TRUSTS

3.1 Relationship between AML law and data protection law

Two main challenges were identified. The first one relates to the **tendency of EU and national AML/CFT laws to be vague with regard to carrying out a balancing between law enforcement and data protection objectives**. This balancing is often in practice **shifted to the obliged entities responsible for AML/CFT compliance checks**.

The second one relates to the **legal uncertainty for obliged entities as to the most suitable GDPR legal base for their data processing activities**, and as to the **scope and limitations of these activities taking into account fundamental rights and the data protection framework**.

3.1.1 Description

Legal strategies in a complex tapestry of policy objectives requires careful balancing. It is easy to see why a legal framework intended to protect personal data of natural persons and a legal framework intended to use such data to fight criminal activities may be set, at least in certain occasions, on a collision course. To be sure, it is well-established that, as long as the essence of a given right is not impinged upon,[2] (almost) no right – not even fundamental rights – is absolute and shielded from any limitations whatsoever. This principle applies also to **the fundamental right to data protection**, which **can be limited to achieve other crucial policy objectives, such as the need to counter money laundering (ML) and financing of terrorism (FT) perpetrated by regular customers of financial institutions**. This need has led the EU to enacting a series of directives on anti-money laundering (AML) to harmonise to some extent the national AML strategies.

As explained in D6.2 and D6.3, by definition, AML policies rely on heavy data processing. At the outset, **the peculiar context and dynamics of the ML phenomenon make data processing particularly worrisome** due to two main factors: (i) The amount of data to be processed (collected, analysed, transferred, analysed again by the Financial Intelligence Units – FIUs, etc.) is very large, and the nature of such data is too, as it includes not only data that can allow a direct identification of the person (such as name, surname, age, gender, etc.), but also data on that person's financial transactions, which can reveal – albeit in an indirect

[2] Article 52(1) of the Charter of Fundamental Rights of the European Union.

way – information about his/her financial stability, employment, social security, movements, and even political opinions, religious beliefs, and health;[3] (ii) At least the first processing operations, and in principle the most intrusive ones, need to take place *ex ante*, i.e., before the subset of data subjects concerned can be narrowed down in any way, hence leading to mass data processing affecting millions of natural persons who will have no links with ML or FT. On top of these two factors, **the configuration of the EU AML/CFT framework, which places a large responsibility for data processing upon private entities such as banks and financial institutions ('obliged entities'), does all but raise the data protection concerns**, because the bulk of the initial data processing is entrusted upon private actors *de facto* empowered to enforce the law on behalf of public authorities.

This context places the obliged entities in a particularly delicate situation, whereby they are subject to data protection sanctions, for failing to adequately protect the personal data of their customers; **and to AML/CFT sanctions**, which are particularly strong, for failing to comply with the reporting obligations and to cooperate with the FIUs. Two key issues are worth highlighting here: (i) On the one hand, the compatibility of the current AML/CFT laws with data protection law, especially the case law of the Court of Justice of the EU elaborating on the fundamental right to data protection and the interferences allowed. **AML/CFT laws**, including national laws, on top of demanding large-scale data processing, **tend to be vague as to the data protection safeguards that the obliged entities can – or have to – implement to minimise the impact of AML/CFT data processing on personal data protection**. This leaves the obliged entities with limited guidance on how to operationalise their ancillary role to law enforcement. Therefore, **the balancing exercise to be carried out in the law between two competing policy objectives has a direct impact on the position of the targeted entities**; (ii) On the other hand, the lawful grounds of the GDPR that the obliged entities can rely on to carry out the data processing. This issue is self-standing vis-à-vis the former one, in that it concerns the line of argumentation that the obliged entities are required to choose to justify their decision to process personal data. As explained in D6.3, several of the lawful grounds listed in Article 6 GDPR may be suitable, but – as the TRUSTS partners have pointed out – **the obliged entities do not always have sufficient legal certainty to navigate the rationale behind the various GDPR lawful grounds for processing in the AML/CFT context**. In D6.3 it was argued that the most suitable lawful ground for AML/CFT data processing is Article 6(1)(e) GDPR, i.e., performance of a task in the public interest. This choice finds confirmation in Article 84 of the recent legislative proposal on the Authority for Anti-Money Laundering and Countering the Financing of Terrorism.[4]

The complexities highlighted above are even more compelling in the age of artificial intelligence (AI), which is increasingly used for AML/CFT purposes. If AML/CFT data processing creates uncertainty and has severe implications for data subjects when operated with traditional (human-centred) tools, the use of AI amplifies such challenges. **While AI has the potential to make data analysis more effective and targeted, it is also liable to increase the intrusion into personal data and to extract more information in a more systematic manner**. Moreover, AI systems can issue recommendations that, depending on the configuration at hand, may qualify as decisions based solely on automated means within the meaning of

[3] As far as the three last types of data are concerned, the processing would occur on special categories of personal data as per Article 9 GDPR.

[4] Proposal of Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010.

the GDPR[5] and the Law Enforcement Directive (LED).[6] **It is difficult for the targeted entities**, especially absent AI-specific legislation and/or guidance, **to maintain the balance between these two effects of AI**. AI in AML/CFT is also likely to increase legal uncertainty: whereas with traditional tools the targeted entities tend to 'play on the safe side' and prioritise extensive data processing for fear of AML-related sanctions (which is, in and of itself, not an optimal scenario), the uptake of AI might introduce a new wave of caution and leave the targeted entities in a state of perpetual point-and-shoot approach to data processing for AML/CFT purposes.

3.1.2 Recommendations

For stakeholders

- Stakeholders qualifying as **obliged entities should carry out a Data Protection Impact Assessment (DPIA)** pursuant to Article 35 GDPR before introducing and/or modifying their approach to processing personal data for AML/CFT purposes. This is all the more crucial whenever obliged entities plan on **introducing AI-based tools in their AML/CFT compliance**. A thorough DPIA can help obliged entities comply with the principles of data protection legislation while compensating for the vagueness of AML/CFT legislation on the requirements of AI systems for AML/CFT compliance.
- As argued in D6.3, **obliged entities are encouraged to rely on Article 6(1)(e) GDPR** in order to justify the processing of personal data for AML/CFT purposes, i.e., the performance of a task in the public interest, in line with Article 84 of the legislative proposal on the AML/CFT Authority.
- Obliged entities should closely **follow the developments of the proposed Artificial Intelligence Act (AI Act)** to monitor the provisions on high-risk AI systems and the extent to which AI systems for AML/CFT compliance will be regulated by the AI Act.

For policymakers

- **The European Commission**, the European Data Protection Supervisor (**EDPS**) and/or the European Data Protection Board (**EDBP**) should **consider formulating detailed guidance on the compliance by obliged entities with data protection law**. The guidance should focus on the lawful grounds for processing of Article 6 GDPR and recommend the most suitable ground for processing for AML/CFT purposes. Following the provisional text of Article 84 of the legislative proposal on the AML/CFT Authority, the guidance should encourage relying on Article 6(1)(e) GDPR. The guidance should operationalise the requirements and attention points for the DPIA carried out by obliged entities; and it should devote a section on the safeguards to be adopted when introducing AI systems for AML/CFT compliance.
- The European Commission should consider initiating discussions and/or issuing soft law instruments to **encourage the EU Member States to review national laws on AML/CFT compliance and the role of obliged entities,** with a view to introducing more detailed

[5] Article 22 GDPR.

[6] Article 11 LED.

requirements and conditions that can **boost legal certainty** as to the relationship between data protection and AML/CFT compliance. Review of such legislation is believed, on the one hand, to potentially increase its level of compliance with EU fundamental rights law and the case law of the Court of Justice; and, on the other hand, to potentially increase legal certainty by reinforcing the effect of EU-led guidance (see point above) via binding instruments.

3.2 Processing of AI training data for AI systems

Given the high intrusive potential of AI, **organisations willing to train AI models tend to prefer anonymised data over personal data**, to better comply with data protection principles. However, **this may lead to underperforming AI tools that may not be as effective and hence be less likely to pass the necessity test under Article 6 GDPR prior to deployment**.

3.2.1 Description

This point concerns a **challenge that data controllers willing to rely on AI systems for personal data processing may encounter when trying to comply with the GDPR principle** (especially data minimisation) **and the necessity requirement under Article 6 GDPR for deploying AI systems in real life**. Obliged entities in the AML/CFT context help illustrate this point.

As observed in Section 3.1, the use of an AI-enabled tool to this effect undoubtedly constitutes processing of personal data within the meaning of Article 4 GDPR. The processing requires a lawful purpose and a legal ground, which needs to be different than consent,[7] and that is recommended to be the performance of a task in the public interest as per Article 6(1)(e). Under this legal ground obliged entities are required to show that the processing is 'necessary' to the purpose at hand. **The main endeavour in complying with the necessity criterion is to show that the processing envisaged**, while not necessarily being absolutely indispensable, **is** however **needed because any other form of processing that may be less intrusive for personal data would not enable the controller to achieve its purpose** (i.e., to perform the public interest task). Compliance with the necessity requirement involves the notion of effectiveness and varying degrees of effectiveness. It is not sufficient to show that AI tools are as effective as AML methods – such as non-AI analytics or human analysis – that are by their nature likely to cause intrusions of lower significance into individuals' right to personal data protection. It follows that **for AI-enabled tools to be lawfully used based on the public interest ground, they need to be shown as more effective than other methods**. This would amount to raising the 'effectiveness bar' as well as the bar for achieving the purpose at hand. In this case, the AI tool would increase the effectiveness rate compared to traditional tools, thereby allowing the controller to achieve the same objectives to a higher degree.

[7] Consent is unlikely to serve the purpose, because a) it would run against the requirements of EU AML law that prohibits disclosure of processing to the natural persons concerned; and b) it would defeat the purpose of AML checks: persons who commit money laundering (ML) or fraud are very unlikely to consent to the processing of their personal data.

If this higher effectiveness was demonstrated, it would make sense from a legal policy perspective to allow the deployment and use of the AI system. Even under this approach, however, **obliged entities still face two challenges**:

- First, **they need to possess sufficient evidence** to show 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 of the AI system** in order to have a chance to pass the necessity requirement under Article 6(1)(e) GDPR.[8]

The two challenges are related and **raise the issue of AI training**. In order to know with reasonable certainty how effective an AI system will be in the real world, organisations willing to use AI need to train it beforehand, i.e., making it run the same processes as in the post-deployment scenario, but in a controlled environment. This process uses training data for the tool to develop its analytical capabilities based on the algorithm adopted. **The amount, quality, variability, and representativeness of data are amongst the most crucial variables conducive to an effective 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 'real-life' effectiveness rate** and the more likely it is to pass the necessity test.

Data regarding natural persons can be either personal data or anonymised data. The more personal identifiable information (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 anonymisation or even pseudonymisation – which does not strip the data of their personal character – contain more information than pseudo- or anonymised data. Therefore, in certain circumstances and depending on the level of granularity desired in the analytical capabilities of an AI system, **a system trained with anonymised and/or pseudonimised data might never be fully trained as effectively as with unaltered personal data**. However, the common practice in the AML/CFT industry and others is to pseudo- or anonymise the data to comply with the data minimisation principle, since the training phase can hardly be considered falling within the interests mentioned in the lawful ground (e.g., carry out a task in the public interest) that the data controllers would rely on after deploying the tool.

The question therefore arises as to **how can organisations such as obliged entities be expected to satisfy the necessity test of Articles 6(1) GDPR by demonstrating higher effectiveness of AI systems compared to traditional, non-AI analysis methods, if the data minimisation principle encourages them to anonymise training data?** With the rise of AI, **there appears to be a tension between the methodology of the necessity test** (that requires showing superior effectiveness) **and the constraints of the data minimsation principle in the AI training phase**. This challenge presented itself to one partner within the TRUSTS Consortium. 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 system is better than previous AML/CFT methods. However, because of the first challenge – related to the hesitation to use personal data in training – an obliged entity may never be able to obtain required level of confidence before deployment. Hence, it would attempt to justify the

[8] It is worth noting that obliged entities, and other organisations in a similar position, would need to pass the necessity test also under Article 6(b), (c), (d) and (f).

processing entailed by the AI system based (ideally) on Article 6(1)(e) GDPR surrounded by legal uncertainty as to whether the system would pass the necessity test.

To be sure, **in the DPIA the obliged entity can**, while thoroughly describing the measures aimed to reduce the risks of the processing, **provide strong safeguards against adverse effects of using the AI system in real life, hence increasing its chance to be lawful under data protection law**. **However**, this strategy is unlikely to solve the above issue. It can surely help controllers prove that the AI system is only to a limited extent more intrusive than non-AI data processing methods; but **controllers also need the other prong of the necessity test, i.e., to demonstrate that the AI system is more effective than the traditional methods**. In research **projects such as TRUSTS**, obliged entities may be able to rely on the GDPR regime for 'scientific research';[9] such projects **can contribute to advancing the state of the art within the 'research' umbrella more than it may be possible in ordinary business contexts**. However, the vast majority of AI training for AML and other purposes occur outside research projects.

One step towards making it easier for data controllers to properly train AI tools may be Article 10(5) of the proposed AI Act. This provision would enable providers of high-risk AI systems to process special categories of data if strictly necessary to monitor, detect and correct bias generated by AI. **The spirit of this provision may be inspirational as it recognises that some further data processing may be necessary to ensure that AI systems are effective *and* unbiased**. Still, this provision is limited to a very circumscribed scope. It is unlikely to provide the answer to the aforementioned challenge because: (i) it requires, in turn, a strict necessity test to be relied upon; (ii) it focuses specifically on special categories of personal data, and not in general on any kind of personal data necessary for AI training; (iii) it emphasises the need for safeguards including pseudo- or anonymisation (and rightfully so, given the sensitivity of the data concerned); and (iv) it can be relied on only by the provider of the AI system, which may not always correspond to the controller of the data processing.

Still, the spirit and logic of Article 10(5) may be leveraged to tackle the challenged described in this subsection. The normative question that arises is whether it should be envisaged to ease the requirements for processing personal data to train AI systems that could increase the utility of processing – i.e., in the AML case: increase the success rate in identifying ML and fraudulent transactions – and ultimately achieve to a higher degree the policy objective envisaged (such as combating ML and FT).

3.2.2 Recommendations

For stakeholders

- In line with the recommendations made under Section 3.1, obliged entities acting as data controllers should carry out thorough DPIAs before deploying AI systems for AML/CFT purposes. **Controllers shall implement in the design of the system, and document in the DPIA, the strongest possible safeguards against adverse effects of the system on data subjects** – such as how to ensure data minimisation; how to avoid automated decisions leading to legal or significant consequences; and how to avoid discrimination on several bases. **This exercise will help obliged entities comply with the necessity test under Article 6 GDPR**.

[9] As per Article 5(1)(b) GDPR.

- **Make the best efforts to measure the effectiveness of the current AML/CFT methods**[10] and technologies **in order to obtain a benchmark** to compare with the (approximate) effectiveness of the AI system developed.

For policymakers

- Within their current work on AI policy, and in an integrated approach with the EU's AML/CFT policy, the European Commission, the EDPB and the EDPS should reflect and focus, inter alia, on the perspective of the effectiveness of AI systems to achieve policy objectives vis-à-vis the effectiveness of 'traditional' procedures and methodologies.
- The European Commission should consider developing discussions together with national FIUs and other law enforcement authorities responsible for combating ML/FT in order to **explore pathways to making it easier for obliged entities to have feedback on the effectiveness rate of their AML/CFT monitoring**. This would provide obliged entities with more data to improve the effectiveness of their approaches, including when developing AI systems. **Such pathways should at all times keep in mind the need to keep confidential information crucial to law enforcement**.
- Following the above, the European Commission, the EDPS and the EDPB should consider reflecting on **whether the current set of soft law instruments on personal data processing provides sufficient legal certainty to controllers** willing to train and subsequently deploy AI systems and having to satisfy the necessity test under Article 6 GDPR. If widespread legal uncertainty is indeed remarked, thought should be put into **developing ad hoc guidance to tackle the potential tension between the necessity test and the current practice to implement the data minimisation principle in the context of AI training data**.

3.3 Notion of 'controllership'

The analysis concerns two main elements that may still lead to legal uncertainty concerning the notion of 'controllership' and 'joint controllership' in data marketplace ecosystems. As to the first element, related to 'horizontal' controllership, it may not always be clear **in which circumstances two or more entities performing data-driven collaboration with the support of a digital platform can qualify as joint controllers, or rather as sole controllers** for their own data processing operations.

As to the second element, related to 'vertical' controllership, it may not always be straightforward to **assess the role of the data marketplace platform in the attribution of data protection responsibilities**. **The platform-managing entity may or may not qualify as data controller – even jointly with**

[10] Although, due to the workflow between obliged entities and law enforcement authorities, the former are often in the dark as to what is the 'real' effectiveness rate of their AML/CFT monitoring activities. See e.g., Bertrand, A.; Maxwell, W.; Vamparys, X., *Do AI-based anti-money laundering (AML) systems violate European fundamental rights?*, International Data Privacy Law, 2021, Vol. 11, No. 3.

participating entities – depending on the degree of control and the participation in defining the purposes and means of the processing.

3.3.1 Description

The notion of 'data controller' and 'controllership' – i.e., the state of qualifying as data controller – are key in the breakdown of responsibilities under the EU data protection framework. They determine the organisation(s) responsible for complying with the obligations intended to protect the rights of the data subjects in the processing of personal data. As explained already in D6.2, the notion of controllership is a flexible notion that, for one, needs to be adapted to the context in which data processing operations are carried out;[11] and for two, is a particularly complex one to comprehend in today's online environments such as data marketplaces and data exchange platforms. This is the case even after the Court of Justice issued three landmark decisions in the *Wirtschaftsakademie*[12], *Jehovan's witnesses*,[13] and *Fashion ID*[14] cases and the European Data Protection Board (EDPB) issued updated guidelines in 2020 to reflect the implications of that case law.[15]

In the legal and ethical assessment of TRUSTS conducted in D6.3, several processing operations were analysed. These included operations envisaged to take place 'in real life' under the three main TRUSTS use cases, and operations conducted during the project by consortium partner to test the use cases (i.e., use case pilots). During this analysis, while the attribution of the controller role to the organisation initiating the data exchange was rather straightforward based on the components of the definition of 'data controller', **two elements still raised some doubts, i.e.: a) the attribution of 'joint controllership' to scenarios whereby two or more organisations are involved in the data exchange within the TRUSTS architecture (i.e., 'horizontal' joint controllership); and b) the role of the TRUSTS platform** – and hence of the entity envisaged to manage it – **in the attribution of the controllers' responsibilities**, potentially leading to joint controllership along with participating organisations (i.e., 'vertical' joint controllership).

3.3.1.1 'Horizontal' joint controllership

The first element essentially amounts to asking **whether and in which circumstances the participation of two or more organisations in data transfers and exchanges** (conducted with the help of the Federated Learning approach of TRUSTS) **gives rise to instances of joint controllership; and when, instead, each separate organisation should be regarded as sole controller for "its own" data processing operation(s)**.[16] In this respect, **with regard specifically to TRUSTS Use Case 2**,[17] it was argued that, to the extent that several organisations use the TRUSTS platform's application, downloaded on local premises, to anonymise

[11] In light of the case law of the Court of Justice and the guidance issued by the Article 29 Working Party in 2010, which already argued for a functional – rather than formal – approach to establishing who is the data controller.

[12] Case C-210/16, *Wirtschaftsakademie*, ECLI:EU:C:2018:388, 2018.

[13] Case C-25/17, *Jehovah's witnesses*, ECLI:EU:C:2018:551, 2018.

[14] Case C-40/17, *Fashion ID v Verbraucherzentrale NRW eV*, ECLI:EU:2018:1039, 2018.

[15] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Adopted on 7 July 2021, available at: eppb_guidelines_202007_controllerprocessor_final_en.pdf (europa.eu).

[16] This question stems, inter alia, from the acknowledgment by the EDPB that not all processing involving several entities give rise to joint controllership. See Guidelines 7/2020, para. 53.

[17] Agile marketing through data correlation. This reasoning may however apply to many other use cases deployable in the TRUSTS platform.

their own data sets, they would each qualify as sole data controller for that data processing operation. This is the case only insofar as these organisations would not simply share their anonymised data sets with a potentially wider community of participants, without there being already the intention to join forces and use each other's anonymised data sets for marketing purposes. In this case, **it can be submitted that there is neither a *common decision* nor two *converging decisions* of the several entities giving rise to joint determination of purposes and means,[18] because each organisation acts merely with the intention to make the anonymised data sets available to potential future collaborations** through the TRUSTS platform.

Conversely, it can be argued that, **insofar as two or more organisations decide to anonymise their individual data sets to provide data for a previously planned joint collaboration**, then the assessment would change. In this case, **each participating entity would act based on a common decision to pool their data and use them** for marketing purposes through the TRUSTS platform. This common decision would concern both the purpose of the processing – i.e., anonymisation with a view to making data available to each other – and the means of it – i.e., the use of the anonymisation application provided by the TRUSTS platform.

Still, this distinction is based on the interpretation of the Court's case law and the EDPB's Guidelines. It is to be noted that **none of the cases so far adjudicated by the Court, nor any of the EDPB's practical examples in the Guidelines, appear to match the workflow and dynamics observed in TRUSTS and, potentially, in other data marketplaces**.[19] Hence, **some degree of uncertainty as to the above assessment might nonetheless remain**. For instance, if one were to consider that the mere intent of each organisation to pool their data with others in the future, through their participation in TRUSTS, is considered as sufficient to prove a concerted action and hence the common decision to carry out the data processing operation – i.e., data anonymisation. This approach appears less convincing especially because it would be very difficult to even identify in practice the organisations which would then qualify as joint controllers: for instance, if twenty organisations separately decide to anonymise and share their data sets via the TRUSTS platform, and subsequently only five decide to pool their anonymised data together and perform data analytics on them, only ex post would it be possible to identify the subset of organisations that initiated a collaboration. This collaboration, however, was not commonly decided before the data processing operation began, and hence it would be difficult to argue for joint controllership.

Finally, another point that relates to 'horizontal' joint controllership concerns **actual vs. potential access to the data by the parties involved**. According to the above assessment two organisations may be regarded as joint controllers if their processing operations, while carried out on data to which the other party has no access to, are performed with a common goal. This assessment relies on the fact that the CJEU considered that access to the data at hand is not a necessary requirement for controllership.[20] This

[18] See Guidelines 7/2020, para. 54.

[19] The closest example is the 'Research project by institute' provided by the EDPB on p. 22. However, the key differences are a) that in the EDPB's example all the participating institutes decide to create the platform and participate in the data-drive collaboration, whereas in TRUSTS participating organisations may decide to merely share the data and only at a later stage cooperate with others based on those data; and b) that there is no separate entity managing the platform, whereas in TRUSTS the managing entity is functionally and formally separate from the participating organisations.

[20] Case C-210/16, *Wirtschaftsakademie*, cited supra, note 12.

idea was taken onboard by the EDPS in its Guidelines related to Regulation (EU) 2018/1725,[21] where it stated that the fact that a party does not have access to data allowing the identification of natural persons "does not influence the joint controllership situation";[22] and even more decisively by the EDPB in its 7/2020 Guidelines, where it stated that a party who has decisive influence over the purpose and means of the processing should qualify as controller "even though he or she will never have actual access to the data."[23] The EDPB formulation appears to exclude an interpretation of the case law that targeted actual access vs. potential access, i.e., that would qualify as controllers only those parties who *might* have access to the raw data at some point in the future although they did not *actually* have access to them at the time of processing.[24] **This state of play, that emphasises the intention of the parties** (towards co-deciding on the purposes and means) **rather than the factual reality** (access to, and thus control over, the data) **catches into the net of controllership virtually any organisation that participates in joint projects through TRUSTS and similar marketplaces**. By extending controller's responsibilities to data which they will never have access to, **such an approach appears also to run counter the very goal of TRUSTS-like experiences, i.e., to enable cooperation on data without granting access to each participant**.

3.3.1.2 The role of the platform and 'vertical' joint controllership

The second element highlighted above concerns the role of the platform that sits at the core of the ecosystem enabling data sharing – the TRUSTS platform in this case – along with the entity responsible for its management. Data processing operations such as those planned in the main TRUSTS use cases give rise to some uncertainty in light of the 'converging decisions' criterion adopted by the EDPB based on the Court's case law. **It could be argued**, for instance, that, although it does not actively participate in the decision of the organisation(s) to anonymise their data sets, **the TRUSTS platform would still qualify as a joint controller because of a) the overarching decision to enable data sharing, and b) its influence on the means used by the organisations**. By making the anonymisation application available for download and local use, it could be argued that TRUSTS complements the decision of the participating organisations, in that the processing as such would not be possible without both parties' participation in the purposes and the means of the processing.[25]

It can **however** be argued that this interpretation is not convincing. Although the decision by the TRUSTS managing entity to enable data exchanges and joint analysis goes in the same direction as the decision, by participating organisations, to anonymise data sets for those purposes, **it seems far-fetched to consider this convergence as an instance of converging decisions by two joint controllers**. This is, first, because the presence of converging decisions should be assessed by looking at the behaviour of the entities with regard to the specific data processing operation at hand; and second, because a different interpretation would automatically trigger joint controllership in any data processing operation conducted in the context of TRUSTS. It seems preferable, therefore, to consider that in these instances the TRUSTS entity does not participate in the determination of purposes of the specific data processing operation.

[21] EDPS, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 November 2019.
[22] Ibid., Section 5.1, p. 24.
[23] EDPB, 7/2020 Guidelines, para. 42, p. 16.
[24] See also Rossello, S., MUSKETEER, D2.6 Data ownership and data governance: policy recommendations for the legal framework, KU Leuven Center for IT & IP Law (CiTiP), 2019, Section 3.2.2, pp. 15-16.
[25] EDPB, 7/2020 Guidelines, para. 55.

What is left, then? **TRUSTS may be considered to participate in the determination of means by making available the anonymisation application**. This could qualify TRUSTS as participating jointly in the determination of the means **based on the Court's judgment in *Fashion ID***. In that case, the Court concluded that Fashion ID, by making available a 'Facebook Like' button to website users, had been a decisive factor in the processing operations concerning the users' personal data.[26] **However**, it could also be argued that the situation in TRUSTS is different from *Fashion ID* in that, strictly speaking, **the use by organisations of the TRUSTS-provided anonymisation application is not absolutely necessary for them to anonymise their data sets**.[27]

3.3.2 Recommendations

For stakeholders

- Both TRUSTS – and entities managing similar data marketplaces – and organisations willing to exchange data through the platform should **carefully consider their responsibilities with regard to the processing of personal data. They should keep in mind that anonymisation constitutes processing** and needs to be justified under Article 6 GDPR.
- The entities mentioned above should, by involving their Data Protection Officers (DPOs), map all the use cases and workflows envisaged by the processing of personal data; they should **cooperate with one another whenever the processing is envisaged to facilitate a collaboration or joint activities, agree on their mutual responsibilities, and draft appropriate arrangements if they conclude to be joint controllers** as per Article 26(1) GDPR.
- TRUSTS and the participating organisations should consider **mapping out typical real-life use cases in order to support possible initiatives by the EU institutions** aimed to clarify the application of rules on data controllership to data marketplaces.

For policymakers

- The European Commission, the EDPS and the EPBD should consider **reflecting on the complex set of data processing scenarios entailed by data marketplaces and consider issuing targeted guidance in line with the interpretation provided by the Court of Justice in its case law**. In particular, as a result, the EDPB should consider **adding ad-hoc examples on data marketplaces to its 7/2020 Guidelines**.
- The European Commission, the EDPS and the EPBD should consider the guidance on joint controllership and in particular the notion of 'access to the data' as not precluding controllership. **It would be advisable to clarify this notion and state that it applies only to those**

[26] C-40/17, *Fashion ID*, ECLI:EU:2018:1039, paras. 77-79. This would also match the description provided in the EDPB Guidelines at para. 64: "*It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing*." See also para. 65 mentioning the example of platforms.

[27] EDPB, 7/2020 Guidelines, para. 68: "[…] the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other."

situations where, although a party does not have access to the data at the time of the processing, it may still obtain access to and control over them in the future.

4 Recommendations in the EU data legal framework

Below we focus on challenges, open points and lessons learned that have emerged with regard to EU 'data law'. This term refers to legislation – including proposed legislation that has not yet entered into force – aimed to regulate and provide a governance structure to data markets and, more generally, data sharing. The section presents each point and, depending on which group is affected, provides recommendations to stakeholders and/or policymakers.

We focus on the following points:

- The applicability of the Data Governance Act (DGA)[28] to TRUSTS;
- The implications of the DGA for TRUSTS stakeholders;
- The DGA regime for international transfers of data;
- The role of data intermediation services in data exchanges envisaged by the Data Act Proposal;
- The obligation in the Data Act Proposal to make data available & its interplay with the fairness regime.

4.1 Scope of the Data Governance Act

Based on a joint reading of several provisions of the DGA, the analysis shows that **data marketplaces platforms such as TRUSTS are likely to fall within the scope of application of the DGA**. However, the DGA proposes **several criteria to identify data intermediation service (DIS) providers that are not require clarification to enhance legal certainty**.

4.1.1 Description

The first point worth discussing in relation to EU data governance law is **the scope of application of the Data Governance Act** (DGA). It is worth noting that the DGA introduces a set of harmonised conditions and obligations to enable DSSs to facilitate data sharing, while enhancing the control of natural and legal persons over their data.[29] This policy rationale **matches the core identity and purpose of TRUSTS, which is to lead to a trust-based ecosystem of data exchanges and data-driven collaboration for value creation within the EU**.

D6.3 "Legal and Ethical Assessment" provided an analysis of the applicability of the DGA to TRUSTS based on the former DGA Proposal by the European Commission. It was argued that, based on the definitions provided in Article 9 of the proposal, read jointly with Recital 22, TRUSTS may or may not be considered as falling within the scope *ratione personae* of the proposal as a data sharing service (DSS) provider depending on the use case at hand.

[28] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724.

[29] DGA Proposal, Recital 22.

The adoption of the DGA on 30 May 2022, with significant amendments compared to the initial proposal, calls for a different analysis. However, one criterion mentioned in former Recital 22 was adopted in the text of the adopted Regulation, notably in Article 2(11), which provides the definition of the concept of 'data intermediation service' (DIS). DIS is to be understood as:

> *'a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, excluding at least the following:*
>
> *(a) services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users;*
>
> *(b) services that focus on the intermediation of copyright-protected content;*
>
> *(c) services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things;*
>
> *(d) data sharing services offered by public sector bodies that do not aim to establish commercial relationships.'*

It is worth focusing first on the grounds of exclusion.[30]

Article 2(11)(a). Based on this ground, introduced with a similar wording in Recital 22 of the former proposal, **whenever a platform such as TRUSTS ingests and transforms data obtained from a data holder and provides them to a data user, it should not be considered as a DIS provider**. In this scenario, the data holder and data user would enter into separate contractual relationships with TRUSTS but not between each other. The possible use cases of the TRUSTS platform do envisage such dynamics: an organisation may share (part of) its data set to TRUSTS with a view to extracting monetary value from it at a later stage, without directly transacting with another organisation seeking to obtain the data set.[31] **This might lead to consider TRUSTS as falling outside the scope of the DGA *only* in relation to this specific scenario**. Such a possibility would then make TRUSTS a particular case of an entity that may or may not be considered as a DIS provider depending on the case at hand (see below 'General definition').

Article 2(11)(b). This ground of exclusion can be understood as meaning that DIS providers whose main activity is to obtain, transform and redistribute content protected by copyright fall outside the scope of the DGA. **Whilst TRUSTS envisages to handle copyright-protected data, it cannot be argued that its main focus or activity is linked to such type of content**. Therefore, it cannot be said that TRUSTS falls outside of the scope of the DGA based on Article 2(11)(b).

[30] We do not focus on Article 2(11)(d) as it is manifestly irrelevant to TRUSTS.

[31] In this case, the data user would subscribe a smart contract with TRUSTS and have access to the data set (already available on the TRUSTS platform) covered by that smart contract.

Article 2(11)(c). **This ground of exclusion is also not applicable to TRUSTS, although the vagueness of its formulation may not foster legal certainty**. First, while it is clear that TRUSTS is not a service 'exclusively used by one data holder' (because it is designed to pool data from multiple data holders), more problematic is the concept of 'multiple legal persons in a closed group'. It is not entirely clear what is meant by 'closed group'; not just in relation to the size of the group at hand, but also because the definition mentions, as an example, 'collaborations established by contract'. The term may therefore refer to clearly circumscribed pools of organisations that have decided to cooperate with one another and – although not a necessary condition – to regulate their activities via a contract.

From a literal reading of this formulation, it can be argued that the activities promoted by TRUSTS are indeed collaborations (between data holders and users) grounded on contracts, namely – in the case of TRUSTS – contracts executed via blockchain. From a less formalistic and more substantive point of view, however, it can be argued that this ground is not meant to apply to data sharing platforms such as TRUSTS. The Regulation then refers '*in particular*' to collaborations focusing on ensuring the functionalities of IoT devices. TRUSTS would not be the provider of services for such collaborations, and while the term 'in particular' does not formally rule out the applicability of this ground of exclusion to TRUSTS, **it can be argued that the spirit of this provision is to cover service providers handled by a limited number of entities involved in an IoT-related ecosystem**, such as manufacturer(s), software developers, users, etc., i.e., scenarios that are envisaged to fall within the scope of the Data Act Proposal (see further below). Still, **the ground of exclusion is not crystal-clear and may be the source of some legal uncertainty as to which service providers are the real target of the provision**.

General definition. After considering the grounds of exclusion of Article 2(11), we focus on the definition of DIS provider, based both on Article 2(11) – spelled out above – and Article 10 DGA, which designates those services that are subject to the conditions laid down in the Regulation. Article 10 states that these services are:

> *(a) intermediation services between data holders and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data, as well as the establishment of other specific infrastructure for the interconnection of data holders with data users;*
>
> *(b) intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make non-personal data available, and potential data users, including making available the technical or other means to enable such services, and in particular enabling the exercise of the data subjects' rights provided in Regulation (EU) 2016/679;*
>
> *(c) services of data cooperatives.*

This section will not focus on letters b) and c) as they are manifestly irrelevant to TRUSTS. It is worth focusing instead on letter a) and reading it jointly with Article 2(11) to extract a comprehensive 'combined' definition of DIS provider for the purposes of the DGA. The main criteria of this definition purport that a DIS provider:

- *Aims to establish commercial relationships* (Article 2(11)): This is undoubtedly the purpose of TRUSTS and similar data marketplace platforms; in that it encourages the pooling of resources between companies seeking to obtain profit from shared collaborations over data;

- *Enables relationships between data holders and data users* (Article 10(a)): Related to the above criterion, TRUSTS does indeed target communities of data holders seeking to share their data sets and potentially collaborate on them; and communities of companies and other organisations seeking to benefit from the added value of those data;
- *For the purposes of data sharing* (Article 2(11)): Inherent to the commercial purpose of TRUSTS is the purpose of encouraging data sharing across organisations, both personal data (duly anonymised) and non-personal data;
- *Between an undetermined number of data subjects and data holders on the one hand and data users on the other* (Article 2(11)): This criterion focuses on the 'undetermined' number of actors. This is exactly the population targeted by TRUSTS, which is open to potentially any company or organisation interested in sharing and/or obtaining data. The term 'undetermined' also arguably marks a conceptual difference from the term 'closed group' mentioned in Article 2(11)(c), further dismissing the relevance of that provision for TRUSTS;
- *Through technical, legal or other means* (Article 2(11)): This criterion is rather open. TRUSTS does satisfy the two specified means as it offers both technical means – including a digital platform to browse data sets and find collaboration partners, anonymisation applications, AML services and applications, etc. – and legal means – mainly in the form of smart contracts to regulate transactions between data holders and users;
- *Including making available the technical or other means* (Article 10(a)): This is a more specific version of the above criterion, which TRUSTS, as explained above, does satisfy.
- *Those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data* (Article 10(a)): This criterion is purely optional, but TRUSTS does fall within all its possibilities, because: it enables data sharing to occur between two or more participants; it implies the creation and usage of a digital platform, as mentioned under the above criterion; and it enables not only the exchange but also the joint use, in the form of collaboration and value extraction through technical means (data analytics, federated learning, etc.) by the participating organisations.

Based on the above considerations, it can be argued that **TRUSTS satisfies all the basic criteria of the definition of provider of DIS**, and in particular – under Article 10(a) DGA – for the purposes of the conditions laid down in the DGA for the operation of its services (see below Section 4.2). This conclusion leads to consider again the observation, made above about Article 2(11)(a), that in the specific scenario envisaged in that provision (i.e., data sharing without direct relationships between data holders and data users) TRUSTS would not be considered as a DIS provider. **The Regulation appears to be keeping two instances distinct from one another: on the one hand, the case of a data sharing service between several data holders and users** providing technical, legal or other means (Articles 2(11) and 10 DGA); **and, on the other hand, the case of a data sharing service that *excludes* direct relationships between data holders and data users** (Article 2(11)(a)). It can be argued that TRUSTS is one example of data sharing service provider that merges the two scenarios into one single entity. Put differently, **both scenarios may play out under TRUSTS depending on the use case. Arguably, this is a likely situation for many, if not most, data marketplace platforms following a similar blueprint as TRUSTS. It appears therefore artificial to spell out as mutually exclusive two scenarios that can, in actuality, coexist**.

Based on the general applicability of the concept of DIS to TRUSTS, **it is therefore not clear what would be the practical consequence of Article 2(11)(a) on TRUSTS and similar platforms**. One approach, based on a formalistic reading of the Regulation, could entail excluding the application of the DGA to TRUSTS and similar platforms whenever it acts within the situation envisaged by Article 2(11)(a). Such an approach might however sit at odds with the spirit of the Regulation itself, which – according to the above reasoning – seeks to target data marketplaces as one example of DIS providers. In this regard, it appears more sensible to read Article 2(11)(a) as applying to those entity whose only or essential activities fall within the formulation of that article (i.e., providing services without bridging data holders and data users). As long as an entity such as a data marketplace does instead provide connections between these groups of actors in other instances, it would qualify a DIS provider and, as such, be subject by rule to the legal regime of Chapter III. **Given that the conditions for DIS providers apply *ratione personae*, it appears more reasonable to consider in principle data marketplaces as DIS providers, regardless of whether they do, in some instances, provide services within the meaning of Article 2(11)(a)**.

4.1.2 Recommendations

For stakeholders

- TRUSTS and other entities managing similar data marketplaces **should consider the DGA provisions on DIS providers as in principle applicable to them insofar as they satisfy the definition of Articles 2(11) and 10 DGA.**
- Data marketplaces should operate based on the understanding that, if they satisfy this definition, **they are subject to the conditions of Chapter III DGA regardless of whether they do engage, in some instances, in the activities referred to in Article 2(11)(a)**.

For policymakers

- The European Commission should consider issuing guidance to **provide examples as to the type of entities falling within the definition of DIS providers**, especially with regard to data marketplaces. It would be advisable that the guidance **clarifies that data marketplaces generally fall within this definition** as per the reasons set out in this section.
- The European Commission should consider providing guidance on the effect of Article 2(11)(a) on certain data marketplaces that, while being generally subject to the regime of Chapter III DGA, may not qualify as DIS providers when performing the activities referred to in that Article. It would be advisable to provide clarity as to the legal regime applying to data marketplaces in such situations, and state that **data marketplaces that satisfy the requirements of the definition in Articles 2(11) and 10, qualify as DIS providers regardless of whether they engage, in some instances, in the activities referred to in Article 2(11)(a)**.
- The European Commission should consider clarifying the third ground of exclusion of Article 2(11) DGA, namely letter (c), in particular in relation to the structure and envisaged group of participants of data marketplaces such as TRUSTS. It would be advisable to clarify that **the notion of 'closed groups' generally excludes the potentially indeterminate number of organisations willing to participate in data marketplaces**.

4.2 Implications of the DGA for TRUSTS stakeholders

Having clarified that the DGA is likely to apply to TRUSTS and similar platforms, it is submitted that **the implications of the DGA are far-reaching**, as its conditions may affect the very right of DIS providers to provide services on the market. **The implications and breadth of these conditions is, however, not always clear, as shown by the concept of 'neutrality' of DIS providers.**

4.2.1 Description

Having discussed the challenges related to the applicability of the DGA to TRUSTS and similar data marketplaces, the next point concerns **the implications of the DGA for the TRUSTS managing entity and ecosystem**. It was observed in Section 4.1 that the DGA, as well as TRUSTS, aim to foster trust in data transactions and data sharing. **Trust can be considered as the 'glue' between two potentially conflicting interests (both at the core of the DGA's spirit) – i.e., the facilitation of data flows and the increased control by data holders over their data**. In this sense, trust is understood as a link between data users and data holders that goes beyond the 'mere' regulatory efforts but that, in the intentions of the Commission, is intended to be facilitated by regulation.

In the eyes of the Commission, **one key vehicle for creating and enhancing trust in the data marketplace ecosystem is *neutrality***. The DGA states that "*A key element by which to increase the trust and control of data holders, data subjects and data users in data intermediation services is the neutrality of data intermediation services providers with regard to the data exchanged between data holders or data subjects and data users*."[32] While the basic understanding of the term 'neutrality' is clear in the sense that suggests impartiality and absence of manipulation by the subject supposed to be neutral, the articulation of this concept and its practical implications in this area are far from straightforward. The DGA also explains that from the idea of neutrality it follows that DIS providers need to "*act only as intermediaries in the transactions, and do not use the data exchanged for any other purpose*".[33] One consequence of this idea, in particular the ban on 'using the data for any other purpose', is that DIS providers need to abstain from exploiting their unique position of middle ground between data users and data holders, and from using the data transiting via their servers to pursue their own (commercial) interests. Recital 33, echoed by Article 12(a), builds a prohibition for DIS providers on 'cross-usage' of data, i.e., the usage of data obtained in a transaction within one market to pursue different commercial interests in another market.

There are a few aspects of this idea that deserve discussion. First, the breadth and conceptualisation of the concept of 'neutrality'; second, the extent to which this neutrality obligation is envisaged to be effective.

As to the first aspect, it is worth exploring **how to conceptualise the neutrality obligation on DIS providers**, i.e., the prohibition to use the data for any other purpose: **Is it to be read literally, as meaning that DIS providers should do nothing more than merely allowing the transition of data between two or more parties?** This reading would make the concept of neutrality in this area closely resemble that of 'neutrality'

[32] Recital 33 DGA, echoed in Article 12(a).

[33] Recital 33 DGA.

in the e-Commerce Directive addressed to information society services acting as intermediaries,[34] whereby intermediaries are to provide a service of merely technical and automatic nature, that only allows for the transit of data. This interpretation may seem to conflict with the idea conveyed by the DGA, according to which DIS providers *"should be allowed to adapt the data exchanged in order to improve the usability of the data by the data user where the data user so desires, or to improve interoperability by, for example, converting the data into specific formats*."[35] This sentence suggests a more active role to be potentially played by DIS providers over the data exchanged; however, the conflict may turn out to be more limited than expected: Recital 32 suggests that this active role by DIS providers is subject to the will of the data user, i.e., triggers the role of the freedom to contract of all parties involved. By contrast, the obligation to remain neutral is not conditional, i.e., seems to be the by-default scenario in which DIS providers will have to operate, and that can be excepted only when the other contracting party (data user) accepts to receive a more articulate service from the DIS provider. This reading would also place autonomy and control on the data user, which would be more empowered vis-à-vis the DIS providers than in a scenario where the latter could take the initiative to make adaptations to the data. Still, **it can be argued that the concept of neutrality in the DGA deserves more specification and analysis to comprehend its breadth and implications**.

As to the second aspect, it is worth exploring the extent to which such a negative obligation is likely to significantly increase trust compared to a scenario whereby DIS providers were not subject to it, and were only limited in their use of other parties' data by existing rules, such as data protection law, legislation on trade secrets, intellectual property law, private contracts between parties, etc. The principle of freedom of contract allows data holders, data users, and data exchange platforms to potentially agree on subsequent use of the data exchanged – insofar as in line with applicable EU and national law; at the same time, applicable law already restricts the choice of different actors as to what they can do with the data being exchanged, depending on whether they are dealing with personal data, data covered by intellectual property rights, etc. **It could** therefore **be argued that the existing set of rules – on top of the DGA – already mandates a certain degree of neutrality for data exchange intermediaries, which leads to the question as to how significant the trust-enhancing effect of the neutrality obligation in the DGA can be in practice**.

With this mindset, **the set of conditions and obligations laid down in the DGA is likely to have major implications in terms of sanctions stemming from their nature and intensity**. The DGA itself highlights the conditional nature of many of its provisions directed at DIS providers, in particular in Article 12, which recites "conditions for providing data intermediation services". The conditions listed in Articles 11 and 12, on top of the neutrality obligation and the prohibition on cross-usage of data, concern the notification obligation;[36] the obligation to appoint a legal representative in the EU (for DIS providers established outside of the EU);[37] the separate entity requirement;[38] the need to ensure fair, transparent and non-

[34] Baloup, J.; Bayamlıoğlu, E.; Benmayor, A.; Ducuing, C.; Dutkiewicz, L., Lalova, T.; Miadzvetskaya, Y.; Peeters, B., *White Paper on the Data Governance Act*, CiTiP Working Paper 2021, KU Leuven Centre for IT & IP Law – imec, 23 June 2021, p. 31.

[35] Recital 32 DGA.

[36] Article 11(1) DGA.

[37] Article 11(3) DGA.

[38] Article 12(1) DGA.

discriminatory access to the service;[39] procedures to prevent fraud and abuse;[40] measures to prevent unlawful transfers of non-personal data;[41] and measures to guarantee the security of storage and transmission of such data.[42] This set of conditions includes measures usually found in ex-post competition law decisions (such as the structural separation of an undertaking into two separate legal entities) and in ex-ante regulation of utilities service providers, and appears overall to be a particularly stringent set of requirements for DIS providers to be authorised to provide services.

4.2.2 Recommendations

For stakeholders

- TRUSTS and other entities managing similar data marketplaces should adopt the necessary **technical and organisational measures to ensure and boost trust in participating organisation** (such as TRUSTS' dataspace connector, federated learning model, and smart contracts system for transactions) **and to ensure an objective, unbiased handling of the data shared**. They should in particular **design their business model in such a way as it does not conflict with the obligation to minimise their influence over the data** being exchanged via the marketplace.

For policymakers

- The European Commission **should consider issuing guidance on the notion of 'neutrality' as an obligation for DIS providers**. It is advisable to clarify that **the obligation to be neutral does not imply that DIS providers can be nothing more than mere transient entities between data holders and data users**; it should be acknowledged that DIS providers can offer a vast range of data-enhancing services to enable organisations to extract value from data. To better comprehend the notion of 'neutrality', it would be advisable to **provide a non-exhaustive list of practices that are allowed and prohibited to DIS providers**.

[39] Article 12(f) DGA.

[40] Article 12(g) DGA.

[41] Article 12(j) DGA. See also below, Section 4.3.

[42] Article 12(l) DGA.

4.3 International transfers of data

The DGA may not provide sufficiently detailed criteria and guidance to data intermediation services confronted with foreign requests for transfer of/access to non-personal data. This may be a crucial challenge especially **when IPR-protected data and trade secrets are involved**: data intermediation services are *de facto* asked to **perform a self-assessment of the foreign requests.** The lack of guidance is aggravated by potential **legal uncertainty on the applicable law between the DGA and the GDPR**.

4.3.1 Description

Article 31 of the DGA has introduced a regime to protect non-personal data held inter alia by data intermediation services (such as platforms like TRUSTS) from international transfers and requests for access by non-EU/EEA governments that may prejudice compliance with EU law or relevant national law.[43] With this regime, the DGA aims to complement the EU law protection granted to personal data against potentially unlawful international transfers (Articles 44-50 GDPR) by covering non-personal data that may be subject to intellectual property (IP) rights and/or constitute trade secrets. This regime is therefore quite relevant to organisations participating in TRUSTS and similar marketplaces, since they may well engage in and/or facilitate transactions entailing the sharing of (parts of) data sets that include commercially sensitive information and/or trade secrets. The Data Act Proposal (see below) aims to further enhance this regime with provisions that are very similar to those of the DGA, and apply to data processing services (i.e., cloud computing services).[44]

The regime introduced by Article 31 DGA may give rise to legal uncertainty and place data intermediation services[45] in a delicate position. Unless the transfer or access is requested within an existing international agreement between the third country and the EU or a Member State, data intermediation services would need to perform potentially intricate assessments in two subsequent steps: (i) decide whether compliance with the request for access/transfer would jeopardise compliance with EU or national law; and (ii) in the affirmative scenario, decide whether or not to grant access/make the transfer based on the criteria of Article 31. The paragraph below analyses both steps individually.

Decision on risk for compliance with EU or national law. Article 31(3) DGA enumerates the conditions under which the data intermediation service can decide whether to make the transfer/grant access to the third-country requestor. However, before that, Article 31(3) states that these conditions apply when the data intermediation service is the addressee of the decision by the third country "*and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State*." Only if that is the case should data intermediation services apply the three conditions. This implies that **DIS providers are required to assess first whether compliance with the third-country**

[43] Article 31 DGA, "International access and transfer".

[44] Article 27 of the Data Act Proposal. See on this Baloup, J., *Chapter VII of the Data Act – GDPR-like rules imposed on cloud services providers regarding protected non-personal data*, in Ducuing, C.; Margoni, T.; Schirru, L. (eds), *White Paper on the Data Act Proposal*, Center for IT & IP Law (CiTiP) Working Paper Series 2022, pp. 66-70.

[45] And public sector bodies (PSBs), natural or legal persons to which the right to re-use data was granted under Chapter II, or data altruism organisations. The section focuses only on data intermediation services as it is aimed notably at the TRUSTS platform, but its conclusions may apply, *mutatis mutandis*, to the above-mentioned entities as well.

decision would entail breaching an obligation under EU or national law. Whilst this assessment reflects Article 31(1) requiring data intermediation services to possess the legal, technical and operational resources to prevent possibly unlawful data transfers/access, **assessments such as this may not always be straightforward**. They require at the very least in-depth legal expertise in the EU and/or national provisions and case law whose breach may be caused by complying with the request.

Decision to make the transfer/grant access. Once **the DIS provider** concludes that compliance with the third-country decision can give rise to breaches with EU or national law, it **may give effect to the request only if sufficient rule of law safeguards are in place, subject to three conditions**: (i) the third-country decision needs to be subject to requirements of proportionality, transparency as to its reasons, and specificity; (ii) the law of the third-country needs to provide for a judicial authority to review a possible reasoned objection by the data intermediation service; and (iii) under the law of the third country, this foreign judicial authority needs to be empowered to take into account the interests of the data provider.[46] **These conditions are cumulative and arguably not straightforward to apply in practice** due to the following reasons:

- First, in general, not only does **this set of conditions require DIS providers** to perform a comprehensive assessment of the law of the third country in question; it also asks them **to make a subjective assessment as to whether the requirements of proportionality and statement of reasons in the decision issued by the third-country authority are satisfactory**. This can be quite challenging in practice absent guidance or standards to rely on: (i) in relation to stating the reasons of a decision, given that judicial practice in some EU Member States does not always sanction lack of provided reasons in judicial decisions, DIS providers might consider as appropriate foreign rules that pay mere lip service to the obligation to provide reasons; (ii) in relation to proportionality, it may also be challenging to ascertain whether the foreign law mandates proportionality to be set out in the decision, and if the decision actually does so;
- Second, the third condition can be subject to criticism with regard to the minimum required standards for the taking into account of the data provider's interest by foreign courts. The DGA merely requires the law of the third country to *empower* its courts to take those interests into account, implying that the courts might not actually do so absent a legal obligation in its domestic law. **This can represent a threat to a fair and comprehensive considerations of the provider's interests in rejecting the request**, **especially as these interests are – in the spirit of the Regulation – linked to ensuring compliance with EU or national law**. Moreover, the 'empowerment' standard may be difficult to ascertain in practice: even if third-country law were to be silent on this matter, one might be able to argue that it does *empower* courts to take the provider's interests into account, as long as it does not *forbid* them to do so.

It is worth noting that the current Data Act Proposal introduces a very similar regime for data processing services to that of the DGA; it differs, however, from the DGA in that it enables the addressee of the third-country decision to "*ask the opinion of the relevant competent bodies or authorities […] in order to*

[46] Article 31(3) DGA.

determine whether these conditions are met".[47] This possibility was mentioned in Article 31 DGA but subsequently expunged.

On top of the above-mentioned challenges, **an additional issue concerns the interplay of Article 31 with the GDPR regime governing international transfers (notably Article 48)**. Not only are personal and non-personal data often stored together in 'mixed' data sets;[48] they are also increasingly hard to clearly distinguish. **This can lead to legal uncertainty for data intermediation services as to which rules** – Article 48 GDPR or Article 31 DGA – **would apply to each specific case**. Considering moreover the interpretation issues of Article 48 still left open,[49] the question of the scope of application may not help data intermediation services to reach desirable compliance.

In this regard, it can be argued that the need to not prejudice the protection of personal data in any circumstance might actually guide the choice of applicable law by data intermediation services. Article 1(3) DGA provides that the DGA is without prejudice to the GDPR and data protection rules, and introduces a primacy clause for data protection law above the DGA itself in case of conflict. The Free Flow of Data Regulation (FFDR)[50] and the Data Act Proposal[51] also apply without prejudice to the GDPR. How can these clauses be helpful? Large data sets storing data that can be combined in several ways may *de facto* enable – albeit indirectly – the identification of natural persons, regardless of whether they include data that indisputably qualifies as personal data. It can be very hard for DIS providers – or any data holder for that matter – to be reasonably certain of the opposite in a given situation. Therefore, **in practice, data sets that contain several categories of data, especially where they contain at least some personal data, may end up being handled in compliance with the stricter regulation, i.e., the legal framework on personal data**, in order to avoid penalties. **However**, it needs to be stressed that, **whilst this is likely to be the safest choice for DIS providers in practice, it does not detract from the need for greater consistency between the GDPR and DGA regimes on international transfers**. **Otherwise, not only would legal uncertainty persist, but the DGA regime might risk becoming less and less relevant if DIS providers were to consistently follow the GDPR regime as a result of a 'playing it safe' approach and not of an informed substantive assessment**.

4.3.2 Recommendations

For stakeholders

[47] Data Act Proposal, Article 27(3). In the latest round of amendments by the European Parliament, an amendment was suggested that would subject the acceptance of the request only to a review by the competent bodies or authorities to assess if the three conditions are met. See Draft report by Pilar del Castillo Vera (PE732.704v01-00), 2022/0047(COD) of 14 November 2022, Amendment 1008.

[48] As recognised by the Free Flow of Data Regulation (FFDR), Article 2(2). Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[49] In particular, the "without prejudice" clause of Article 48, according to which the basic rule allowing for foreign requests for access/transfer to be enforceable only if they are based on international agreements, is 'without prejudice' to other grounds for transfer mentioned in Chapter V GDPR.

[50] Article 2(2) FFDR.

[51] Data Act Proposal, Article 1(3).

- In line with Article 31(1) DGA, TRUSTS and other entities managing similar data marketplaces should consider equipping themselves with **appropriate expertise in the subject matters mentioned in Article 31(3) in order to take the decision referred to in that article**.

For policymakers

- The European Commission should consider reflecting on the implications of Article 31(3) DGA in terms of the tasks DIS providers need to carry out to make a decision on the request for access/transfer of data. It would be advisable to **consider providing for an optional advisory mechanism** – such as the one initially referred to in the proposed text – that DIS providers can rely on **to reduce the uncertainty and avoid taking ill-informed decisions on complex substantive matters of rule of law in third countries**.
- The European Commission, the EPBD and the EDPS should consider issuing guidance to **ensure alignment between the interpretation of Article 31 DGA and that of Article 48 GDPR with regard to the distinction between personal and non-personal** data and the regime applicable to specific situations.

4.4 Role of data intermediation services in the Data Act Proposal

The Data Act Proposal could do more to enable DIS providers under the DGA to play a facilitator role in the legal regime laid down in Chapter II of the Act, specifically as chosen 'third parties'. At the same time, in order for **DIS providers** to effectively play such a role, they **should be regarded as neutral and trustworthy parties by data holders and users**. **This outcome** may not be straightforward as it **will depend on the DIS providers' ability to accommodate their commercial interest as undertakings with the neutrality expectations** under the DGA and the Data Act.

4.4.1 Description

On 23 February 2022 the European Commission presented a legislative proposal for a Regulation on fair access to and use of data: the 'Data Act' Proposal.[52] **The proposal aims to introduce general rules with a view to facilitating the creation and strengthening of an EU-wide common market for data, seen as pre-condition for the creation of EU-wide data spaces. The concept of 'data space' is particularly relevant to TRUSTS in the light of the Commission's definition**: data spaces shall include: ""(i) the deployment of data sharing tools and services for the pooling, processing and sharing of data by an open number of organisations, as well as the federation of energy-efficient and trustworthy cloud capacities and related

[52] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). COM/2022/68 final.

services", (ii) data governance structures […]" and they will aim at "(iii) improving the availability, quality and interoperability of data […]".[53]

Both in terms of means – i.e., making available data pooling and processing tools – and goals – i.e., enabling organisations to produce and obtain higher value from the data, **the TRUSTS project responds to this regulatory objective**. While the three use cases developed during the project do not immediately involve data generated by products in an Internet of Things (IoT) environment, **the TRUSTS platform can cater to business opportunities for holders of IoT-generated data willing to pool these data together**. It is under this lens that the Data Act becomes relevant for TRUSTS and the participating organisations. More specifically, TRUSTS can allow for the participation of: (i) organisations that collect data generated by IoT devices, and who would qualify as 'data holders';[54] and (ii) organisations that are interested in receiving these data, and who would qualify as 'data recipients'.[55] In this framework, TRUSTS would still qualify as a data intermediation service within the meaning of the DGA.

The Data Act Proposal can be seen as an attempt to complement the logic of the DGA.[56] It follows that **the interaction between the DGA and the envisaged Data Act could be instrumental to achieving the overall goals of the EU's digital regulation strategy. And yet, the current version of the Data Act Proposal does not appear to fully recognise the potential of DIS providers** (within the meaning of the DGA) **in facilitating the relationships between data holders and data users**. Chapter II of the Data Act Proposal illustrates this point. It lays down the set of rights and obligations of the various stakeholders targeted by the Data Act. The architecture of Chapter II is, on the one hand, 'bilateral' in that it firmly sits on the interaction between the data holder and the data user; on the other hand, it introduces the notion of 'third party' as data recipient chosen by the user.[57] Entities qualifying as DIS providers under the DGA and that have proved to be trustworthy intermediaries might play the role of third parties and hence act as facilitators to the legal regime envisaged in Chapter II. **The Data Act lacks** however **the 'connective tissue'** with the DGA in this regard: i**ts provisions do not seem to be designed to emphasise the potential role that DIS providers have to play in the fair allocation of data amongst holders and users**.[58]

On the one hand, therefore, it can be argued that the current version of the Data Act is a missed opportunity when it comes to leveraging the efforts made in other areas of the EU's digital regulation. On the other hand, however, if **the decision** is taken **to consider the role of DIS providers more prominently within the scope of the Data Act**, the EU legislator **should pay attention to** one aspect in particular: **the balance between the commercial interests and the trust-enhancing neutrality expectations of DIS providers**. One key requirement to promoting the reliance on DGA-based DIS providers as third parties for the purposes of the Data Act is the existence of trust in the DIS providers' ability to comply with the obligations set out in Article 6 of the Data Act Proposal. Article 6, however, prohibits third parties from carrying out activities that, from a purely commercial perspective, may well fall within the core interests

[53] Commission Staff Working Document on Common European Data Spaces, SWD (2022) 45 final, 23.2.2022, Section 2.

[54] Data Act Proposal, Article 2(6).

[55] Ibid., Article 2(7).

[56] Ducuing, C.; Margoni, T., *Analysis of the Data Act Proposal: Overall structure*, in Ducuing, C.; Margoni, T.; Schirru, L. (eds), *White Paper on the Data Act Proposal*, Center for IT & IP Law (CiTiP) Working Paper Series 2022, p. 20.

[57] Data Act Proposal, Article 5.

[58] See also Ducuing, C.; Schirru, L.; De Noyette, E.; Margoni, T., *The role of data intermediaries: Missed opportunity?*, in Ducuing, C.; Margoni, T.; Schirru, L. (eds), *White Paper on the Data Act Proposal*, Center for IT & IP Law (CiTiP) Working Paper Series 2022.

of a DIS provider, such as TRUSTS or similar data marketplaces. In particular, Article 6 prohibits third parties from:

- *Making the received data available to another third party, in whatever form*. This prohibition already limits the data sharing potential of data marketplaces by constraining the reception of data to the needs and goals of the user alone. The proposed text introduces this limitation for good reasons, i.e., to safeguard the user and to protect the rights of the data holder. However, in doing so, it envisages a 'closed-loop' relationship between the third party (potentially a DIS provider), the data holder and the data user. Whilst TRUSTS and similar data marketplaces are open to acting as intermediaries between just two entities, it remains to be seen whether DIS providers on a larger scale will have a business interest in acting as intermediaries within the meaning of Chapter II of the Data Act, or if they will seek scenarios fostering more open collaboration and value creation of data amongst several participants. At the same time, it is not guaranteed that data users (especially data subjects) will be encouraged to resort to DIS providers as third parties. **The extent to which DIS providers honour the neutrality obligations of the DGA and become transparent and trustworthy intermediaries is likely to be key** to them playing a role in the dynamics governed by Chapter II of the Data Act.
- *Using the data to develop a competing product or sharing the data with another party for that purpose*. This prohibition rightfully intends to protect the data holder's right to a distortion of competition channelled through the participation of a third party. At the same time, it may act as a limitation to the general offer of services by data marketplaces to potential participants: Joint collaborations of undertakings around commonly shared data sets (still in compliance with relevant legislation) inherently open to the possibility that individual participants gain value from those data sets and use this value for their own commercial interests, including developing their own products or services. **It remains** therefore **to be seen to what extent DIS providers will see business opportunities in handling Data Act-based relationships vis-à-vis other, more open data sharing projects**.

Whilst neutrality is likely to play a key role in both of the above instances, **it might not be straightforward to encourage DIS providers to strike a sensible balance between their commercial nature and the neutrality and trustworthiness expected of them** from the DGA regime but also – in this particular case – from the 'third party' notion of the Data Act. It can be argued that **this balancing is one of the cornerstones of the overall regulation of digital intermediaries, both individually under the DGA regime, and in general when considering all (proposed and in force) pieces of legislation operating together**.

4.4.2 Recommendations

For stakeholders

- In a similar vein to the recommendations made in Section 4.2.2, TRUSTS and other entities managing similar data marketplaces should take the appropriate measures to ensure their neutrality vis-à-vis the data exchanged via their platform, and **explore the opportunity to present themselves as trustworthy partners to be chosen as third parties by data users** under Chapter II of the Data Act Proposal.

For policymakers

- The European Commission should consider initiating talks with the data and digital community, in particular involving representatives of data marketplaces and of IoT-related products and services, to **discuss the role of the former in facilitating the regime of Chapter II of the Data Act**.
- In case of positive feedback on the role of DIS providers, the European Commission should consider **amending the Data Act Proposal to strengthen their role in the interactions envisaged in Chapter II of the Data Act.** For instance, the Proposal might **create suitable incentives for data users to choose trusted DIS providers as third parties responsible for processing the data in the interest of data users**, and avoid situations whereby this role is played by data holders, who may exhibit a conflict of interest vis-à-vis this operation.

4.5 Obligation to make data available & fairness of contractual terms

The Data Act provisions on statutory obligations (Article 8) make references to the fairness rules (Article 13) for SMEs, potentially creating **legal uncertainty as to exact scope of these obligations, and to the logic behind the application of the two sets of rules** in practice. Moreover, the fairness rules only protect data recipients qualifying as SMEs, whereas **non-SME data recipients might also need protection against unfairness and discrimination when in a situation of economic dependence vis-à-vis data holders**.

4.5.1 Description

Under Article 8(1) of the Data Act Proposal, data holders required by EU or national law to make data available to recipients are required to do so under fair, reasonable, and non-discriminatory (FRAND) terms, further specified in Article 8(2) and regulated under Article 13. This set of provisions can be subject to criticism from two perspectives: (i) their scope with regard to statutory obligations to make data available; and (ii) their scope *ratione personae*.[59]

Scope with regard to statutory obligations. The exact scope of Article 8(1) remains unclear as it refers to obligations – for instance included in sector-specific regulation – that enter into force after the Data Act becomes applicable.[60] However, the Proposal does not contain provisions that help circumscribe the potential scope of such obligations, nor that limits them to future provisions that make explicit reference to Articles 8 and 13 of the Data Act. **This can be a source of legal uncertainty for businesses operating in regulated markets and willing to share IoT-generated data, including via the services of the TRUSTS platform**.

[59] See also Bayamlıoğlu, E., *Chapter III and IV of the Data Act – B2B data sharing and access*, in Ducuing, C.; Margoni, T.; Schirru, L. (eds), *White Paper on the Data Act Proposal*, Center for IT & IP Law (CiTiP) Working Paper Series 2022, pp. 41-46.

[60] Data Act Proposal, Article 12(3).

Moreover, **there appears to be some uncertainty around Articles 8(1) and 8(2) of the Data Act Proposal with regard to their relationship with Article 13**. Whereas Article 8(1) appears to refer to a statutory obligation laid down in the law, the language of Article 8(2) reminds of contractual language whereby two parties agree to the making available of the data. This discrepancy in language may lead some to wonder how the fairness rules of Article 13, which imply freedom of contract by both parties, can apply to Article 8(1), which refers to a restriction of the freedom of one party (the data holder) via a statutory obligation to share data. **One possible interpretation is that the Data Act Proposal** sought to keep the door as open as possible to any type of statutory obligation stemming from EU or national law. In that respect, therefore, Article 8(1) should be read as starting from the premise that these statutory obligations might well be very generic and merely oblige the entity qualifying as data holder to make the data available. It would then be up to the data holder, jointly with the recipient, to determine the modalities of this 'making available', which would justify the reference to an agreement in Article 8(2). This agreement should then comply with the fairness rules of Article 13.[61] In other words, the Data Act **may have sought to create safeguards against data sharing modalities that**, while in response to an unavoidable obligation laid down in the law, **may in practice be discriminatory and unfair if left unregulated**. While this interpretation might be the correct one, **the provisions of Articles 8 and 13, read jointly, do not appear to be conclusive on this point and may benefit from a clearer formulation vis-à-vis future statutory obligations**.

Scope *ratione personae*. The next criticism concerns the breadth of the scope of these provisions with regard to the protected entities. Article 13 of the Data Act Proposal explicitly mentions that the FRAND obligations only apply when data holders are required to make data available to SMEs. On the one hand, the intent to especially protect smaller undertakings, which may deal with larger firms equipped with a greater bargaining power, is welcome; on the other hand, it can be argued that **SMEs are not the only category of undertakings that deserve protection**. The position of disadvantage of data recipients vis-à-vis data holders may not necessarily descend from their size, but also from a condition of economic dependence, for instance dependence from the data that the holder is required to share. **If the recipient is in fact dependent on those data, no matter the size of the two undertakings, the data holder may be led to abuse its advantageous position and comply with its obligation to share under unfair terms**.

4.5.2 Recommendations

For stakeholders

- Organisations qualifying as data holders for the purposes of the Data Act Proposal, and participating in data marketplaces such as TRUSTS, should **constantly monitor EU and national law applicable to them in order to be aware of possible statutory obligations to share data as per Article 8**. This is especially the case given the uncertainty as to what these envisaged obligations might entail and their relationship with the fairness regime of Article 13.

For policymakers

[61] Only if the data recipient is a micro enterprise or a Small or Medium-Sized Enterprise (SME), see Data Act Proposal, Article 13(1) and further below in this section.

- The European Commission should consider **providing more clarity as to the nature of the (future) statutory obligations referred to in Article 8 of the Data Act Proposal**. One solution could be to add in the Recitals examples of such obligations as well as the of the fields in which they may be introduced.
- The European Commission should consider **amending Articles 8 and 13 of the Data Act Proposal to clarify the interplay between the two provisions**. If the intended logic is that Article 13 applies to the practical modalities for implementing statutory obligations, it is advisable to make this link more explicit.
- The European Commission should consider **amending Article 13 of the Data Act Proposal to include**, amongst the undertakings deserving special protection, **also those undertakings that, acting as data users, are likely to be in a situation of dependence vis-à-vis the data holders**.

5 Recommendations in the consumer protection framework

Below we focus on one open point and lesson learned that have emerged with regard to the EU consumer protection framework: The protection of consumers (and human beings) against the cognitive and/or mental harm caused by AI. We present the core of the problem and then provide recommendations to stakeholders and policymakers.

5.1 Consumer protection against cognitive and/or mental harm caused by AI

The use of AI to facilitate the provision of many services **can lead to** technology-specific risks, in particular **the risk to cause cognitive and/or mental harm**. This category of harm is rather novel in EU law. To date, **the legal instruments dealing with the protection of human beings and of consumers do not appear to offer sufficiently robust safeguards against such risks**.

5.1.1 Description

As explained in D6.3,[62] **AI can cause for individuals several risks that EU law on consumer protection has not tackled so far, at least not directly**. These risks can be enumerated along the following lines:

(i) Risk of exclusion and/or discrimination of certain (categories of) individuals due to the underlying rules of the AI algorithm and/or its training and types of data it ingests over time;

(ii) Risk of unduly exposing the vulnerable aspects of individuals with more precise and intrusive tools than the ones available with traditional technologies;

(iii) Risk of amplifying the information asymmetry between individuals (including when acting as consumers) and businesses using AI systems, due to the opaque and hardly explainable nature of some systems; and

(iv) Risk of ultimately eroding the degree of control and autonomy of individuals (including when acting as consumers) concerning the decisions they make.

The risks outlined above are liable to lead to what is often referred to as cognitive or mental harm. It is interesting to note that these risks affect natural persons both as such (i.e., as human beings) and, potentially, as consumers. For instance, the first risk may lead to adverse effects on the human dimension of individuals protected by human and fundamental rights; but it could also deprive certain (categories of) individuals of equal access to goods and services or to equal treatment in business-to-consumer relationships. The second risk may also affect human dignity and the private sphere of individuals, while also leading to adverse effects for the consumer dimension of individuals. The third risk may impinge upon the human-centric spirit of AI by impinging upon the right to information, while also making business-consumer relationships more complex and difficult to understand and handle for consumers. And finally, the fourth risk may have serious repercussions for human dignity from a human rights and ethical perspective, while having a specific effect on the consumer dimension.

[62] See Section 6.2.2 of D6.3.

It appears from the above that several potential risks of AI systems on individuals can be tackled from a human rights- (and/or ethics-based) based perspective, as well as from a perspective related to the context of the case at hand, for instance business-consumer relationships. **The interplay between these two dimensions raises a legal policy question, namely the need to account for the risks of AI under both (human rights/ethics and specific) dimensions without duplicating regulatory efforts and with a view to maximising the protection of individuals**. It needs to be stressed that the human rights-centred dimension is the most crucial one, as it relates to rights that are of constitutional and fundamental nature in the legal order of the EU and the Member States. The protection against the risks of AI from a fundamental rights perspective should therefore take precedence over any scheme of protection provided for in other areas of law (including consumer law), precisely because of the fundamental nature of the interests these rights protect. Still, it is important to also focus on the consumer law dimension of the risks posed by AI and make sure that EU legislation provides sufficient safeguards, both of pre-emptive and reactive nature, against them.

In this regard, it was already observed in D6.3 that **the current EU consumer protection legal framework was not designed to account for the risks enumerated above. This is mainly due to the principle of technological neutrality underlying this legal framework**. The goal of a legislative approach based on this principle is to make the legislation as flexible as possible for it to maximise its impact regardless of the technical means employed in business-consumer relationships. **The flipside of this approach is that it may not be able to account for specific risks stemming from the peculiar features of a particular technology** that disrupts the traditional map of risks posed by most other technologies before it. **This is the case of AI**.

For instance, the Unfair Commercial Practices Directive (UCPD)[63] does prohibit practices that "materially distort the economic behaviour" of consumers;[64] however, on the one hand, the UCPD emphasises that practices of this kind are most likely to be harmful to consumers whose ability to recognise them may be lower than the average by reason of mental infirmity or age;[65] and on the other hand, it ends up channelling this concept of unfair practices towards two main categories: misleading practices[66] and aggressive practices.[67] The former have to do with the manipulation of the information about a product or a service, which leads the consumer to make a choice he/she would not have made; the latter imply a certain degree of pressure and/or coercion on the part of the business. **Neither concept appears to fully account for the risks posed by AI marketing systems, which may lead to cognitive and/or mental harm even without manipulating information or exerting pressure, let alone coercion**. Looking at horizontal regulation on product safety, the General Product Safety Directive (GPSD)[68] adopts an open approach linking the prohibition to market unsafe products to the absence of compliance with recognised standards of safety. The main challenge in relation to cognitive and mental harm is that, whilst standards are effective

[63] 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.

[64] Article 5 UCPD.

[65] Ibid.

[66] Article 6 UCPD.

[67] Article 8 UCPD.

[68] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety.

to regulate quantifiable harm, they are usually ill-equipped to deal with categories of harm that are hard to quantify or monetise, such as cognitive and mental harm. As explained in D6.3, the proposed AI Act[69] is the first legal instrument that focuses also on preventing cognitive and mental harm on top of material harm caused by AI. **While the AI Act does tackle some of the practical cases where AI may cause cognitive or mental harm, it is still limited to cases where harm is the result of an intentional design of the AI system, thereby not accounting for the unintentional harm possibly resulting from the 'natural' learning process of the algorithm**. Finally, it is to be noted that the recent legislative proposals for non-contractual liability for damaged caused by AI,[70] and for the amendment of the Product Liability Directive[71] do not take explicitly into account cognitive and/or mental harm caused by AI. In particular, the proposal for the AI Liability Directive did not include explicit references to cognitive and/or mental harm because the regulation of such categories of harm in the national law of the EU Member States is still fragmented. However, the proposal does include in its definition of 'duty of care'[72] the protection of fundamental rights as a set of interests that the national or EU law-based standards of conduct shall safeguard.

5.1.2 Recommendations

For stakeholders

- TRUSTS, other entities managing similar data marketplaces, and participating organisations **should be aware of the risk of cognitive and/or mental harm caused by AI systems** used to analyse the data. **Measures preventing or reducing the risk of cognitive and/or mental harm should be embedded as early as from the design and development** of the AI system.
- Upon deployment of the AI system, the above stakeholders should also **constantly monitor its learning curve to prevent the AI system to develop the capability of causing cognitive and/or mental harm**.

For policymakers

- The European Commission, in conjunction with the High-Level Expert Group on AI (HLEG),[73] should consider **initiating a consultation on non-economic categories of harm caused by AI with all the EU Member States**, in order to gauge their support to civil law regulation of such categories of harm, both from a product safety and from a liability perspective.
- Based on the results of the consultation, the European Commission, in conjunction with the HLEG on AI, should **consider ways to revisit the AI Act Proposal with a view to reducing the risk of AI systems causing cognitive and/or mental harm**. The amendments should be designed

[69] 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.

[70] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). COM(2022) 496 final.

[71] Proposal for a Directive of the European Parliament and of the Council on liability for defective products. COM(2022) 495 final.

[72] Article 2(9) of the Proposal for an AI Liability Directive.

[73] The HLEG provides advice on the EU's AI strategy. For more information, see: High-level expert group on artificial intelligence | Shaping Europe's digital future (europa.eu).

assuming a non-intentional attitude of the AI system designers and of the system itself towards causing such type of harm.

6 Conclusions

This Deliverable has addressed lessons learned and legal challenges collected during the course of the TRUSTS project. The multidisciplinary nature of the TRUSTS project has allowed the research team to explore several areas of law and collect open points and lessons learned from a multitude of legal frameworks. From a legal policy perspective, this contributes to demonstrating the interconnections between areas of law and the fact that one challenge in one specific area may affect the achievement of policy objectives in other areas. This is especially the case in the areas of digital and data regulation: as data are produced and exchanged by virtually any sector of the economy, and data marketplaces aim to facilitate and repurpose these data flows, potentially any sector-specific regulation is capable of affecting, to an extent, the creation of a smooth EU market for data and data spaces.

This Deliverable demonstrated that challenges and open points in the AML/CFT legal framework and in the consumer protection framework may hamper the functioning of data markets. On top of these, the Deliverable showed that the current and proposed legislation on data – especially the Data Governance Act and the Data Act Proposal – may benefit from further guidance and, in certain cases, reformulations to increase consistency and legal certainty. The TRUSTS project and its outputs are likely to represent a major test case in this respect: the variety of services and applications provided by the TRUSTS platform, combined with the large spectrum of potential participants (in terms of sectors covered) and the wide array of data to be shared, make TRUSTS a suitable candidate to assess the EU's regulatory approach in the data sphere.