TRUSTS
Trusted Secure Data Sharing Space

D6.2 Legal and Ethical Requirements

Authors: **Ducuing Charlotte, Dutkiewicz Lidia, Miadzvetskaya Yuliya (CiTiP – KU Leuven)**

August 2020

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

D6.2 Legal and Ethical requirements

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	D6.2		
Work Package	WP6		
Contractual due date	M10	Actual submission date	27 October 2020
Nature	Report	Dissemination Level	Public
Lead Beneficiary	KUL		
Responsible Author	Ducuing Charlotte, Dutkiewicz Lidia, Miadzvetskaya Yuliya		
Contributions from			

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete[1]	Changes	Contributor(s)
V0.1	03/08/2020	5%	Initial Deliverable Structure	KUL (Ducuing Charlotte, Dutkiewicz Lidia, Miadzvetskaya Yuliya)
V0.2	22/10/2020	90%	Internal submission for internal review (KUL)	KUL (Ducuing Charlotte, Dutkiewicz Lidia, Miadzvetskaya Yuliya)
V0.3	24/10/2020	95%	Internal review (KUL)	KUL (Emre Bayamlıoğlu)
V1	29/10/2020	100%	Submission to LUH	KUL

Disclaimer

[1] According to TRUSTS Quality Assurance Process:

1. to be declared

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
29WP	Article 29 Working Party
AI	Artificial Intelligence
AML	Anti-money laundering
B2B	Business-to-business
CJEU	Court of Justice of the European Union
DPIA	Data protection impact assessment
EDPB	European Data Protection Board
ePD	ePrivacy Directive
EDPS	European Data Protection Supervisor
ePR	ePrivacy Regulation
EPRS	The European Parliamentary Research Service
FATF	Financial Action Task Force on Money Laundering
FIU	Financial Intelligence Units
GDPR	General Data Protection Regulation
HBER	Horizontal Block Exemption Regulation
HLEG	The High-Level Expert Group on Artificial Intelligence
IDSA	International Data Spaces Associations
IPSs	Internet Service Providers
ISSs	Information Society Services
KYC	Know Your Customer
ML/TF	Money laundering and terrorist financing
PEP	Politically exposed person
PSD2	The Second Payment Services Directive
TFEU	Treaty on the Functioning of the European Union
VBER	Vertical Block Exemption Regulation

1 Executive Summary

Deliverable 6.2 titled 'Legal and ethical framework' identifies the relevant EU legal frameworks applicable to various data transactions that are envisaged in TRUSTS. More specifically, it provides insight into the privacy and data protection legal framework supporting the data sharing compliance with the EU rules. It determinates the issue of "controllership" over personal data, the ensuing allocation of data protection responsibilities and the legal basis for processing personal data. It informs partners on the main concepts of the ePrivacy legal frameworks and their relationship with the GDPR. Furthermore, this deliverable is a continuation of the work done in WP9 with regard to pseudonymization and anonymization of personal data. It provides further conceptual legal information on privacy preserving techniques that might be relevant for TRUSTS partners.

This deliverable deliberates on the consideration of data as an economic asset, known as the 'commodification' of data. It further outlines the latest developments in EU law with respect to exchange of the 'non-personal data' and to what is generally called now the 'free flow of data'. Moreover, the deliverable discusses the notion of 'data sovereignty' and outlines the on-going institutional debates on future regulation of data, which could be of relevance for data markets.

The setting up of a platform for the exchange of data implies the creation of a whole ecosystem in order to enable data providers and data users to exchange data. The deliverable envisages that the qualification of TRUSTS as an online platform and/or intermediary may trigger the application of specific legislative frameworks specifically dedicated to them.

This deliverable offers an overview of the role of platforms and/or intermediaries in the field of data sharing. As (an) intermediary(ies), the TRUSTS platform could be subjected to the Platform to Business Regulation ('P2B Regulation') adopted at EU level in 2019. The deliverable offers an insight into the P2B Regulation, including its scope of application, the substantive provisions and procedural obligations as well as enforcement-related ones will be introduced. The deliverable further explains whether and to what extent online platforms and intermediaries can be held liable for the content that their users place on their infrastructure under the 'e-Commerce Directive'.

Moreover, Section 6 provides an overview of EU legislation applicable to data sharing in B2B context. It begins with an outline of the regulation of unfair commercial practices between businesses, mainly at national level, taking Germany, France and Belgium as an example.

For absence of a horizontal legal framework regulating B2B transactions, the EU has been active in elaborating soft law guidelines for businesses. The deliverable elaborates on the general guiding principles for B2B data sharing provided in the European Commission 'Guidance on sharing private sector data in the European data economy' of 2018. It then provides a non-exhaustive list of considerations which may help companies in the preparation and/or negotiation of data usage agreements.

Even though the contractual framework remains the main legal regime governing data sharing, competition law remains an important background regime. This deliverable discusses the role of data for competition law analysis. Then, it provides a general overview of Article 101 and article 102 TFEU. More

specifically, the deliverable points out to the main competition law issues which may be relevant for the data market ecosystems such as this of TRUSTS. Such issues include: (i) the exchange of information, and in particular sensitive information, directly between competitors or indirectly through a common agency (e.g. platform); (ii) the refusal to give access to data under so-called 'essential facilities doctrine'. It also outlines the between competition law and personal data protection law (such as the GDPR), when personal data are at stake.

Section 8 of this deliverable provides an overview of the relevant regulatory frameworks relating to transactions over financial data. First of all, it covers frameworks aiming at facilitating the fight against anti-money laundering and terrorist financing. Then it looks at Payment Services Directives, their scope of application and their relationship with the GDPR with the objective of informing the consortium partners of potential challenges in an anticipatory manner.

Given that the blockchain technology is contemplated to be used in TRUSTS data market ecosystem, including smart contracts which could automate data transactions, Section 9 introduces the blockchain technology and smart contracts and outlines the points of contact of such technologies with the law. It discusses their relevance for data markets and outlines the EU policies towards blockchain legal and regulatory framework. Taking into account that the legal analysis of smart contracts makes part of the scope of Task 3.2. this deliverable only outlines in general terms potential points of contact between the blockchain technology and the operation of the law.

Section 10 build on the work already performed in Deliverable 9 on the possible ethical implications of data sharing within the TRUSTS platform. It offers a high-level analysis of ethical issues in data sharing with the use of AI-driven tools. It provides an overview of the ethics requirements for Trustworthy AI as defined by the High-Level Expert Group (HLEG) in non-binding 'Ethics Guidelines for Trustworthy AI'. Then, this deliverable elaborates on data-driven discrimination and data bias.

The research will be necessary in the later stage of the project to provide detailed legal requirements guiding the development of the TRUSTS platform. At this time of the project lifetime, when technical details are not yet defined, it is not possible to provide specifically tailored recommendations for TRUSTS. Application of the hereby described rules to TRUSTS will be conducted in the later stage of the project. As such, the findings of this Deliverable will be further substantiated and contextualized in Deliverable D6.3.

2 Introduction

2.1 Mapping Projects' Outputs

The objective of this Deliverable is to identify relevant overarching legal rules and ethical principles, and provide guidance for their implementation within the TRUSTS project. To that end, this Deliverable is based on the research on the EU legislation, principles and values regarding the sharing of personal and non-

personal data. The approach followed in this Deliverable consists of the analysis of the EU legal framework and its applicability to the TRUSTS project. It follows up on the work performed in WP9 relating to ethics requirements of the project.

The objective of this Deliverable is to analyse the European laws and regulations relevant to the platform, define legal and ethical requirements and identify potential legal and ethical obstacles. The emphasis of this Deliverable has been be put on:

1) Privacy and Data Protection (the General Data Protection Regulation, the e-Privacy Directive and forthcoming Regulation);
2) Regulation on the free flow of non-personal data, data ownership and data sovereignty;
3) Contractual considerations of data sharing agreements;
4) The role of platforms and/or intermediaries in the field of data sharing;
5) Financial data framework, including Anti-Money Laundering rules and Payment Service Directive and their convergences and divergences with the GDPR;
6) Competition law, including information exchange, the refusal to deal data and the intersection of competition law and data protection law;
7) Blockchain technology;
8) Data-driven discrimination, data bias and the AI Ethical Guidelines.

The work performed under this Deliverable provide a valuable legal input to activities in WP3, WP4 and WP5, where the platform will be designed, tested and validated.

2.2 Deliverable Overview and Report Structure

Deliverable 6.2 titled 'Legal and ethical framework', is the first legal deliverable in TRUSTS, which follows up on the work performed in WP9 relating to ethics requirements of the project, which were submitted at the end of June 2020.

This Deliverable is structured as follows:

- Section 3, Privacy and data protection focuses on a few data protection-related questions particularly relevant to data market ecosystems such as this of TRUSTS;
- Section 4, Regulation of data as an (economic) asset elaborates on the notion of data as an economic asset, which can be traded in its own right, otherwise called the 'commodification' of data. It also outlines the latest developments in EU law with respect to data exchange and to what is generally called now the "free flow of data";
- Section 5, Law applicable to online platforms and intermediaries analysis the application of specific legislative frameworks applicable to online platform and/or intermediary, including the Platform to Business Regulation ('P2B Regulation') and the liability exemptions for certain intermediaries under the E-Commerce Directive;

- Section 6, Economic law applicable to data transactions outlines of the regulation of unfair commercial practices between businesses, mainly at national level and provides insights into the European Commission soft law guidance on B2B data sharing;
- Section 7, Competition law and access to data discusses the role of data for competition law analysis, analysis the applicability of the Article 101 and article 102 TFEU to the TRUSTS project and outlines the interconnection between competition law and data protection law;
- Section 8, Financial law applicable to data transactions provides an insight into the financial law applicable to data transactions, including the Anti-Money Laundering Directives and the Second Payment Services Directive;
- Section 9 Blockchain and law introduces the blockchain technology and smart contracts and outlines the points of contact of such technologies with the law.

  The legal analysis of smart contracts makes part of the scope of Task 3.2. In this context, this deliverable only outlines in general terms potential points of contact between the blockchain technology and the operation of the law.

- Section 10, Ethical challenges in data sharing, describes the ethics requirements for Trustworthy AI as defined by the High-Level Expert Group (HLEG) and elaborates on data-driven discrimination and data bias.

  In this Section we have offered a high-level analysis of ethical issues in data sharing with the use of AI-driven tools. For further analyses of the possible implications of data sharing within the TRUSTS platform we refer to our Deliverable 9.

3 Privacy and data protection

When setting up a data marketplace such as TRUSTS, privacy and data protection law shall obviously be paid special attention. With big data and even more so with AI, personal and non-personal data become indeed increasingly intertwined so that it can never be completely ruled out that personal data would not be processed at some point. The main principles and obligations applicable to the processing of personal data are outlined in WP9, in order to comply with the post-grant ethics requirements, with a view to the specific characteristics of data processing activities contemplated in the respective use cases.

This section will focus on a few data protection-related questions particularly relevant to data market ecosystems such as this of TRUSTS. First, the determination of controllership and the ensuing allocation of data protection responsibilities. The second sub-section highlights the legal basis for processing personal data. Third, the main changes and concepts of the ePrivacy Directive and Regulations will be elaborated. And fourth, privacy preserving techniques, such as anonymization and pseudonomisation, will be tackled from a legal perspective.

3.1 Controllership in a data market context

Data marketplaces are characterised by a specific business organisation with data providers on the one hand, data users on the other hand, and a certain number of intermediaries between them. The number and role of intermediaries may differ as well as the character more or less centralised of the marketplace. The more decentralised or even distributed the data marketplace ecosystem, the more likely the chain of legal responsibilities may be blurred. This is particularly true for data protection law. Enquiring about who is / are the controller(s) – and to a lesser extent, the processor(s) – amounts to look for the entity(ies) responsible for complying with data protection law. This very crucial point is however not an easy one. Particularly in contemporary online networked environment, the roles and responsibilities of acts have become blurry. The Court of Justice of the European Union ('CJEU' or 'the Court') has been recently requested to clarify how controllers should be identified in such complex environments.

This section begins with introducing the various roles known to data protection law, *i.a.* controller, processor and recipient. Then, the recent case law of the Court on (joint) controllership will be outlined. The third sub-section introduces the draft guidelines issued by the European Data Protection Board ('EDPB') following the recent case law in order to provide practical guidance for companies.

3.1.1 'Controller', 'processor' and 'recipient' and other roles in the GDPR

The General Data Protection Regulation ('GDPR')[2] distinguishes several roles, which imply a certain level of legal responsibilities.

a) The controller

The controller is defined as the "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".[3] As summarised by the Article 29 Working Party ('29WP'), the controller(s) is(are) the entity(ies) who determine the "why and how" of the data processing activities.[4] The controller(s) is(are) the entity(ies) responsible for complying with data protection obligations with respect to the data processing activities in question.

The definition of a controller is not new with the GDPR; it is the exact same definition as in the earlier Data Protection Directive.[5] While the definition suggests the factual possibility of joint controllership, such a possibility was not expressly reckoned in the Data Protection Directive. In contrast, the GDPR dedicated an article (Art. 26) to "*joint controllers*". Joint controllers are two or more controllers "jointly determin[ing] the purposes and means of processing". They shall "in a transparent manner determine their respective responsibilities for compliance with the obligations under [the GDPR], in particular as regards the exercising of the rights of the data subject […], by means of an arrangement between them […]".[6] Such arrangement shall "duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects" and its "essence" shall be made available to the data subjects.[7] In any case, the data subject may exercise his / her rights in respect of and against each of the controllers.

b) The processor

Next to the controller, the GDPR also lays down obligations applicable to the '*processor*'. The processor is defined as the "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[8] The GDPR extended the scope of obligations that the processor shall abide by, directly based on statutory law. For instance, not only shall the processor bear security

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88 ('General Data Protection Regulation').
[3] GDPR, Art. 4 (7).
[4] Article 29 Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor", 00264/10/EN WP 169'. The Opinion is available here: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (last visited 26th August 2020).
[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50 ('Data Protection Directive').
[6] GDPR, Art. 26 (1).
[7] GDPR, Art. 26 (2).
[8] GDPR, Art. 4 (8).

obligations[9] but also a notification obligation vis-à-vis the controller in case of a personal data breach and a general duty of assistance to the controller in ensuring compliance with a range of obligations, including the conduct of a data protection impact assessment.[10] The processor shall not infringe the GDPR "by determining the purpose and means of processing" or else he shall be considered to be a controller in respect of that processing.[11] In such case, he shall be fully responsible and liable for such processing. Rather, the processor is liable to process personal data "only on documented instructions from the controller".[12]

c) The data subject

The beneficiary of data protection is, obviously, the 'data subject', defined indirectly by reference to the notion of 'personal data'.[13]

d) The recipient

Next to the controller, processor and data subject, the GDPR identifies also the '*recipient',* defined as "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular enquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing".[14] The definition of a recipient refers to the 'third party', defined as "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data".[15] Third parties do consequently not have data protection obligations with respect to the personal data processing at stake. The recipient can therefore be either such a 'third party' or a controller or processor with respect to the personal data at stake. The notion of the recipient is used in the GDPR rather passively: i.e. transparency requirements include for the controller the obligation to provide the data subjects, where applicable, with the identification of recipients or categories of recipients.[16] This being said, the recipient (just like the processor, see above) may also qualify as controller with respect to the same data, when pursuing his own purpose.

e) Intermediary conclusion

To sum up, the GDPR refers to several roles. Clearly, the most significant ones are the data subject as beneficiary on the one hand, and the 'controller' – and to a lesser extent the 'processor' – as the entity mainly responsible for compliance on the other. It is therefore crucial to identify the controller or else the

[9] GDPR, Art. 32.
[10] GDPR, Art. 28 (3) (f).
[11] GDPR, Art. 28 (10).
[12] GDPR, Art. 28 (3) (a).
[13] GDPR, Art. 4 (1). See also WP9 deliverables.
[14] GDPR, Art. 4 (9).
[15] GDPR, Art. 4 (10).
[16] GDPR, Art. 13 and 14.

GDPR can simply not be applied. Determining the controller is however made increasingly difficult online by the fact that activities of various operators are intertwined. The case of data markets is an illustration of such complex ecosystems, with not only the data provider and data user but also a myriad of intermediaries in-between. The question how to delineate where the obligations of one start and finish is not answered easily based on the wording of the GDPR itself – just like the Data Protection Directive before it. For this reason, the Article 29 Working Party issued a much referred to opinion in 2010 in order to clarify the concepts of 'controller' and 'processor'.[17] In 2019, the European Data Protection Supervisor ('EDPS'), namely the data protection authority in charge of data processing activities conducted by the European Union's institutions, issued guidelines on the concepts of 'controller', 'processor' and 'joint controllership'.[18] Following the recent case law of the CJEU, the EDPB also issued draft guidelines meant to constitute an update of the 2010 opinion of the Article 29 Working Party. To an appreciable extent, the recent case law of the Court constitutes indeed a breakthrough with respect to the common understanding of 'controller' and 'joint controllers'. This case law has to be taken into account in order to rightly delineate the data protection obligations of actors in the context of a data market. To conclude, who is 'controller', 'processor' or 'joint controller' in the data market has crucial implications with respect to responsibility allocation. Criteria to identify them in a given context are outlined in the following section.

3.1.2 The recent case law of the CJEU on (joint) controllership

The identification of controllership has been (surprisingly) subject to little case law by the CJEU until recently. Until then, companies had to rely on national case law and cases before national data protection authorities. In this context, the (soft law) Opinion of the Article 29 Article ('29WP', latter replaced by the 'EDPB' under the GDPR regime) has been very influential and will therefore be outlined in the first sub-section. Then, every of the three recent cases before the CJEU will be introduced in turn. Finally, an intermediary conclusion will summarise the legal regime following these cases and identify the questions that they left open (or even triggered).

a) Background: the 2010 Opinion of the Article 29 Working Party ('29WP')

According to the Opinion of the Working Party 29 of 2010, the notion of 'controller' should be analysed functionally, namely based on the factual influence that the entity has, rather than based on a "formal analysis".[19] The controller(s) is(are) the entity(ies) who determine(s) the 'why and how' of the data processing. This stands in contrast with the 'processor' who, in the 2010 opinion of the Article 29 Working Party, may to some extent determine the means (the 'how', especially technically) but may not determine the purpose(s) (the 'why' of the processing), or else the processor would become controller for that sake. In many cases however, it is likely that several entities may be involved, to some extent, in the

[17] Article 29 Working Party (n 4).
[18] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7th November 2019. The Guidelines are available here: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf (last visited 26th August 2020).
[19] Article 29 Working Party (n 4) 9.

determination of the 'why' and/or 'how' of the data processing. This begs the question whether and under which conditions the entities should be either separately responsible for compliance or jointly responsible or in order words 'joint controllers'. The Article 29 Working Party recognises that joint determination [of purpose and means] does not necessarily mean that the entities at stake *equally* participate in the joint determination.

After the recent case law of the Court, to what extent the Opinion of the Article 29 Working Party still holds true and can still be referred to remains to be analysed. In the three cases *Wirtschaftsakademie,*[20] *Jehovan todistajat*[21] and *Fashion ID*,[22] the Court did indeed disrupt the traditional understanding of (joint) controllership and its legal implications quite significantly.

b) The Wirtschaftsakademie case

The *Wirtschaftsakademie* case is about a fan page administrator on the Facebook social network. The Court analysed whether such a fan page administrator shall be considered as a controller for the processing of data pertaining to the visitors of the fan page (whether members of the Facebook social network or not). Concretely, by creating a fan page on Facebook, Wirtschaftsakademie, just like any other such operator, signs up to Facebook related terms and conditions. The terms and conditions notably grant the fan page administrator the possibility to obtain anonymous statistical information on visitors to the fan page via a function called 'Facebook Insights'.[23] Such information is collected via cookies placed on the terminal of the visitors, which enable Facebook to identify them and match other information already collected on them. The court case does not enquire about how and for which purpose(s) Facebook processes such information for its part, while it is recognised that Facebook does process such data.

The Court considers that, by creating a fan page and thereby agreeing to Facebook terms and conditions – although in the form of a 'take-it-or-leave-it' agreement -, the fan page administrator (Wirtschaftsakademie in this case) allows Facebook to place its cookies, which could not be done otherwise. According to the Court, the fan page administrator determines certain parameters of the data processing, such as the target audience. The fan page administrator receives economic gain from such operation, in the form of the possibility to obtain anonymous statistics derived from the processing of personal data by Facebook. In those circumstances, the Court finds, the fan page administrator shall be regarded as "taking part in the determination of the purposes and means of processing the personal data of the visitors to its fan page".[24] Wirtschaftsakademie is therefore qualified as a controller, jointly with Facebook. The fact that the fan page operator does not access the personal data was found irrelevant by the Court. Finally, with respect to the distribution of responsibilities, the Court states that joint responsibility (namely, of Facebook and of the fan page operator) does not automatically mean "equal responsibility". The responsibility of controllers shall be determined according to the circumstances. Yet, the Court does not clarify the legal implications of such statement.

[20] CJEU 5 June 2018, C-210/16, ECLI:EU:C:2018:388 ('Wirtschaftsakademie case').
[21] CJEU 10 July 2018, C-25/17, ECLI:EU:C:2018:551 ('*Jehovan todistajat* case').
[22] CJEU 29 July 2019, C-40/17, ECLI:EU:C:2019:629 ('*Fashion ID* case').
[23] Wirtschaftsakademie case, para 15.
[24] Wirtschaftsakademie, para 39.

c) The Jehovan todistajat case

The *Jehovan todistajat* case is, in essence, about whether the Jehovah's Witnesses Community shall be considered a controller, jointly with its preaching members, with respect to the processing of personal data conducted in the course of door-to-door preaching activities. In this case, the qualification of the preaching members as controllers was not questioned.

First and similar to the *Wirtschaftsakademie* case, the Court highlights that, in light of the objective to ensure an effective and complete protection of individuals with respect to their privacy and data protection, a broad definition of the concept of 'controller' shall be favoured. The Court disregards the fact that the Community, in organising, coordinating and encouraging the door-to-door preaching, does not access the data, nor does it give its preaching members written guidelines or instructions in relation to the data processing.[25] The exercise of an "influence over the processing of personal data, for [its] own purposes" is considered by the Court as the criterion for finding that the Community participates in the determination of the purposes and means of the processing:[26] (1) The Community does not have a mere "knowledge on a general level" of the existence of such data processing activities.[27] Its influence is rather characterised in that it determines "in which specific circumstances [the preaching members] collect personal data relating to persons visited, which specific data are collected and how those data are subsequently processed".[28] (2) The data processing activities are conducted as a "memory aid for later use and for a possible subsequent visit". They make thereby part of the activities conducted to "spread the faith" of the Community, which constitutes therefore the purpose of the data processing. As a result, the Community should be regarded as a controller, jointly with its preaching members.

d) The Fashion ID case

The *Fashion ID* case deals with a website operator (Fashion ID) which embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin (in this case, the 'Like' button of Facebook) and, to that end, to transmit to that provider the personal data of the visitor.[29] The question that the Court undertakes to answer is whether such a website operator shall be considered a controller, jointly with Facebook. In this case, the Court both confirms findings of the two previous cases and makes ground-breaking statements.

The Court again confirms that a broad definition of the concept of 'controller' is to be derived from the aim of data protection law to ensure a high level of protection of the fundamental rights and freedoms of natural persons. Again, the Court states that, in case of joint controllership, it is not necessary for each of the controllers to have access to the personal data.[30] The Court finds that, by embedding on its website the Facebook 'Like' button, Fashion ID "appears to have made it possible for Facebook Ireland to obtain personal data of visitors to its website and that such a possibility is triggered as soon as the visitor consults

[25] *Jehovan todistajat* case, para 63.
[26] *Jehovan todistajat* case, para 68.
[27] *Jehovan todistajat* case, para 71.
[28] *Jehovan todistajat* case, para 70.
[29] *Fashion ID* case, para 64.
[30] *Fashion ID* case, para 65.

that website, regardless of whether or not the visitor is a member of the social network Facebook, has clicked on the Facebook 'Like' button or is aware of such an operation".[31] The Court considers that Fashion ID was "fully aware of the fact that [such plugin] serves as a tool for the collection and disclosure of the personal data of visitors to that website".[32] The Courts finds that, by embedding such social plugin on its website, Fashion ID exerts a "decisive influence over the collection and transmission of the personal data of visitors […], which would not have occurred without that plugin".[33] Against this background, the Court finds that Fashion ID participates in the determination of the purposes and means of the processing and thereby qualifies as a controller, jointly with Facebook.

However, and this is where the ground-breaking character of the case lies, the Court limits the scope of such finding to the first phases of the data processing, namely the collection of the data and their "disclosure by transmission" (to Facebook). By contrast, the "subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission [via the social plugin]" are out of the scope of the joint controllership. In support of this finding, the Court considers that it is "impossible that Fashion ID determines the purposes and means" of such operations.[34] This new 'phase-based' or 'step-based' approach follows, in a way, the two earlier cases, where the Court clarified that joint liability does not imply equal responsibility of the various operators engaged in the processing of personal data. Aside such phase-based approach, the Court identifies the case where the controllers would respectively be involved "to different degrees" in the processing of personal data, although this case is not further discussed.[35]

In the *Fashion ID* case, the Court goes a step further than in the two previous ones, by looking into the *concrete legal consequences of such phase-based approach*, in terms of allocation of data protection obligations. The Court was requested to determine whether Fashion ID shall bear the obligations to obtain consent for the data processing activities and to inform the individuals of the existence of such activities. Having found that Fashion ID is a controller, the Court answers positively to these questions. More than that, the Court finds that it is the *sole* obligation of Fashion ID to obtain consent rather than of Facebook "since it is the fact that the visitor consults that website that triggers the processing of the personal data".[36] The same applies to the duty to inform.[37] In doing so, the Court follows the Advocate General who considers that such an allocation of responsibilities between the controllers would best ensure "efficient and timely protection of the data subject's rights". However, and in light of the phase-based approach, the Court restricts the scope of both the consent gathering and the information duty to the phases for which Fashion ID is responsible.[38] This means that Fashion ID shall obtain consent and provide information to

[31] *Fashion ID* case, para 75.
[32] *Fashion ID* case, para 77.
[33] *Fashion ID* case, para 78.
[34] *Fashion ID* case, para 76.
[35] *Fashion ID* case, para 70.
[36] *Fashion ID* case, para 102.
[37] *Fashion ID* case, para 102.
[38] *Fashion ID* case, para 101 and 102.

data subjects *solely with respect to the phases of data collection and disclosure by transmission* via the social plugin for which, according to the Court, Fashion ID determines the purposes and means.

As to the purpose of data processing,[39] the Court notes that "Fashion ID's embedding of the Facebook 'Like' button on its website allows it to optimise the publicity of its goods by making them more visible on the social network Facebook when a visitor to its website clicks on that button". According to the Court, Fashion ID agreed to the processing of personal data by Facebook, at least implicitly, "in order to benefit from the commercial advantage consisting in [such] increased publicity". As a result, and without having enquired about the specific advantage that Facebook gains from such processing, the Court states that the processing operations are "performed in the economic interests of both Fashion ID and Facebook Ireland".[40]

e) Intermediary conclusion

The three cases, and particularly *Fashion ID*, are of major significance not only to identify who is/are responsible for compliance with data protection obligations, but also to subsequently unfold the nature and scope of such obligations. On the one hand, the Court adopts a broad interpretation of the concept of 'controller'. On the other, the Court, particularly in *Fashion ID*, then restricts the scope of responsibility of controllers, in case of joint controllership, to the phase or 'degree' of the data processing activity where they exert a genuine influence. However, this recent case law raises many questions. The three cases show discrepancies not only between them but also within a given case, which blur the legal interpretation of data protection law. Indeed, not all legal scholars have the same understanding of the Court's reasoning on a number of major aspects. For instance, does the Court require a joint purpose pursued by the joint controllers? The Court seems to suggest both a positive and a negative answer. I.e. in the *Fashion ID* case, the Court notes that, with respect to purpose, both Fashion ID and Facebook have an "economic gain" from the data processing (see above). [41] In contrast, the Court recognises that Fashion ID, and similarly Wirtschaftsakademie, jointly determine the purposes and means of the data processing with Facebook, based on their agreement with Facebook (although 'take-it-or-leave-it') illustrated by, respectively, the embodiment of the 'Like' button and of the creation of a fan page on the Facebook social network. Then, as underlined by Specht-Riemenschneider and Schneider, joint controllership would not be triggered by (a) joint purpose(s) but by a joint *decision / determination* of the said purpose(s).[42] Other authors consider that the recent case law of the Court should be interpreted as implying that controllership would be triggered by the reunion of three elements: the participation of the entity in the processing of data, the participation of the entity in the determination of the means and finally the participation in the determination of the purpose(s).[43] Mahieu et al. have the broadest interpretation of the case law, by

[39] The Court confusingly refers to "the purposes of those operations involving the processing of personal data" (para 80) rather than, in a more straightforward way, the purpose of the data processing activities.
[40] *Fashion ID* case, para 80.
[41] S. Kremer, 'Gemeinsame Verantwortlichkeit: Die Neue Auftragsverarbeitung?', Computer Und Recht 2019/35, no. 4, p. 227; Golland 2019.
[42] Louisa Specht-Riemenschneider and Ruben Schneider, 'Stuck Half Way: The Limitation of Joint Control after Fashion ID (C-40/17)' (2020) 69 GRUR International 159.
[43] Primož Gorkič, 'Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.: More Control, More Data Protection for Website Visitors? (C-40/17 Fashion ID)' (2019) 5 European Data Protection Law Review 579.

concluding (from the *Wirtschaftsakademie* case) that, under the Court's interpretation, "any actor who has a purpose for a data processing operation, and can directly influence that processing, can be considered a data controller".[44]

It is therefore yet very unclear how this case law should be applied to the broad range of activities conducted online, beyond the very situations analysed in the three cases. In this context, the European Data Protection Board ('EDPB', the successor of the Article 29 Working Party) published draft guidelines in early September 2020 on the concepts of 'controller' and 'processor' in the GDPR,[45] as an update of the Opinion of 29WP of 2010, now partly obsolete (although it is yet unclear to what extent). These guidelines are analysed in the following section.

3.1.3 Draft Guidelines from the EDPB

At the time of writing, the draft Guidelines are only a 'Version 1.0' subject to an open consultation until mid-October 2020. Guidelines from the EDPB are not legally binding; they consist in soft law instruments to interpret legal provisions. However, they are likely to be decisive in the decision-making practice of data protection authorities, and may also be endorsed (fully or in parts) by Courts. This section will outline the parts of the draft guidelines bearing most relevant for the question of determination of controllership. The three first sub-sections will introduce the draft Opinion of the EDPB in three various cases, namely the situations of single controllership, joint controllership and no controllership. The consequences in terms of allocation of data protection responsibilities will then briefly be outlined.

a) One controller or single controllership

Following the recent case-law of the CJEU, the EDPB reiterates that it is not necessary for a controller to have access to the data. The EDPB surprisingly extends this rule to *all situations of controllership*, even in case of sole controllership, while the CJEU was only mentioning joint controllership, thereby implying that at least one controller should indeed have access to the data. Following the *Wirtschaftsakademie* case, the EDPB considers that "someone who outsources a processing activity and, in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data".[46] The EDPB maintains its earlier distinction between 'essential' v 'non-essential' means of data processing (already

[44] René Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe' (2019) 10 JIPITEC 86–87 <https://www.jipitec.eu/issues/jipitec-10-1-2019/4879>.
[45] EDPB, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 1.0' (2020) 07/2020 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf>.
[46] ibid 42.

present in the 2010 decision of the Article 29 Working Party), that the controller shall decide or have a decisive influence over, although such a distinction was not used by the Court in its recent case-law.[47]

b) Joint controllership

When it comes to joint controllership, the EDPB clarifies that the "overarching criterion for joint controllership to exist is the *joint participation* of two or more entities in the *determination* of the purposes and means of a processing operation" (emphasis added). Such "joint participation" should be twofold, namely the determination of the purpose(s) on the one hand and the determination of the means on the other.[48] Joint participation is equated with "decisive influence over whether and how the processing takes place", which can take several forms, such as a "common decision" or "converging decisions" regarding "the purposes and essential means".[49] The EDPB considers that the recent case law of the CJEU illustrates situations of "converging decisions", in the sense that the decisions of the parties at stake (e.g. Wirtschaftsakademie and Facebook, or Fashion ID and Facebook or else the Jehovah's Witnesses Community and its preaching members) "complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing. The EDPB invites to enquire whether the processing would *not be possible* without "both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked".

i. Joint determination of the purposes

According to the EDPB, "joint controllership exists when entities involved in the same processing operation process such data for *jointly defined purposes*" (emphasis added). The EDPB clarifies that:

- This will be the case where entities have (the) same (or common) purpose(s);
- This will also be the case where the entities pursue purposes "*which are closely linked or complementary*" (emphasis added), which the EDPB openly derived from the recent case law of the CJEU. This would be so in case of "mutual benefit arising from the same processing operation", however subject to the criterion already laid down, namely that "each of the entities involved participates in the determination of the purposes and means of the relevant processing operation".
- However, the "*mere existence of a mutual benefit* (e.g. commercial) arising from a processing activity does not give rise to joint controllership" (emphasis added).
- An entity that does not pursue its own purpose when processing the data shall not be a controller, but a processor.[50] By pinpointing the pursuit of one own purpose, the EDPB thereby seems to disregard the *determination* or *decision* on the purpose(s) and means as the relevant factor (in

[47] Should the Court have applied such a distinction, the outcome of the case (e.g. in *Wirtschaftsakademie*) might have been different. It is hard to believe that the fact that Wirtschaftsakademie (or any other fan page administrator) can (rather marginally) design the parameters of the fan page and have an influence on its audience, could be found constitutive of 'essential' means for the processing.
[48] EDPB (n 45) s 50.
[49] ibid 51.
[50] ibid 53.

contradiction to the above). This maintains the confusion triggered by the recent case law of the Court on the criterion(a) for determining controllership (discussed in the above sub-section).

ii. Joint determination of the means

In the case of joint controllership, the EDPB (after the CJEU) maintains that each controller does not have to determine all the means, which is just stating the obvious. After the recent case law of the Court, the EDPB indicates that one of the controllers may provide the means of the processing *and make it available for personal data processing activities by the other entity(ies)*. In such a case, the fact for such other entity(ies) to make use of these means "so that personal data can be processed for a particular purpose" forms an integral part of the "determination of the means of the processing". What is clearly described here is the fact that Wirtschaftsakademie (and other Facebook fan page administrators) *make(s) use of the Facebook platform*, in the course of which personal data are processed.[51] The EDPB considers that such a scenario may arise "in case of platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up". According to the EDPB, "the use of an already existing technical system does *not exclude joint controllership* when users of the system *can decide on the processing of personal data to be performed in this context" (*emphasis added).[52] This being said, the mere "use of a common data processing system or infrastructure" will not automatically lead to the qualification of joint controllership. Whether the processing could be performed by one party without the intervention of the other party, should thereby be a determining criterion.[53]

c) Situations where there is no controllership

The EDPB confirms the earlier interpretation of the Article 29 Working Party that the exchange of personal data between entities which do not jointly determine the purposes and means shall "be considered as a transmission of data between separate controllers". One would be the "recipient" of the data. Similarly, there would be no joint controllership in the case where "several entities use a shared database or a common infrastructure, if each entity independently determines its own purposes".[54] Then the EDPB goes on with examples, which are expected to clarify the message. However, both examples describe cases where the users (of, respectively, a shared database or a common infrastructure) *process different personal data sets,* which are relatively 'easy' situations.

Next to that, the EDPB also explicitly refers to the situation where "various actors successively process *the same personal data* in a *chain of operations*, each of these actors having an *independent* purpose and *independent* means in their part of the chain" (emphasis added). Such situations could be particularly found in data market ecosystems such as TRUSTS.

[51] ibid 62.
[52] ibid 63.
[53] ibid 66.
[54] ibid 68–69.

The Guidelines include, in an annex, a flowchart in order to help one clarify his/her situation in the chain of responsibilities (see pp. 46-47) in a given situation.

d) Consequences of the allocation of data protection responsibilities

The EDPB clarifies the relationship between controller and processor and provides practical guidelines in this respect. These aspects are not really new and are therefore not further discussed here at this stage.

Then the EDPB aims to clarify the relationships between joint controllers. The EDPB maintains the previous opinions of the Article 29 Working Party that the controllers should determine and agree on their respective responsibilities (pursuant to Art. 26(1) GDPR) and provides for illustrations of topics that should be subject to such an agreement.

With respect to the consequences of joint controllership, the EDPB is particularly expected to clarify the consequences of the phased-based approach newly adopted by the CJEU. First, the EDPB reiterates in several instances that the determination of the controller(s) should be related to the phases of the data processing activities, thereby following the recent case law of the Court and particularly *Fashion ID.* Again confirming the case law of the Court, the EDPB reiterates that joint controllership does not necessarily mean "equal responsibility" of the various entities. Apart from that, the EDPB does not further clarify the *specific* legal consequences of the step-based approach in terms of responsibilities and liability of the controllers.

3.1.4 Conclusion - Looking into the future: impact on TRUSTS data market ecosystem

At this stage of the development of the project, it is not possible to determine data protection responsibilities in the data market ecosystem. Such an endeavour can indeed not be conducted in the abstract. As discussed in this section, the analysis should be based on factual control of the respective entities on data processing activities. In any case, the determination of roles in the TRUSTS data market ecosystem should take into account data protection law and especially the recent case law of the CJEU. The more blurry the boundaries between the roles of entities, the more likely they will end-up qualifying as joint controllers.

Incidentally, the above-study of the allocation of data protection responsibilities and particularly the overview of the recent case law of the CJEU unravel another aspect, which could be of significance for data markets. While it may bring about fundamental legal questions,[55] the 'step-based' or 'phased-based' approach adopted by the Court may facilitate the exchange of personal data in data markets.

[55] For instance with respect to the notion of 'purpose' in data protection law and particularly to the principle of purpose limitation, see Charlotte Ducuing and Jessica Schroers, 'The recent case law of the CJEU on (joint) controllership: have we lost the purpose of 'purpose'?', *Computerrecht* 2020, *Forthcoming.*

3.2 Legal basis for processing personal data

First off, it is worth reminding that in order to apply the right legal regime for data usage, each dataset should be qualified according to the nature of data it involves (personal data, non-personal data, mixed data). The legal conditions for processing personal data are regulated by the GDPR. Article 4(2) of the GDPR defines "*processing*" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means (…)', including 'use, disclosure by transmission, dissemination or otherwise making available (…)".[56]

Article 5 GDPR sets the principles that must be respected by all entities processing personal data:

i. personal data must be processed lawfully, fairly and in a transparent manner in relation to the individual (lawfulness, fairness and transparency principle)[57];
ii. personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)[58];
iii. personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [59] (data minimisation principle);
iv. personal data must be "accurate and, where necessary, kept up to date"[60] (accuracy principle);
v. personal data must not be kept for longer than is necessary for the legitimate purposes for which they are processed (storage limitation principle)[61];
vi. personal data must be processed in a manner that ensures appropriate security including protection against unauthorized or unlawful processing, accidental loss, destruction or damage (integrity and confidentiality principle).[62]

The data controller must moreover demonstrate compliance with the abovementioned principles (accountability).[63]

Since the GDPR has as its main objective the protection of the "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"[64], it does not come as a surprise that data disclosure or transfer of personal data is only possible under specific conditions.

Data controllers must inform data subjects if and how their data is transferred to a third party. Privacy clauses should be inserted in contracts, general terms and conditions, purchase conditions, etc., to inform contract partners how they process personal received and transmitted to each other. As soon as the scope of the data transferred or the processing carried out so requires, the Parties have to enter into a data processing agreement which should clarify that:

[56] GDPR, Art. 4(2).
[57] GDPR, Art. 5(1)(a).
[58] GDPR, Art. 5(1)(b).
[59] GDPR, Art. 5(1)(c).
[60] GDPR, Art. 5(1)(d).
[61] GDPR, Art. 5(1)(e).
[62] GDPR, Art. 5(1)(f).
[63] GDPR, Art. 5(2).
[64] GDPR, Art. 1(2).

- the processor will process personal data only on written instructions of the data controller;
- the processor uses all appropriate technical and organizational measures to protect the security of the data;
- (if applicable) the processor will not subcontract to another processor unless instructed to do so in writing by data controller;
- the processor will collaborate with the data controller to uphold their obligations under the GDPR, particularly concerning data subjects' rights;
- the processor agrees to delete all personal data upon the termination of services or return the data to the data controller;

To make personal data available, data controllers must meet one of the legal bases of Article 6 of the GDPR, and for sensitive data additionally the conditions of Article 9. Consent can serve as a legal basis for collecting data for monetization purposes. Data providers must however make sure that the consent meets the criteria of Article 7 of the GDPR, namely that it has been provided unambiguously, it was informed, free and not conditional on the provision of services. The consent remains valid if it has not been withdrawn by the data subject.[65]

It is unlikely that contractual relation with a data subject will be accepted as a legal basis for personal data sharing within the TRUSTS platform. To be able to rely on this legal basis, the data processing must be absolutely necessary in the framework of the normal performance of the contract with the data subject. More elaborated data processing that goes beyond the execution of the contract *sensu stricto* – and that often involves third parties – usually is considered not to fulfil such necessity requirement. In the Guidelines 2/2019, the EDPB specifies that "where processing is not considered 'necessary for the performance of a contract', i.e. when a requested service can be provided without the specific processing taking place, the EDPB recognizes that another lawful basis may be applicable".[66]

The last possible basis to share personal data is where "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject".[67] In sharing personal data in B2B context, the identified purpose might be an economic profit from personal data. Such a purpose may however be considered insufficiently specific to meet the so-called "necessity test". Apart from the necessity test, the legitimacy test must prove that the interest is lawful, sufficiently clear, and represents a real and present interest. Finally, the balancing activity requires to consider data subject rights, freedoms and whether data processing involves profiling. All these considerations make it

[65] Václav Janeček and Gianclaudio Malgieri, 'Commerce in Data and the Dynamically Limited Alienability Rule' (2020) 21(5) German Law Journal 924-943 20.

[66] EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. The Guidelines are available here: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (last visited 11th October 2020).

[67] GDPR, Art. 6(1)(f). See also Article 29 Working Party 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'. The Opinion is available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (last visited 11th October 2020) .

extremely difficult to use the category of legitimate interest as a legal basis for trading personal data. [68] It will be necessary to evaluate on a case-by-case basis. In addition, if the shared data are not only personal, but also sensitive (Article 9(1) GDPR), they can never be processed for legitimate interest purposes. In such a case only the two legal bases apply: (i) "explicit consent for one or more specified purposes" (Article 9(2)(a) GDPR); (ii) when processing relates to "[sensitive] data which are manifestly made public by the data subject" (Article 9(2)(e) GDPR).

Additionally, under the GDPR, data subject consent can be withdrawn at any time.[69] In such a case, the data controller is required to return the data to data subject or/and delete the data and terminate data processing activities. The question raises how will this affect the B2B data sharing contract? Twigg-Flesner argues[70] that one plausible answer to this question would be that by withdrawing the consent for processing data and thereby terminating the licence to use the data, the licence to use the digital content is equally terminated immediately. Alternatively, however, the situation will differ if the personal data related to a data subject who has withdrawn his or her consent has been combined with the personal data of others and processed to produce new datasets. It is argued that "at this point, even though the personal data supplied by the individual who has now withdrawn his consent is no longer available to the trader for further processing, the analytical findings already obtained presumably are beyond the reach of the individual's consent".[71] It is therefore important to monitor the legal basis for data transactions, including consent in case of processing personal data based on consent, as there is a risk for the data sharing contract to be invalidated *ex post.*

[68] ibid.
[69] GDPR, Art. 7(3).
[70] Christian Twigg-Flesner, 'Disruptive Technology – Disrupted Law? How the Digital Revolution Affects (Contract) Law' in Alberto De Franceschi (ed), *European Contract Law and the Digital Single Market* (1st edn, Intersentia 2016) <https://www.cambridge.org/core/product/identifier/CBO9781780685212A016/type/book_part> accessed 25 August 2020.
[71] ibid.

3.3 The E-Privacy Directive and forthcoming Regulation

On the 10th of January 2017, the European Commission released its proposal for a new ePrivacy Regulation ('ePR')[72] replacing the 2002 ePrivacy Directive ('ePD')[73] in the electronic communication sector. The current section will provide details into the ePrivacy Directive and ePrivacy Regulation legal framework.

Even though this legal framework is not of high compliance priority for activities performed in the framework of the TRUSTS project, a few basic concepts are worth mentioning. The main legal notions will be singled out in this section of the deliverable in order to guide the TRUSTS consortium partners.

3.3.1 The ePrivacy Directive

The general obligations derived from the ePrivacy Directive apply to the processing of personal data with regards to the provision of publicly available electronic communications services in public communications networks in the EU.[74] It shall be also noticed that ePrivacy Directive' material scope of application is more extensive and goes beyond electronic communications service providers to include the cookie provision. However, it remains until now very unclear how to interpret this provision and especially how it relates to the GDPR.

An electronic communications service is defined as "*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.*"[75]

The data analytics tools as described in the TRUSTS use-cases do not fall within the scope of this definition, since they do not involve *"wholly or mainly in the conveyance of signals"*. The primary function of the TRUSTS data analytics tools is to perform analytics on data and data service, rather than the conveyance of signals. Consequently, most obligations that apply to providers of electronic communications services will not be applicable to the use-cases of the TRUSTS project.

[72] See, for the original text proposed by the European Commission: Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ('ePrivacy Regulation') (2017) 2017/0003(COD) <http:// data.consilium.europa.eu/doc/document/ST-5358-2017-INIT/en/pdf> accessed 3 April 2018.
[73] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 31.7.2002, p. 37–47 ('ePrivacy Directive').
[74] ePrivacy Directive, Art. 3.
[75] ePrivacy Directive, Art. 2.

At the same time, the concept of consent under the ePrivacy Directive is the same as under the GDPR, meaning that consent must be freely given, specific, informed, and unambiguous.[76] The user must also receive clear and comprehensive information in accordance with the GDPR, including about the purposes of processing.

3.3.2 The ePrivacy Regulation

More than a mere updating exercise, the European Commission's draft suggested to drastically broaden the scope of a normative framework which, until today, mainly focused on telecommunications. Being an integral part of the Digital Single Market strategy, the main objective of the proposal is to provide a high level of privacy protection for users of electronic communications services and a level playing field for all market players. As such, the text deals with various issues, ranging from the confidentiality, storage and erasure of communications to incoming call blocking and marketing communications. While it was initially expected to be finalised before May 2018 – matching the GDPR's entry into force –, ongoing debates in the Council cast serious doubts on the reasonableness of this projection.[77]

On 22 November 2019, the Council rejected the latest version of the ePR.[78] More than two years after the initial proposal, there is still no consensus between Member States on several issues. In December 2019, the European Commission announced that it will present a revised ePrivacy proposal as part of the Croatian Presidency of the EU. As a result of these developments, it is still unclear when, and even whether, an ePrivacy Regulation will eventually be adopted. Among the issues discussed in the Council are: the need to clarify the relationship between ePrivacy and the GDPR, privacy settings, the legal grounds for data processing other than consent, as well as the applicability of the new rules to service providers assisting competent authorities for national security purposes, and the concept of public interests as a basis justifying restrictive measures.[79] In July 2020, the German Presidency published their first discussion paper in order to prepare the work for the following months with the aim of reaching a General Approach and/or a mandate to start negotiations with the European Parliament.[80]

The next section will discuss the scope of application of the ePrivacy Regulation and its relationship with the GDPR.

[76] ePrivacy Directive, recital 17; GDPR, Art. 94; GDPR, Rec. 32.
[77] See, on the progress of the legislative procedure: <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-e-privacy-reform> (last accessed 3 April 2020).
[78] The version of 8 November 2019 available at: <https://data.consilium.europa.eu/doc/document/ST-13808-2019-INIT/en/pdf> (last accessed 10 September 2020).
[79] Legislative train, Proposal for a regulation on privacy and electronic communications available at: https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform (last accessed 10 September 2020).
[80] Council of the EU, Presidency, Discussion paper 9243/20 of 6 July available at: <https://data.consilium.europa.eu/doc/document/ST-9243-2020-INIT/en/pdf> (last accessed 20 October 2020).

3.3.3 Scope of application

The proposed ePR applies to '*the processing of electronic communications content in transmission and of electronic communications metadata carried out in connection with the provision and the use of electronic communications services*'.[81] The scope of application of the proposed ePR is broader than the scope of the ePD. It is therefore crucial to substantiate all the above-mentioned notions in order to circumscribe the ePR's material scope of application.

First, Article 4(3)b ePR defines 'electronic communications content' as '*the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound*'. Second, Article 4(3)c ePR underlines that 'electronic communications metadata' encompass '*data processed by means of electronic communications services for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication*'. Finally, when it comes to the notion of 'electronic communications service', Article 4(1)b ePR refers to Article 2(4) of the proposed Directive establishing a European Electronic Communications Code ('DEECC')[82], which provides the following definition: '*a service normally provided for remuneration via electronic communications networks, which encompasses 'internet access service' as defined in Article 2(2) of Regulation (EU) 2015/2120; and/or 'interpersonal communications service'; and/or services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and service*'.

This legal framework will not be relevant most probably in the context of the TRUSTS platform. However, one should already keep in mind that the text is still being discussed by the Council and the Parliament. Thus, the exact scope and meaning of some core notions are yet to be delineated. Since its very first draft, the proposal has also led to intense controversies among practitioners and legal scholars.[83] Therefore, it is of utmost importance to underline that the following paragraphs might – and most probably will – have to be revised once the final version of the ePR is adopted.

[81] ePrivacy Regulation, Art. 2(1)(a).
[82] Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communication Code (12 October 2016) 2016/0288(COD) available at : <http://eur-lex.europa.eu/ legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN> (last accessed 3 April 2018).
[83] Niko Härting, 'Study on the Impact of the Proposed EPrivacy Regulation' <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/epr_-_gutachten-final-4.0_3_.pdf> accessed 16 January 2018; W Gregory Voss, 'First the GDPR, Now the Proposed EPrivacy Regulation' (2017) 21 Journal of Internet Law; Andrew Cormack, 'The Draft EPrivacy Regulation: No More Lex Specialis for Cookie Processing?' (2017) 14 SCRIPTed 345.

3.3.4 Relationship between the GDPR and ePrivacy legal frameworks

To date, the exact functioning of the TRUSTS platform is currently under specification. To that end, the relationship between the proposed ePR and the GDPR, whose respective material scope of application might partially overlap, must be clarified. However, and as already stressed above, this should be regarded as a preliminary exercise whose outcome might fluctuate depending on the evolution of the legislative text.

While the GDPR seeks to ensure the protection of data subjects' fundamental rights with regard to the processing of their personal data, the proposed ePR complements and particularizes these rules in the broader context of the provision and use of electronic communications services.[84] On the one hand, the proposed ePR guarantees the confidentiality of electronic communications irrespective of whether or not the data involved are considered personal under Article 4(1) GDPR. In that sense, the proposed ePR *complements* the GDPR by applying to situations that would otherwise remain unregulated. On the other, the ePR also partially overlaps with the scope of the GDPR since the definition of 'personal data' and 'electronic communications data' are not mutually exclusive. In that case, the ePR acts as a *lex specialis* and *particularizes* the GDPR by sidestepping its applicability whenever both normative frameworks apply to the same subject matter. This is known as lex specialis derogate.[85]

In other words, one can distinguish three types of data. First, electronic communications data under Article 4(3)a ePR that do not qualify as personal data under Article 4(1) GDPR. In that case, only the rules from the ePR will apply and therefore act as a complimentary normative framework creating rules that are not otherwise foreseen in the GDPR (e.g. confidentiality of electronic communications data),[86] or at least not within the same scope (e.g. when it comes to the protection of legal persons that are excluded from the GDPR, but explicitly covered by the ePR).[87] This could be the case, for instance, for non-personal data transiting through machine-to-machine communications. Second, personal data that do not qualify as electronic communications data. Third, electronic communications data that also qualify as personal data. In this last hypothesis, the ePR will particularise and override the general rules contained in the GDPR. This is particularly relevant when it comes to the legal bases for the processing of personal data listed in

[84] ePrivacy Regulation, Rec. 1 and 2a and Art. 1(3).

[85] This principle, which is the abbreviation of *lex specialis derogat legi generali*, states that if two laws govern the same factual situation, the one governing a specific subject matter (the *lex specialis*) will override the one regulating a general matter (the *lex generalis*). See Trans-Lex <https://www.trans-lex.org/910000/_/lex-specialis-principle/> (last accessed 3 April 2020).

[86] Article 5 ePR introduces a general prohibition of processing that is not foreseen in the GDPR.

[87] Recital 14 GDPR states that '*this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal persons*'. This also follows from the interpretation given by the Article 29 Working Party to the term 'natural person'. However, certain data protection rules might still indirectly apply to information relating to businesses or legal persons whenever the criteria of content, purpose or result allow the information on the legal person to be considered as 'relating to' a natural person (*e.g.* when the name of the legal person follows from the name of the individual). See on that point: Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP136), pp.23-24. On the contrary, the ePR also protects the communications of legal persons (Article 1(2) ePR).

Article 6 GDPR and the permitted processing of electronic communications data enumerated in Article 6 ePR. Where both Regulations apply, controllers will have to comply with the latter rather than the former.

3.4 Anonymisation and pseudonymisation as privacy preserving techniques

This section of the deliverable is a follow-up to the work performed in WP9, in particular in D9.6 on anonymisation and other privacy preserving techniques. Some additional information will be provided in this section on identifiability, linkability and de-anonymisation in order to inform the partners about all the potential risks related to the processing of personal data.

The notion of personal data refers to any information relating to an identified or identifiable natural person (the data subject).[88] The identifiable natural person is an individual who can be identified, directly or indirectly, in particular by reference to an identifier, inter alia a name, an identification number, location data or an online identifier.[89] In this way, these criteria should be interpreted and used, in order to assess whether data on which privacy enhancing or de-identification techniques have been performed, are considered as personal data or as anonymous information and hence whether the GDPR applies or not. More information on anonymization techniques will be provided in WP4 activities.

The GDPR provides for some guidance in order to interpret the concept of an 'identifiable person'. More specifically, according to the relevant recital from the GDPR, "to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".[90] As 29WP has noted, a mere hypothetical possibility to single out the individual is not enough to consider a person as 'identifiable'.[91] In addition, the recital continues by pointing out that "the principles of data protection should therefore not apply to anonymous information, i.e. information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".[92]

Furthermore, according to the CJEU interpreting the abovementioned concept of 'means reasonably likely to be used' in the context of dynamic IP addresses, it is not necessary that all the information enabling the identification of the data subject is in the hands of one person, i.e. the data controller. However, in the case where additional data is required in order to identify the individual, what matters is the means

[88] In legal terminology, a natural person means an individual human being, as opposed to a legal person that may be an individual, company or other entity with specific legal rights and obligations.
[89] GDPR, Art. 4 (1).
[90] GDPR, Rec. 26.
[91] Article 29 Working Party, Opinion 04/2007 on the concept of personal data, WP 136, 30 June 2007, p.15.
[92] GDPR, Rec. 26.

reasonably likely to be used in order to access and combine such additional data.[93] Therefore, dynamic IP addresses, for example, are considered to constitute personal data for online media service providers, who can rely on legal channels in order to obtain the required additional information held by internet service providers, enabling the former to identify the individual behind the said dynamic IP address at a specific moment of time.[94]

The personal or non-personal character of the data depends on the identifiability of the individual based on all means reasonably likely to be used. Identifiability also depends on the actor using such means to identify the individual.[95] In the context of data, on which privacy enhancing or de-identification techniques have been performed, a major factor affecting their identifiability is the operation on the data of the technical process of data anonymization, encryption and splitting. However, while the discussion on the legal effects of anonymization, encryption and other forms of privacy enhancing or de-identification techniques on personal data is ongoing already for some years now, a consensus has yet to be achieved.[96]

On the one hand, there is an absolute approach supporting that data that have undergone such techniques will almost always remain personal as long as anyone in the world is able to identify the individual (for example because they can reverse the process) and also because it is claimed no technique is "perfect" and endurable against future technological developments.[97] On the other hand, a relative, risk-based approach[98] builds on the criterion of 'means that are reasonably likely to be used' in order to identify an individual. Following the latter, privacy enhancing techniques provide for different degrees of de-identification taking into account contextual elements, such as the technical process, the safeguards restricting access to the data and the overall realistic risk of re-identification. In other words, if excessive effort, in technical, organisational and financial terms, is required to have access to the means reversing each privacy enhancing technique, identification of the natural personal may not be considered as likely.

The abovementioned recital from the GDPR[99] also notes the importance of taking into consideration the available technology at the time of the processing and technological developments. However, the process and timing of this consideration is not clear from the wording of the recital. More specifically, it is questionable whether future developments should be also taken into account at the time of the first processing, at a later point of re-assessing and testing or validating the robustness of the privacy enhancing

[93] CJEU 19 October 2016 C582/14 Patrick Breyer v Bundesrepublik Deutschland ECLI:EU:C:2016:779 ('Breyer case') para 43-45.
[94] Ibid, para 47-48.
[95] Article 29 Working Party, WP 136, p. 19-20.
[96] S. Stalla-Bourdillon, A. Knight, 'Anonymous Data v. Personal Data – A false debate: an EU perspective on anonymization, pseydonymization and personal data', Wisconsin International Law Journal, 2017, p. 288-289. Most common points of references also mentioned in the paper above are the following: UK Information Commissioner's Office (ICO) 'Anonymization: Managing data protection risk code of practice', 2012, available at https://ico.org.uk/media/1061/anonymisation-code.pdf and Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP 216, 10 April 2014.
[97] Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' 7 (2016) JIPITEC 169, p. 12-13.
[98] Article 29 Working Party, Statement on the role of a risk-based approach in data protection legal framework, WP 218, 30 May 2014.
[99] See Ref. 41.

technique adopted in each case or on a regular constant basis. According to the 29WP regarding the concept of personal data in their Opinion from 2007, in order to assess identifiability, the whole time period for which personal data will be processed should be taken into account. In this way, if, for example, personal data are due to be processed for a period of 10 years and within this period of time, for instance in the 9th year, technical developments provide for means reasonably likely to be used in order to identify the individuals, then data are personal from that moment in time (i.e. the 9th year) on.[100] Consequently, following this interpretation, the status of data as non-personal or personal will change at the moment when technical developments allow for it.

Furthermore, the common identification risks that have been observed with regards to anonymization and other privacy enhancing or de-identification techniques are singling out, linkability and inference, as will be explained subsequently.[101] These three risks are also considered as criteria based on the lack of which the de-identification technique may be considered as an effective means of turning personal data to anonymous information.[102] A risk of identification due to singling out occurs when there is a possibility to distinguish the data relating to one individual from all other information in a dataset, for example because the individual has a unique value or a unique combination of values, such in a data set which records the height of individuals, where only one person is 190cm tall, that individual is singled out.[103] Moreover, the ability to link identifiers within one or more datasets will make it more likely that an individual is identifiable. In this case, a major risk factor derives from the existence of one or more other sources that may be combined with the set of the privacy enhanced data. For example, taken individually the first and second name "John" and "Smith" might not be capable of distinguishing one of a large company's customers from all other customers, but if the two pieces of information are linked, it is far more likely that "John Smith" will refer to a unique, identifiable individual.[104]

Finally, in some cases, it may be possible to infer a link between two pieces of information in a set of data, even though the information is not expressly or originally linked and deduce the value of an attribute from the values of other attributes. This may happen, for example, due to the inclusion of statistics regarding specific identifiers or values attributed to the individual. To illustrate this more clearly, if a dataset contains statistics regarding the seniority and pay of the employees of a company, although such data would not point directly to the salaries of individuals in the dataset, an inference might be drawn between the two pieces of information, allowing some individuals to be identified.[105] Taking into account these risks as well as the robustness of the privacy enhancing technique, one may estimate the level of effective de-identification. The level of robustness may be further assessed by the strength of the encryption algorithm used, the length of the encryption key and the security of the key management.[106]

[100] Article 29 Working Party, WP 136, p. 15.
[101] Data Protection Commissioner Ireland, 'Anonymisation and Pseudonymisation', available at: https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm Last accessed on 24.10.2017.
[102] Article 29 Working Party, WP 216, p. 11.
[103] ibid.
[104] ibid.
[105] ibid.
[106] Spindler and Schmechel (n 99) 172.

Anonymization, for instance, is considered to provide for different levels of de-identification, and depending first on the technical possibility and then on the risks of re-identification, data may sometimes still be legally considered as personal. As such, according to the absolute approach only data that have been irreversibly anonymized and whose original raw dataset has been deleted may be considered as data that are no longer personal.[107] When personal data are encrypted, the data will always remain personal to the holders or to the authorised users of the decryption key (two way cryptography) while they may even be considered as personal if it is considered that there are means reasonably likely to be used by others for decrypting them.[108] In the opposite case where encrypted data are considered to ensure that no unauthorised party will have access to them, then they no longer refer to an identified or identifiable person.[109] The technique of data splitting aims at fragmenting data in a manner that the split data no longer contain personal information. In a similar way as with encryption, data are considered personal when they are linked back together using again means reasonably likely to be used. Data anonymization, encryption and splitting may be considered as effective, based on the relative approach, the criteria of singling out, link-ability and inference and the concept of 'means reasonably likely to be used'. As such, data are no longer personal when it would require an excessively high effort or cost or it would cause serious disadvantages to reverse the process and re-identify the individual.

In addition to these concepts, the GDPR has introduced the notion and definition of 'pseudonymisation'. More specifically, pseudonymisation refers to the processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[110] Pseudonymisation is commonly perceived as a data security measure that reduces link-ability by replacing any identifying characteristic or attribute by another identifier, a pseudonym.[111] The reason why this new concept is important is because according to the GDPR, pseudonymised data are personal data.[112]

However, what further complicates an already unclear legal field is the interpretation of this new definition and by extension the question whether and to what extent this definition includes privacy enhancing techniques apart from irreversible anonymisation. In particular, the interpretation of 'additional information' may be either very broad, so as to include, for example, the technical means able to reverse a privacy enhancing technique, such as a decryption key, or rather narrow referring to actual information in the sense of direct identifiers regarding the natural person under identification.[113] In following a more broad interpretation linked to the absolute approach on privacy enhancing techniques, data could be

[107] Article 29 Working Party, WP 216, p. 5.
[108] W. Kuan Hon, Ch. Millard and I. Walden, 'The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing', International Data Privacy Law, 2011, Vol. 1, No. 4, p.219.
[109] Spindler and Schmechel (n 99) 169.
[110] GDPR, Art. 4 (5).
[111] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP 216, p. 20.
[112] GDPR, Rec. 26.
[113] S. Stalla-Bourdillon, A. Knight, Anonymous Data v. Personal Data – A false debate: an EU perspective on anonymization, pseudonymization and personal data, p. 300-301.

considered pseudonymised, and hence personal, insofar as the technical process they have undergone is reversible. Moreover, 29WP explicitly refers to encryption with secret key as one of the most used pseudonymisation techniques.[114] Be that as it may, it remains questionable whether reversibly anonymised, encrypted and split data will always be considered personal, as pseudonymised data, or whether they will be rendered 'anonymous information' towards the parties that cannot access the additional information, reverse the respective technical process and identify the individual using means reasonably likely to be used, according to the abovementioned analysis.[115]

Finally, it should be pointed out that most analyses of the concept of personal data, the means reasonably likely to be used and the legal effects of privacy enhancing techniques, as presented in this sub-section, adopt the view point of the data controller, in the sense that they are focused on the conclusion of whether the data controller holds the means reasonably likely to be used in order to identify the data subject and hence whether data are personal vis-à-vis the data controller.

[114] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP 216, p. 20.
[115] Spindler and Schmechel (n 99) 171.

4 Regulation of data as an (economic) asset

Data market ecosystems are based on the consideration of data as an economic asset, which can be traded in its own right, otherwise called the 'commodification' of data. Up to now, the legal framework has generally not followed this economic and business pattern. It is generally agreed in the legal scholarship that there is not – nor *should there be* - an ownership right on data. The misalignment between the legal framework and the economy reality may constitute an obstacle for data markets to flourish. As the case of data reminds us (but this is certainly not specific to data), the 'market' does never exist or flourish without a sustaining infrastructural legal system to bring trust.

The topic is immense and this section cannot provide an exhaustive overview of the on-going legal debates. It will focus on a few targeted aspects. On the legislative side, the section will first outline the latest developments in EU law with respect to data exchange and to what is generally called now the "free flow of data", with an introduction to the Free-Flow of Data Regulation. The second sub-section focusses on 'data sovereignty'. This technology is contemplated by the partners as a means to support data transactions in a data market. With data sovereignty, technology could play a *regulatory* role, which obviously requires to better understand the interfaces with the law. Finally, the third and last sub-section will outline the on-going institutional debates on future regulation of data, which could be of relevance for data markets. Chapter 4 has strong connections to Chapter 6, which deals with the economic regulation of data transactions more generally. Both chapters should therefore be viewed as complementary one to the other.

4.1 The Free Flow of Non-Personal Data Regulation

In 2018, the Regulation on a framework for the free flow of non-personal data in the EU ('Regulation on the free flow of non-personal data')[116] was adopted. The purpose of the EU legislator with the Regulation is to remove (some) obstacles hampering the "free flow of data" in the EU. The free flow (or movement) of data in the EU is viewed as the fifth freedom of movement, after the freedom of movement of goods, services, capital and persons enshrined in EU primary law.[117] While this "fifth freedom" interpretation of the Regulation is questionable from a legal perspective, it remains true that the Regulation is the first legislative initiative applying expressly to "non-personal data" as a regulatory subject-matter. The

[116] 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, OJ L 303/59, (Free Flow of Non-Personal Data Regulation).

[117] This "fifth freedom" interpretation was held by EU institutions and then spread easily amongst analysts, see the press release of the European Parliament, Free flow of non-personal data: Parliament approves EU's fifth freedom, 04.10.2018. The press release is available here: https://www.europarl.europa.eu/news/en/press-room/20180926IPR14403/free-flow-of-non-personal-data-parliament-approves-eu-s-fifth-freedom (last visited 30th July 2020).

processing of personal data is subject to the GDPR,[118] with both the objectives to protect the fundamental rights to privacy and data protection of natural persons with respect to the processing of data related to them[119] and to ensure "the free flow of personal data between Member States".[120] With the Regulation on the free flow of non-personal data, the EU legislator aimed to enact a regulatory counterpart in order to ensure the free flow of other, namely non-personal, data.[121]

This section aims to introduce the Regulation on the free flow of non-personal data in the context of TRUSTS. The new legal notion of "non-personal data" will first be defined and its unclear identification vis-à-vis personal data will be discussed. In the second sub-section, the main legal provisions of the Regulation will be introduced.

4.1.1 Personal v non-personal data

a) Non-personal data: a default definition

With respect to its scope *rationae materiae*, the Regulation applies to 'non-personal data', namely "data other than personal data".[122] More specifically, the Regulation applies to "the processing of electronic data other than personal data in the Union, which is (a) provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the Union; or (b) carried out by a natural or legal person residing or having an establishment in the Union for its own needs".[123] (Non-personal) data is defined in the Regulation as "data other than personal data as defined in point (1) of Article 4 of [the GDPR]".[124]

As a reminder, "personal data" are defined in the GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". In other words, the definition of non-personal data is meant as a negative one. One first has to enquire whether the data in question consist in "personal data" within the meaning of the GDPR. Failing that, the data shall qualify as "non-personal data", subject to the Regulation on the free flow of non-personal data. Recital 9 provides examples of 'non-personal data', such as "aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines". The Regulation accounts for the possibility that non-personal data (when

[118] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1.
[119] GDPR, Rec. 1 to 3.
[120] GDPR, Rec. 3.
[121] GDPR, Rec. 8 to 11.
[122] Free Flow of Non-Personal Data Regulation, Art. 1.
[123] Free Flow of Non-Personal Data Regulation, Art. 2 (1).
[124] Free Flow of Non-Personal Data Regulation, Art. 3 (1).

anonymised data) may be turned into personal data, in which case such data should be treated as personal data.

The notion of 'non-personal data' was first introduced in the legislation with the Free Flow of Non-Personal Data Regulation, but then further used in other documents from the European Commission, such as the 'Guidance on sharing private sector data in the European data economy' (Staff Working Document) of 2018,[125] further discussed in Section 6.2.1.

b) Interface between the Free Flow of Non-Personal Data Regulation and the GDPR

While this definition would suggest an impervious partition between 'personal data' on the one hand and 'non-personal data' on the other, it is clear that the data economy is based on the processing of large datasets comprised of a mix of both types of data. Art. 2 (2) clarifies that "in the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of [the GDPR]". However, this provision leaves us with two main questions as for whether and how concretely the Regulation applies to the grey zone of datasets composed of both personal and non-personal data remains indeed unclear. First, how should the expression "inextricably linked" be interpreted? Second, in case of mixed datasets where personal and non-personal data are 'inextricably linked', does the Regulation apply and, if so, to what extent?

The Regulation tasks the European Commission with the duty to submit a report until 29 November 2022 evaluating the implementation of the Regulation, *i.a.* in respect of "the application of the Regulation, especially to data sets composed of both personal and non-personal data in the light of market developments and technological developments which might expand the possibilities for deanonymising data".[126] Until then, the European Commission shall publish "informative guidance on the interaction of the Regulation and [the GDPR], especially as regards data sets composed of both personal and non-personal data", by 29 May 2019.[127] The European Commission published indeed Guidance on the Regulation on 29th May 2019.[128] In line with the exclusive competence of the Court of Justice of the European Union to interpret EU law and as recalled by the European Commission, the Guidance provides no "authoritative interpretation" of the legal provisions. In other words, the document is not legally binding. The European Commission discusses the case of anonymised data, namely personal data which have been processed so that the individuals can no longer be identifiable, and recalls the case law of the CJEU in that respect. The issue of anonymised data and reidentiability is not discussed further here. For further elaboration on that, see Deliverable 9.6 and [WP4]. The Guidance provides a broad definition of the expression 'inextricably linked' – i.e. encompassing both technical and economic elements - whereby

[125] European Commission, 'Staff Working Document, Guidance on Sharing Private Sector Data in the European Data Economy Accompanying the Document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a Common European Data Space"' SWD(2018) 125 final.
[126] Regulation on the free flow of non-personal data, Art. 8 (1).
[127] Regulation on the free flow of non-personal data, Art. 8 (3).
[128] European Commission, Communication to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250 final.

"separating [personal from non-personal data] would either be impossible or considered by the controller to be economically inefficient or not technically feasible", e.g. in the case where it would require the duplication of the software. The Guidance also reckons the "changing nature of data", namely the fact that labelling some data as "personal" is contextual. In any case, neither the GDPR nor the Regulation mandate businesses to "separate the datasets". According to the Guidance, in the case of a mixed dataset where personal and non-personal data are 'inextricably linked', "the data protection rights and obligations stemming from the GDPR fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset". While the interpretation of "inextricably linked" is to be welcomed, the Guidance does not conclusively clarify *how* the Regulation applies in the case of mixed datasets with personal and non-personal data where the GDPR would concurrently apply. The Guidance only states the obvious, namely that the GDPR is fully applicable to such datasets.

Our interpretation of Art. 2 (2) of the Regulation with respect to mixed datasets with personal and non-personal data inextricably linked is the following. a) The GDPR applies to the processing of such datasets, following the provisions of the GDPR and the clarification provided by the European Commission in the Guidance. b) While the Regulation on the free flow of non-personal data applies to the processing of such data as a rule, Art. 2 (2) does not expressly lay down an exception to such rule. As a result, the Regulation shall remain applicable to the processing of mixed datasets inextricably linked as well. c) Both the GDPR and the Regulation on the free flow of non-personal data are therefore concurrently applicable. Art. 2 (2) shall be interpreted as meaning that**, in case of contradiction between two provisions**, the provision of the GDPR shall prevail over this of the Regulation on the free flow of non-personal data. Art. 2 (2) **shall therefore be interpreted as a rule of prevalence**.

The European Commission states in its Guidance that "there are no contradictory obligations under the [GDPR] and the Free Flow of Non-Personal Data Regulation", which sounds bizarre given the very ambition of Art. 2 (2) to regulate the interface between the two legal instruments *in case of contradiction.* Anyways, such statement is not based on a thorough legal analysis. Theoretically, nothing prevents contradictions between the two legal instruments in a given situation. This is especially so because (as further discussed in sub-section 4.1.2), both legislative instruments do not regulate relationships between the same entities, as also highlighted by the European Data Protection Supervisor ('EDPS'). For example, the 'B2B data portability' provision of the Free Flow of Non-Personal Data Regulation' of Art. 6 could well overlap with the privacy of individuals in the case where personal data would be involved.[129] In such case (and without prejudice to the equivocal nature of the 'light touch' regulation in Art 6., which is further discussed in sub-section 4.1.2), would the 'data portability' afforded to the businesses (i.e. professional users of data

[129] European Data Protection Supervisor (EDPS), Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union, 8 June 2018, 5. The comment is available here: https://edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-framework-free-flow-non-personal-data_en (last visited 31st July 2020).

processing services) be applicable?[130] This being said, the scope of application of the Free Flow of Non-Personal Data Regulation is illustrated by Figure 1.

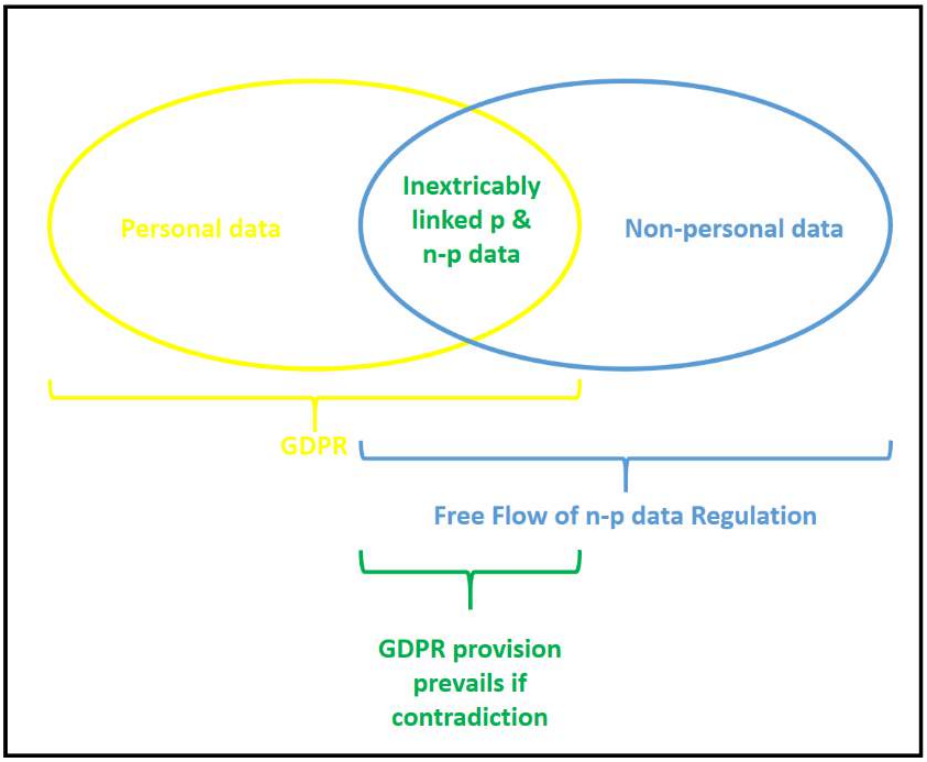

Figure 1: The interface between the application of the GDPR and the Free Flow of Non-Personal Data Regulation

c) Intermediary conclusion: critical remarks

The introduction of the notion of 'non-personal data' in EU law has been received with caution by the legal scholarship. The "dynamic nature of the notion of personal data"[131] in the data economy makes it difficult, if not squarely impossible, to identify 'non-personal data' once and for all.[132] The blurred delineation between the two legislative instruments were also found to likely result in strategic over-compliance with data protection rules from businesses in order to shield themselves from the obligations stemming from

[130] On the issue of B2B data portability, see also Inge Graef, Raphael Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation' (Social Science Research Network 2018) SSRN Scholarly Paper ID 3256189 8–9 <https://papers.ssrn.com/abstract=3256189> accessed 29 July 2019.

[131] ibid 4.

[132] For this reason, Graef, Gellert and Husovec consider that "the notion of personal data is too dynamic, fluid and open-ended to provide a foundation for a new regime *that would only apply when no personal data is at stake*" (emphasis added), ibid. While the argument holds true, our understanding is *not* that the Free Flow of Data Regulation would apply only where no personal data are at stake (see above). It could apply to the processing of mixed datasets, subject to a rule of prevalence to the benefit of the GDPR in case of contradictory provisions.

the Free Flow of Non-Personal Data Regulation.[133] Our view is that the ambit of the Free Flow of Non-Personal Data Regulation to constitute a counterpart to the GDPR concerning the free flow of 'non-personal data' constitutes the root cause for these legal issues. It is grounded on a misconception of the GDPR as 'the law of personal data' while there should also be a 'law of non-personal data'. The GDPR does however not regulate (personal) data as a monolithic subject-matter but rather the *processing* of data which, at some point and in some circumstances, relate to individuals, such processing having the potential to interfere with their fundamental rights. In other words, the GDPR is not a 'data law'. Its application is notoriously much contingent on the context of processing, not only with respect to the risks to individuals' fundamental rights but also (and even) with respect to the very identification of data as "personal", which is a relational or 'situational' notion.[134] Additionally, while the GDPR regulates the processing of personal data for "the protection of natural persons"[135] – and consequently prohibits restrictions to the free movement of personal data with the EU for related reasons -, its scope does not extend to the regulation of personal data (processing) for other reasons. For this reason, "personal data can [obviously] be simultaneously regulated by various regimes".[136] It is probably the growing commodification of data in the data economy – or in other words the perception of data as a stand-alone product which can be 'exchanged' – that has led to such misconception. In summary, just like the GDPR is not 'the law of personal data', the Free Flow of Non-Personal Data Regulation cannot be the 'law of non-personal data'.

4.1.2 Main provisions of the Free Flow of Non-Personal Data Regulation

With the purpose to ensure the free movement (or free flow) of non-personal data in the EU, the Regulation sets up to remove two main obstacles: (1) data localisation requirements put in place by Member States' authorities; (2) As demonstrated by the preparatory works, data localisation requirements arise from "a lack of trust in cross-border data processing, deriving from the presumed unavailability of data for the purposes of the competent authorities of the Member States, such as for inspect and audit for regulatory or supervisory control".[137] For this reason, the Regulation also clarifies under which conditions competent authorities can request or obtain access to cross-border data. (3) Finally, the Regulation also tackles vendor lock-in practices in the private sector.

a) Free movement of data within the EU – prohibition of data localization requirements

The Regulation lays down the principle of data localisation requirements [by Member States' authorities]. 'Data localisation requirement' is defined broadly as "any obligation, prohibition, condition limit or other requirements provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU,

[133] ibid 10.
[134] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40.
[135] GDPR, Art. 1 (3).
[136] Graef, Gellert and Husovec (n 130) 13.
[137] Free Flow of Non-Personal Data Regulation, Rec. 24.

which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State".[138]

In turn, the processing of data is broadly defined as "any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[139] Recital 17 clarifies that this broad definition of 'data processing' encompasses "the usage of all types of IT systems, whether located on the premises of the user or outsourced to a service provider. It should cover data processing of different levels of intensity, from data storage (Infrastructure-as-a-Service (IaaS)) to the processing of data on platforms (Platform-as-a-Service (PaaS)) or in applications (Software-as-a-Service (SaaS))".

By way of exception, data localisation requirements can however be adopted in case justified by public security and subject to the principle of proportionality. Any existing or draft regulation amounting to a data localisation requirement shall be notified to the European Commission, which conducts a compliance audit. The details of data localisation requirements shall be made publicly available by Member States via a national online single information point. Such prohibition does not apply to data localisation requirements based on EU law.

b) Data availability for competent authorities – access to cross-border data

The fear to loose jurisdiction over data is one of the main reasons why Member States(' public authorities) impose data localisation requirements. Art. 5 of the Regulation aims to alleviate such fears, by providing measures to ensure "data availability". "Access to data by competent authorities may not "be refused on the basis that the data are processed in another Member States". Rec. 25 clarifies that obligations to provide access to data can for instance be fulfilled by users by "providing and guaranteeing effective and timely electronic access to the data to competent authorities, regardless of the Member State in the territory of which the data are processed". The recital further indicates that such access "can be ensured through concrete terms and conditions in contracts between the natural or legal person subject to the obligation to provide access and the service provider". The Regulation also aims to ensure that competent authorities dispose of tools to have such requests for access enforced.

Strangely enough, Art. 5 (4) reads: "Member States *may* impose effective, proportionate and dissuasive penalties for failure to comply with an obligation to provide data, in accordance with Union and national law", which suggests that failure to comply with such obligations could, just as well, not be subject to sanctions (emphasis added). Aside from penalties, Member States may impose interim measures on such users in case of "abuse of rights", where justified by "the urgency of accessing the data and taking into account the interests of the parties concerned". The (undefined) expression "abuse of rights" however suggests that a mere failure to comply with a request for access to data would not suffice to trigger such

[138] Free Flow of Non-Personal Data Regulation, Art. 3 (5).
[139] Free Flow of Non-Personal Data Regulation, Art. 3 (2).

interim measures. Interim measures may include "re-localisation of data", however subject to the conditions laid down in Art. 5 (4).[140]

In case a competent authority does not obtain access to user's data upon request and provided there is not specific cooperation mechanism under EU law or international agreements to exchange data between competent authorities of different Member States,[141] "that competent authority may request assistance from a competent authority in another Member State" in accordance with the procedure set up by Art. 7 of the Regulation. Concretely, each Member State shall set up and designate a "single point of contact" which should "liaise with the single points of contact in other Member States and the Commission regarding the application of th[e] Regulation".[142] Requests for access to data shall be submitted by the competent authority in one Member State to the designated single point of contact of other Member State, with a statement of reasons and the legal base(s) for seeking access to such data.[143]

c) Porting of data

With respect to the removal of obstacles to the free movement of data initiated by private actors, the Regulation aims to allow for the 'porting of data' for professional users in order to avoid anticompetitive vendor 'lock in'. Lock in can be due to "a specific data format" or to "contractual arrangements" imposed by the data processing service provider.[144] Data portability is deemed to allow users to "choose freely between providers of data processing services and thus ensure effective competition in the market".[145] Data portability is not defined in the Regulation, but obviously follows the right to data portability afforded to data subjects in the circumstances defined in Art. 20 GDPR. Art. 6 of the Regulation aims more generally at easing switching between data processing service providers.

Strangely enough, the Regulation does not directly target such service providers but rather the European Commission as regulated entity. The Commission shall "*encourage* and *facilitate the development* of self-regulatory codes of conduct at [EU level], in order to contribute to a competitive data economy, based on the principle of transparency and interoperability and taking due account of open standards" (emphasis added). The expression "code of conduct" is not defined in the Regulation either. A definition of "code of conduct" can be found in the Unfair Commercial practices Directive,[146] where it refers to "an agreement

[140] The expression is also not further clarified in the related Rec. 28 of the Regulation.
[141] A number of such cooperation instruments do exist, depending on the subject matter, such as "in the area of police cooperation, criminal or civil justice or in administrative matters respectively, Council Framework Decision 2006/960/JHA, Directive 2014/41/EU […], the Convention on Cybercrime of the Council of Europe, Council Regulation (EC) 1206/2001, Council Directive 2006/112/EC, and Council Regulation (EU) 904/2010", Free Flow of Non-Personal Data Regulation, Rec. 26.
[142] Free Flow of Non-Personal Data Regulation, Art. 7 (1).
[143] For further details on the process for cooperation between authorities, see Free Flow of Non-Personal Data Regulation, Art. 7. For further details on access to the premises of a natural or legal person, see Art. 5 (3).
[144] European Commission, Communication to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250 final, section 4.1.
[145] ibid.
[146] 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

or set of rules not imposed by law, regulation or administrative provision of a Member State which defines the behaviour of traders who undertake to be bound by the code in relation to one or more particular commercial practices or business sectors".[147]

The codes of conduct shall cover "inter alia" aspects related to the following items:

- "Best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data;
- Minimum information requirements to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information regarding the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or port data back to its own IT systems;
- Approaches to certification schemes that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services. Such approaches may include, inter alia, quality management, information security management, business continuity management and environmental management;
- Communication roadmaps taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders".

The European Commission shall "ensure that the codes of conduct are developed in close cooperation with all relevant stakeholders, including associations of SMEs and start-ups, users and cloud service providers". As for the deadlines, the European Commission shall "encourage" service providers to complete the development of such codes by 29 November 2019 and "to effectively implement them by 29 May 2020". In its Guidance on the Regulation, the European Commission gives examples of such codes of conduct developed by the cloud industry: the 'EU Cloud Code of Conduct' developed "on the basis of" data protection law, the Code of Conduct of the Cloud Infrastructure Services Providers in Europe (CISPE) concerning cloud computing service providers acting as 'processors' within the meaning of data protection law, the Cloud Security Alliance's Code of Conduct for GDPR Compliance.[148] In her website, the European Commission also refers to cloud stakeholder working groups working on the development of codes of conduct for cloud switching and cloud security certification.[149]

97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149/22.

[147] Unfair Commercial Practices Directive, Art. 2 (f).

[148] European Commission, Communication to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250 final, section 4.2.

[149] European Commission, Cloud stakeholder working groups start their work on cloud switching and cloud security certification, 16 April 2018, available here: https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security and https://ec.europa.eu/digital-single-market/en/dsm-cloud-stakeholder-working-groups-cloud-switching-and-cloud-security-certification (last visited 3rd August 2020).

In brief, there is no obligation for individual service providers to respectively grant a data portability right to their professional customers. Services providers are indeed not addresses of the Regulation and bear therefore no direct obligation. This being said, they should contribute to the development of codes of conduct collectively e.g. via their representing associations. Just like codes of conduct are not defined in the Regulation, their legal value is also not clarified. One could expect that, upon completion, codes of conduct would be endorsed by the concerned service professionals and could thus constitute contractual material in their relationships with professional customers. For lack of regulation of that aspect in the Regulation, the legal value of codes of conduct would depend on the circumstances of the cases. In case of breach of codes of conduct by service providers, it would be up to national courts, subject to national law (e.g. contract law and economic law more generally), to decide on potential sanctions.

Finally, and as mentioned above, how codes of conduct and data porting could interact with data protection law (the GDPR) remains an open question. In the case where professional users would have personal data processed by service providers and subject to case-specific analysis, data portability is likely to be surpassed by data protection law.

d) Evaluation and follow-up

The Regulation is directly applicable and does therefore not require transposition by Member States.[150] The European Commission shall monitor the implementation of the Regulation throughout the EU and report by 29 November 2022. Should the provisions laid down by the Regulation not appropriately remove the obstacles to the free movement of data, it cannot be excluded that the European Commission would thus make new (legislative) proposals then.

[150] Free Flow of Non-Personal Data Regulation, Art. 9.

4.2 Data sovereignty

4.2.1 Introduction – no data ownership but a patchwork of legal frameworks regulating data

Data are increasingly viewed by industry players as a commodity to be traded in their own right. It is obviously particularly so in data markets. Concurrently to this pattern, there is a growing interest from policy-makers in data markets, viewed as a means to foster data sharing and to incentivise brick-and-mortar industry to enter the data economy.

The legal framework is not quite well-aligned with this new pattern towards commodification of data. On the one hand, it is generally agreed that there is no "ownership right" on data in the Member States of the European Union. Most legal scholars also consider that such an ownership right *should not* be set up, due to the specific nature of data. Thus, data can legally not be 'sold' like a table or a watch. On the other hand, a variety of legal frameworks may apply to data and to data transactions, subject to context-specific analysis of the latter. To give a (non-exhaustive) taste of it, data protection law is applicable when personal data are at processed, copyright protection may apply as well as the legal protection of databases. The dataset may be legally protected as trade secret or otherwise subject to contractual arrangements, such as non-disclosure agreement or limitations of (re)use. In additional to that, sectoral legislation may lay down various types of obligations relating to data directly or indirectly, such an obligation to provide access for third parties to reuse the data, or alternatively confidentiality or secrecy obligations, etc. The legal frameworks have indeed accumulated over time, with various rationales. In contrast, the question of whether and how data could be turned into a tradeable asset is a rather new one. Even 'data' as a subject-matter is a rather new construct in the legal thinking. The patchwork of legal frameworks applying to data (transactions) may make it more difficult to 'trade' data, because of uncertainty that it brings about and of the context-specific nature of the legal analysis. This being said, a great array of options can be arranged by transacting parties, by means of a contract.

As a matter of fact, data transactions are mainly regulated by contracts between data 'providers' and data 'users', subject to complementary contractual relationships with potential intermediaries. The extent to which contracting parties may freely decide upon the conditions for data transactions depends upon many elements, e.g. whether personal data are processed, the nature and market power of contracting parties, the purpose for the (re)use of data, etc. The whole deliverable is dedicated to the identification of the legal conditions in which data can be transacted between parties.

This section focusses on the notion of 'data sovereignty', which is often put forward as a means to supersede the absence of 'data ownership'. The notion of data sovereignty has a doubled-edged sword relationship with the law. On the one hand, data sovereignty is based on the existence of a contract between data provider and data user and is therefore reliant on the law. On the other hand, data sovereignty is characterised by a technological enforcement of such contract, deemed more efficient and thus more satisfactory especially for the data provider. Data sovereignty has no institutional or legal meaning and significance, nor does it have a consensual definition and technical operationalisation. This

stands in the way of a comprehensive legal analysis of this notion, which requires concrete arrangements, both at business and technical levels, not yet in place at this stage of the development of the TRUSTS research project. For this reason, the remainder of this section will discuss the notion of 'data sovereignty' based on the definition of features elaborated by the International Data Spaces Association ('IDSA'), particularly in its reference architecture model. In order to provide a first outline of the relationship between the data sovereignty and the law, this section will first look into this new notion in the broader context of increased calls for "sovereignty" in the digital environment. In a second sub-section, the double-edged sword relationship of the notion of data sovereignty with the law is introduced.

4.2.2 The notion of 'data sovereignty'

The notion of 'data sovereignty' has no legal or official meaning. Although increasingly referred to in public relations documents, data sovereignty is not a clear notion. In order to understand the notion of data sovereignty, this section first looks into the notion of 'sovereignty', which does have a precise legal meaning. Then, it briefly outlines the increasing number of references to the term 'sovereignty' in the digital era, before turning to 'data sovereignty' as part of this pattern.

a) 'Sovereignty': the legal definition

The Cambridge dictionary defines sovereignty as "the power of a country to control its own government".[151] Sovereignty is indeed associated with **States rather than individuals.** Sovereignty is the most fundamental principle of public international law. It refers to the "supreme authority within a territory". The system of United Nations is based on the sovereignty principle, so that States are deemed equal in the international community.[152] A corollary to the principle of sovereignty is the non-interference principle so that sovereign States are protected by the UN Charter against interventions by other States "in matters which are essentially within their domestic jurisdiction" (namely their *domaine réservé).*[153]

b) Digital sovereignty

Sovereignty has recently gained traction amongst the EU institutions with respect to the cyberspace and/or to the digital era, with the increased use of terms such as 'technological sovereignty' and 'digital sovereignty'. The European Parliamentary Research Service ('EPRS') published an "ideas paper" on digital sovereignty in 2020, which summarizes the debate on this matter. According to the EPRS, the call for technological or digital sovereignty arises from the concerns raised over "the economic and social influence of non-EU technology companies, which threatens EU citizens' control over their personal data, and constrains both the growth of EU high technology companies and the ability of national and EU rule-makers to enforce their laws". As a policy response, digital sovereignty refers to "Europe's ability to act

[151] See the online Cambridge dictionary, https://dictionary.cambridge.org/dictionary/english/sovereignty (last visited 28th September 2020).
[152] Samantha Besson, 'Sovereignty', *Oxford Public International Law* (Oxford Public International LAw 2011) <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472> accessed 28 September 2020.
[153] ibid.

independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)".[154] Unsurprisingly, the call for digital sovereignty arises from a perceived lack of control. What is noteworthy, however, is the fact that sovereignty seems to be attached not only to Member States and the EU, with reference to their ability to have jurisdiction over data (processing), but also to individuals and companies, such phenomenon being entirely alien to the legal system. Sovereignty as the power to have control over oneself' government is indeed reserved to States, as outlined above. By contrast, individuals and companies are legally bound to comply with laws that are imposed by the sovereignty States.

c) The 'taking back control' paradigm

The use of the term 'sovereignty' for individuals and companies has become part of everyday language in various circumstances. For example, sovereignty is sometimes associated (even by legal scholars) with consumers where the expression 'consumer sovereignty' is grandly used as a substitute to, simply, consumer choice.[155] As illustrated in the 'ideas paper' of the EPRS discussed above, (data) sovereignty is also sometimes associated with data subjects with respect to the control that they should get back on 'their' personal data.

Similarly, the term 'sovereignty' is much used in the context of the blockchain technology, in order to convey the idea that users could thereby control the assets that they entrust to a blockchain network. R. Herian interestingly observes that both scenarios of 'data subjects' sovereignty' and 'sovereignty by blockchain' (or 'self-sovereignty') are based on a "taking back control" narrative although such a control is never truly possible. While 'sovereignty' seems to imply empowerment of the data subject, R. Herian argues that sovereignty of both data subjects and blockchain users is grounded in the idea that they would act as "engaged economic subjects within the ambit of neoliberal capitalism". Such an ideal of self-sovereignty implies an economisation of "all social life" such that individuals would "realise their own value" or in other words they would actively contribute to the exploitation of personal data relating to them ("auto-exploitation").[156] Something that data protection is supposed to prevent (i.e. based on the principles of purpose limitation, necessity and proportionality). In this respect, the attempts towards monetising the value of personal data so that individuals get a 'fair share' of 'their' data are situated on the same slippery slope.

d) 'Data sovereignty': the IDSA concept

The expression 'data sovereignty' has been broadly promoted by IDSA and lies at the heart of the IDSA 'reference architecture model'. It is defined as "a natural person's or corporate entity's capability of being

[154] EPRS, 'Digital Sovereignty for Europe' (EPRS, European Parliament 2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf>.
[155] Jörg Hoffmann, 'Sector-Specific (Data-) Access Regimes of Competitors' (Max Planck 2020) Max Planck Institute for Innovation & Competition Research Paper 20–08 <https://papers.ssrn.com/abstract=3613798> accessed 28 September 2020.
[156] Robert Herian, 'Blockchain, GDPR, and Fantasies of Data Sovereignty' (2020) 12 Law, Innovation and Technology 156.

entirely self-determined with regard to its data".[157] Data sovereignty is the main goal of IDSA as a means to finding "a balance between the need for protecting one's data and the need for sharing one's data with others". In the IDSA reference architecture model, data sovereignty has several related components. It implies no central storage of data, which remains with the owner until it is transferred to a trusted party. Data sovereignty "materialises in 'terms and conditions' that are linked to data before it is exchanged and shared". On the "information layer", the "Connector" ensures that "the data sovereignty of the Data Owner is always guaranteed" (sic.). The Connector is a "dedicated software component allowing Participants to exchange, share and process digital content". Technical enforcement requires, *i.a.,* tracking of data "provenance and lineage". According to IDSA, data sovereignty is at the core of data markets. It should be associated with data monetisation.

The following sub-section turns to the relationship between the notion of data sovereignty and the law.

4.2.3 Data sovereignty and the law: an ambivalent relationship

a) Introduction and rationale of data sovereignty

Data sovereignty is not intended to substitute the law but to 'complement' it, by providing technical enforcement. In short, the baseline hypothesis for the promotion of data sovereignty lies in the perceived lack of control of one over 'his' data, once such data are shared or exchanged (broadly speaking: transacted). While it is always possible to lay down contractual restrictions to the reuse of data by the contracting party (e.g. a given period of time, a given purpose, prohibition of sharing with third parties, etc.), enforcement is in practice very difficult since infringement would often go unnoticed. In addition to that, contractual terms are only enforceable against the contractual parties and not against third parties who may end up unduly holding the data. It results in a chilling effect from industry players to transact 'their' data, deemed to be detrimental not only to them as a missed business opportunity, but also to the economy as a whole since new technologies – and particularly AI – requires more data sharing. Data sovereignty would therefore provide an alternative enforcement to this – deemed insufficient – of the law. This being said, data sovereignty relies on legal provisions and should be compliant with them.

b) Scope

As a matter of scope delineation, the question whether individuals could use the IDSA 'data sovereignty' to 'sale' 'their' data is not discussed here. The TRUSTS data market platform may happen to process personal data but such data would be exchanged *by industry players and not by the said individuals*. This does however not mean that data protection law is out of scope. When processing – and particularly transacting – datasets including personal data, industry players remain indeed at all times responsible for compliance with data protection law.

c) Contract law: the cornerstone of data sovereignty

[157] IDSA, 'Reference Architecture Model Version 3.0' <https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf>.

Data sovereignty openly relies on contracts, be they implicit or explicit. A legal contract is simply defined as an agreement vested with legal character.[158] A contract is essentially forward-looking: the parties agree when concluding the contract to respectively execute a duty in the future, subject to legal enforcement. Contracts govern the willingness of the parties to perform an agreement. At the *very least*, the parties indeed intend to bind each other with respect to the result of the data transaction. In other words, the parties expect the other parties not to *legally* challenge the result of the transaction (i.e. before a Court).

While the existence of a contract between the data provider and the data user (contract A) is obvious, data sovereignty implies the existence of other contracts. There should indeed also be a contract between them and the provider of the 'Connector' and/or of other technical means to enforce the contract (contract B), namely to use such technical means. What can precisely be expected by data providers and data users from the Connector and/or from other such technical means should be laid down in this contract. The nature of the platform and the identification of the roles respectively played by intermediaries remains to be decided in the TRUSTS project. Should it be deployed in real-life scenarios, such intermediary roles would similarly entail the existence of contracts, i.e. with respect to the use of (blockchain-based?) smart contracts.

d) Data sovereignty as contract-based technological property?

While purposively relying on (legal) contracts, data sovereignty aims to go 'beyond' contracts by enforcing technically the conditions agreed between the parties, and in particularly by the data provider for the (re)use of 'his' data. The notion of data sovereignty can be qualified as technological appropriation. Data providers can do 'as if' they were 'data sovereign', in the sense that they can design and have technically enforced the conditions and limitations that they want to impose on any (re)use of 'their' data. Such a mechanism 'looks like' ownership. It mimics contracts of sale or lease, by which good owners grant certain rights on their good to a counterpart, based on property rights. While data are ubiquitous, easily duplicable and therefore non rival goods so that they would not be fit to exclusive rights and enclosure, data sovereignty provides a technical fix. Data sovereignty goes beyond that, by ensuring (or promising to ensure) technical enforcement of contractual provisions. However, it remains unclear at this stage to what extent and how concretely data sovereignty can truly deliver these promises.

Against that background, data sovereignty seems to share similarities, at least on a conceptual level, with blockchain-based smart property or otherwise called blockchain-enabled property, based on tokenisation of everything and especially of data.[159] By creating rivalry of tokens and by enabling their exchange based on blockchain networks without the recourse to trusted intermediaries, the blockchain technology has been deemed to display property management capabilities, both to create property and to support the allocation and exchange of such digital goods. However, while the reach of the blockchain would be limited to on-chain assets (namely, the blockchain tokens), the notion of data sovereignty brings about technical

[158] See for instance the definition of a contract in Belgian law: "The contract is an agreement by which one or several parties oblige herself / themselves to one or several parties to give, do, or not do something" (art. 1101 Belgian Civil Code (freely translated from French version)).
[159] This paragraph is based on a study of a blockchain-based data marketplace, see Charlotte Ducuing, 'D4.5 – Legal Aspect for Smart Contract Adoption' (In2Dreams 2018) Deliverable.

enforcement promises *after* the data exchange takes place (i.e. on a blockchain network). Both technologies could easily complement each other. In any case, **data sovereignty should be analysed in light of earlier scholarly discussions on blockchain-based (smart) property**.

As outline above, providing an exhaustive legal analysis of the notion of 'data sovereignty' is beyond the ambit of this section. The notion as it will/would be embedded in TRUSTS, is also not well-delineated yet. In addition, neither the specific context in which it will be used (including the platform ecosystem) nor the concrete technical tools enforcing 'terms and conditions' are yet in place. However, a few legal risks or limitations can already be anticipated.

e) Risks of misalignments between data sovereignty and applicable legal frameworks

The notion of 'sovereignty' conveys an ideal of full-fledged self-determination with respect to one's data. This, however, would not be permitted by law. Depending on the nature of data and on the context, many legal restrictions are likely to apply, as outlined in this deliverable. Such restrictions may *inter alia* stem from contract law or the regulation of unfair commercial practices. For instance, the contractual terms may be found unduly unbalanced. Technical enforcement (by means of data sovereignty as complemented, where appropriate, by smart contracts) could also qualify as a form of 'self-help', thereby partly displacing legal enforcement. Whether and to what extent this could constitute an infringement (of contract law and/or judiciary law) depends upon national law and can only be analysed *in concreto.*[160]

A very obvious limitation lies in data protection law. While data protection law does not completely prohibit the exchange of personal data, such an activity should respect data protection law principles and rights of data subjects. What seems particularly under tension with data sovereignty is the question how to comply with the principle of purpose limitation[161] and with the general principles of necessity and proportionality. The notion of data sovereignty would imply that an industrial data provider would decide to 'sell' or 'lease' his dataset (i.e. including personal data) to any third party for profit. In contrast to that, the principle of purpose limitation restricts the processing of personal data to the fulfilment of a (or several) "specified, explicit and legitimate purpose". Further processing "in a manner that is incompatible with those purposes" shall be prohibited.[162]

This limitation, found in data protection law, illustrates a more general challenge. Data sovereignty and the overall infrastructure necessary to set up data sovereignty-based data markets are based on standardisation of data exchange processes. In contrast, legal frameworks require context-specific analysis. For instance, what is the specific purpose for the processing of a given personal dataset? Does this purpose necessarily imply an exchange of such data to (a certain) third party(ies)? Such questions cannot easily be 'standardised'. While it does not necessarily imply that data sovereignty would be essentially alien to the law at large (and to the GDPR in particular), legal compliance may pose scalability issues. Fundamentally, commodifying data is at odds with the law.

[160] On this topic, see also Roberto Spigolon and others, 'The Data Transactions Model in Railways Ecosystems (In2Dreams)' (2018) 4.1 32–34.
[161] GDPR, Art. 5(1)(b).
[162] For further explanation on the notion of purpose limitation, see the deliverables in WP9 in response to the post-grant ethics requirements from the European Commission.

4.3 Towards a Data Law? Patterns for future data regulation

The regulation of data as an economic asset is very high on the political agenda, particularly at the EU level. This section will now outline possible patterns for future regulation, which will be further reflected upon in the remainder of the interdisciplinary research conducted in TRUSTS.

On the 19th February 2020, the European Commission adopted a Communication 'A European strategy for data'[163] meant to complement the White paper on AI[164] issued on the same day. The objective of the European Commission with respect to data is explicitly stated in the Data Strategy: "Citizens should be empowered to make better decisions based on insights gleaned from non-personal data. And that data should be available to all – whether public or private, big or small, start-up or giant. This will help society to get the most out of innovation and competition and ensure that everyone benefits from a digital dividend. This digital Europe should reflect the best of Europe - open, fair, diverse, democratic, and confident." In order to achieve such an objective while taking into account the problems in the digital environment, the European Commission lays down four strategic pillars. This section will outline the pillars which may turn out to have legal significance for data market ecosystems such as this of TRUSTS.

a) First pillar: *"A cross-sectoral governance framework for data access and use"*

The European Commission aims to regulate data access and use horizontally, however abstaining from "overly detailed, heavy-handed *ex ante* regulation". As for the regulatory aspects, the European Commission would rather favour an "agile approach to governance that favour experimentation (such as regulatory sandboxes), iteration and differentiation". The Data Strategy does not further substantiate what an "agile approach" would consist of, with respect to regulation. While 'agile' originally refers to a project management methodology in the software industry, it is hard to picture how such an approach would apply to the law-making.[165]

The European Commission identifies (see the Appendix to the Data Strategy) a series of "common European data spaces". Surprisingly, the term 'data space' is not defined in the Data Strategy, other than clarifying that they should be sector and domain-specific. Data space seems to refer to the sector-specific initiatives (both of legislative and non-legislative nature) that the European Commission is willing to launch with respect to data governance. This being said, they are not as 'specific' as one would expect and are likely to overlap. For instance, the 'personal data space' and the 'health data space' on the one hand, or

[163] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM(2020) 66 final, 19.2.2020.
[164] European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 19.2.2020.
[165] The willingness to adopt an "agile approach" likely detracts from the expectation of the European Commission to adapt the law-making process to the fast pace of innovation, an idea which has been developed under the discussion on the potential adoption of a "principle of innovation". On the principle of innovation, see Charlotte Ducuing, 'A legal principle of innovation? – Need for an assessment against the principle of democracy', Presentation at the ACCA Conference of Assistants, 18 September 2020, Leuven.

the 'manufacturing data space' and the 'Green Deal data space' on the other would obviously relate to the same 'domain' at some point.

As part of its horizontal strategy, the European Commission is notably willing to issue a legislative proposal "for the governance" of such data spaces, by the end of 2020, in order to support "decisions on what data can be used in which situations, facilitate cross-border data use, and prioritise interoperability requirements and standards within and across sectors, while taking into account the need for sector authorities to specific sectoral requirements". Where the European Commission intends to draw the line between horizontal and sector-specific legislation (the latter being part of another pillar) remains unclear at this stage. The term "data governance" is not defined in the data strategy but seems to encompass a broad range of topics, including standardisation and "data interoperability", where appropriate inter-sector.

With specific respect to business-to-business ('B2B') data sharing (such as in the context of the TRUSTS data market ecosystem), the European Commission "will explore the need for legislative action" concerning **usage rights for "co-generated data** (such as IoT data in industrial settings), typically laid down in private contracts". Complementarily, the European Commission could "clarify rules for the responsible use of data (such as legal liability)". Such legislative initiatives would make part of a (still hypothetical) 'Data Act' to be proposed in 2021. The willingness to regulate usage rights on (co-generated) data and the liability for data, although not much detailed in the Data Strategy, seem to detract from both the need of businesses for legal certainty in B2B data sharing and a sense of fairness (especially with respect to usage right on co-generated data) while IoT value chains are often unbalanced. In any case, both topics would undoubtedly have a huge impact on industrial data markets. This being said, 'legal liability' with respect to data is a very broad topic. Should it relate to liability for inaccurate data, it would ease data exchange. This being said, it seems very ambitious to regulate the liability for data from an horizontal (non sector-specific) perspective, while data are created and used in very different contexts.

Additionally, the European Commission will evaluate the fitness of the IPR framework to deal with data sharing. The Database Directive could be revised while the Trade Secrets Protection Directive could be subject to (soft law?) clarification. This, and especially a revision of the Database Directive, could diminish the uncertainty with respect to the various legal frameworks applicable to data exchange. It remains yet to be seen how this political objective could be balanced with the willingness to protect database creators.

b) Second pillar: "*Enablers: Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability*"

The second pillar is not of legal nature and is therefore not further discussed in this section.

c) Third pillar: "*Competences: Empowering individuals, investing in skills and in SMEs*"

The third pillar is of mixed nature, namely partly of legal nature of partly non-legal. The legal part of the pillar is not directly related to industrial data market ecosystems such as TRUSTS: the European European Commission is willing to "further support individuals" who should be further "empowered to be in control of their data through tools and means to decide at a granular level about what is done with their data" through the creation of "personal data spaces. Concretely, this could be "supported by enhancing the

portability right for individuals under Article 20 of the GDPR, *giving them more control over who can access and use machine-generated data".* Such legislative initiative could make part of the Data Act. Interestingly, the one data protection law-related aspect that the European Commission is willing to take further relates to the personal 'data sovereignty' paradigm ('taking back control') described in section 4.2.2 of this deliverable. By furthering the data portability right, the European Commission is indeed willing to turn data subjects into active entrepreneurs of 'their' own data for the data economy, rather than to limit the amount of personal data being processed.

d) Fourth pillar: "*Common European data spaces in strategic sectors and domains of public interest*"

The fourth pillar constitutes the sector-specific counterpart of the first one, deemed horizontal. With this pillar, the European Commission is willing to "promote the development" of the common European data spaces identified as domains of public interest in the Appendix to the Data Strategy. Every data space should be considered separately and may require specific rules. However, "common governance concepts and models could be replicated in the different sectors". Such sectoral initiatives will complement the horizontal legislative initiative.

Amongst the data spaces identified in the Appendix, the European Commission singles out the "Common European financial data space". As part of sector-specific initiatives, the European Commission intends to "further facilitate access to public disclosures of financial data or supervisory reporting data". Particularly, the European Commission wishes to "promot[e] the use of common pro-competitive technical standards, which seems to constitute a soft law – rather than a legally binding – initiative. The European Commission is obviously less ambitious for the financial data space than for other data spaces, such as the mobility data space for instance.

5 Law applicable to online platforms and intermediaries

The setting up of a platform for the exchange of data implies the creation of a whole ecosystem in order to enable data providers and data users to exchange data. Several models can theoretically be envisaged, depending on business and technical choices made in TRUSTS. In any case, the qualification as an online platform and/or intermediary may trigger the application of specific legislative frameworks specifically dedicated to them. They will be outlined in this section, which begins with an overview of the role of platforms and/or intermediaries in the field of data sharing. The second sub-section highlights the main provisions of the Platform to Business Regulation ('P2B Regulation'). Finally, the third sub-section explains whether and to what extent online platforms and intermediaries can be held liable for the content that their users place on their infrastructure.

In addition to legal frameworks applying *specifically* to online platforms and/or intermediaries, the activities conducted in a data market ecosystem are subject to *lex generalis* economic law, outlined in the following section.

5.1 Introduction – data sharing platform as (an) intermediary(ies)

As indicated by the European Commission,[166] data marketplace is a specific type of intermediary which may have a following functions:

a) Match-making between potential data supplier and data buyer

In that scenario, the platform matches the supply and demand between the potential suppliers and potential buyers, and facilitates data sharing between the parties. From an economic perspective, it lowers transaction costs through combining different data sources.[167] A major challenge for matching, however, is the unknown quality of traded data. Data customers need to know whether the data they are about to purchase is useful for their business before they engage in such transaction. As a side note, the concept of the so-called "information paradox" or the "disclosure paradox" has been articulated by Kenneth Arrow and may be explained as follows: "In order to complete such a transaction, the buyer of information must be able to place a value on the information and determine how much she is willing to pay. But once the seller discloses the information, the buyer is in possession of the subject of the trade and no longer has any reason to pay for it".[168]

[166] European Commission, 'Staff Working Document, Guidance on Sharing Private Sector Data in the European Data Economy Accompanying the Document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a Common European Data Space"' (n 125).
[167] Heiko Richter and Peter R Slowinski, 'The Data Sharing Economy: On the Emergence of New Intermediaries' (2019) 50 IIC - International Review of Intellectual Property and Competition Law 4.
[168] Michael J Burstein, 'Exchanging Information Without Intellectual Property' 91 Texas Law Review 56.

As a match-maker, the platform needs to get as much "information about the information" as possible beforehand.[169] This allows data customers to assess whether they would benefit from acquiring the data. Therefore, a main function of data sharing platforms is to "level out this information asymmetry without curtailing the incentives for the suppliers to share".[170]

b) The actual transfer of the data (and the agreed compensation), notably the creation of trust that the object of the negotiation will not be altered during the course of the negotiations

It is even said that "the creation and maintenance of trust is a key function of data sharing platforms".[171] Platforms may therefore perform screening of data sharing partners, supervise and protocol the individual transactions, as well as enforce usage constraints.[172]

c) A certification function that the transaction has actually happened, interesting potentially for reporting in the corporate balance sheet

Furthermore, such intermediaries can provide additional services and functionalities. This could include the provision of model contract clauses or (pseudo) anonymization services (if personal or confidential data are exchanged), data analytics etc.

d) Provider of the technical infrastructure

As such data marketplaces may be defined as an "architecture allowing programmability and reuse of content and data, typically through API, and organizing modularity between a stable core and variable components".[173]

As (an) intermediary(ies), the TRUSTS platform could be subjected to the newly adopted Platform to Business Regulation adopted at EU level in 2019.

[169] Richter and Slowinski (n 167) 13.
[170] ibid.
[171] ibid. 14.
[172] ibid.
[173] Jean-Christophe Plantin, Carl Lagoze and Paul N Edwards, 'Re-Integrating Scholarly Infrastructure: The Ambiguous Role of Data Sharing Platforms' (2018) 5 Big Data & Society 2053951718756683.

5.2 The Platform to Business Regulation ('P2B Regulation')

The Regulation on promoting fairness and transparency for business users of online intermediation services ('Platform to Business Regulation' or 'P2B Regulation') was adopted in 2019[174] with a view to restore some balance in the relationships between online platforms (or 'online intermediation services') on the one hand and other businesses on the other. The added-value of online platforms is not questioned by the EU legislator. Quite on the contrary, the recitals of the Regulation reckon the crucial role that online platforms play in the data economy and more particularly for businesses to reach out to consumers.[175] Regulation of platforms is justified by the legislator by the need to cater for increasing network effects online, which result in growing size of online platforms and increased dependence of businesses on them.[176] As a matter of fact, such imbalanced relationships (may) result in practices "which grossly deviate from good commercial conduct, or are contrary to good faith and fair dealing".[177] While consumers may benefit from consumer law harmonised at EU level, businesses find themselves exposed to the fragmented landscape of national legislations, which called for an harmonised legal protection against abuses by platforms, according to the European Commission. In this respect, the P2B Regulation is directly applicable without transposition by Member States being required. The P2B Regulation came into force the 12th July 2020.[178]

This section outlines the P2B Regulation, starting with its scope of application before turning to the substantive provisions. Finally, the procedural obligations as well as enforcement-related ones will be introduced.

5.2.1 Scope of application

a) Scope *rationae personae*

The P2B Regulation applies to "online intermediation services and online search engines provided, or offered to be provided, to business users and corporate website users, respectively, that have their place of establishment or residence in the [EU] and that, through those online intermediation service or online search engines, offer goods or services to consumers located in the [EU], irrespective of the place of establishment or residence of the providers of those services and irrespective of the law otherwise applicable".[179]

The term 'platform' is not used to refer to the addresses of the Regulation. The P2B Regulation addresses two categories of actors: (a) providers of "online intermediation services" and (b) "providers of online search engines".

[174] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186/57.
[175] P2B Regulation, Rec. 2.
[176] ibid.
[177] ibid.
[178] P2B Regulation, Art. 19.
[179] P2B Regulation, Art. 1 (2).

i. Providers of online intermediation services - Online intermediation services are defined as "services which meet all of the following requirements: (a) they constitute information society services within the meaning of [the E-Commerce Directive]; (b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers".[180] It is quite clear that Amazon as the biggest online marketplace was amongst the main regulatory targets of the EU legislator.

ii. Providers of "online search engines" - They are defined as natural or legal persons which provide or which offer to provide a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found".[181] Here again, it is clear that, with this definition, the EU legislator mainly aims to address Google.

b) Scope *rationae materiae*

The scope *rationae materiae* of the Regulation and its subsequent effect on national law remains yet unclear. The Regulation does not affect national civil law, especially contract law. It shall also be without prejudice to national rules which, in conformity with [EU] law, prohibit or sanction unilateral conduct or unfair commercial practices, *to the extent that the relevant aspects are not covered by this Regulation"* (emphasis added).[182] How and in which level of details these aspects shall be considered as "covered by this Regulation" is however not further detailed.

Two extreme interpretations could be envisaged: first, the Regulation could be deemed to cover, broadly, "rules to ensure that [businesses] are granted appropriate transparency, fairness and effective redress possibilities" as stated in Art. 1 "Subject matter and scope". Such an interpretation would be very strict on Member States since it could go as far as to ban all regulation (targeting specifically Platform-to-Businesses' relationships?), with a view to ensuring transparency, fairness and effective redress. Second and on the other side of the spectrum, one could consider that the Regulation "covers", *specifically*, the scope of every provision of the P2B Regulation, e.g. transparency obligations in the terms and conditions of online platforms (Art. 3) or even more specifically which information shall be included into such terms and conditions. Should such an interpretation prevail, Member States could easily regulate in excess of the Regulation. Between these two extreme interpretations, one could also hold that a given practice, e.g. ranking (Art. 5), would be "covered" by the Regulation. In such case, any further national regulation (B2B) unfair commercial practices governing ranking would be prohibited, although the P2B Regulation imposes only transparency obligations. The interpretation is regrettably made even more difficult by the inclusion of a *specific* provision governing the relationship between the P2B Regulation and other provisions in EU or national law with respect to 'exclusivity obligations' imposed by online platforms to businesses. While

[180] P2B Regulation, Art. 2 (2).
[181] P2B Regulation, Art. 2 (5 and 6).
[182] P2B Regulation, Art. 1 (4).

the Regulation does not go as far as to prohibit such commercial practices on behalf of online platforms, it explicitly allows EU or respectively national law to do so.[183] This would suggest that, *a contrario*, other items subject to transparency obligations in the Regulation (e.g. ranking, unilateral termination of the contract, differentiated treatment, …) would be considered as "covered". The question whether and to what extent Member States can regulate beyond this Regulation requires further analysis.

5.2.2 Substantive provisions

a) Terms and conditions and events affecting the contractual relationships[184]

The P2B Regulation mandates providers of online intermediation services (e.g. Amazon with respect to its online marketplace) to clarify a range of topics, explicitly in their terms and conditions for some or in an easily accessible location for the others:

- The suspension or termination of the contractual relationship, initiated respectively by the online platform[185] or by the business user;[186]
- Changes to the terms and conditions;[187]
- The provision of ancillary goods and services to consumers;[188]
- The possibility for the business user to access the information that he provided or generated, or the absence thereof;[189]
- The possibility for businesses to access personal data or other data that either businesses or consumers 'provide' or generate by using the online platform, or the absence thereof;[190]
- Ranking practices (further detailed in the following sub-section);
- Any differentiated treatment that providers of online intermediation services or business users that they control would give to goods or services,[191] e.g. in the case where Amazon favours its own products to the detriments of those of other businesses.[192]

[183] P2B Regulation, Art. 10 (2).
[184] The issue of transparency and particularly of the clarity of terms and conditions is discussed at lenght in the study commissioned by the European Commission: (EY) Ernst & Young, 'Study on Contractual Relationships between Online Platforms and Their Professional Users : Final Report.' (European Commission 2018) Website <http://op.europa.eu/en/publication-detail/-/publication/b3d856d9-4885-11e8-be1d-01aa75ed71a1/language-en> accessed 4 August 2020.
[185] P2B Regulation, Art. 3.
[186] P2B Regulation, Art. 8 (b).
[187] P2B Regulation, Art. 3.
[188] P2B Regulation, Art. 6.
[189] P2B Regulation, Art. 8 (c). The regulation of access to data was informed by the following study commissioned by the European Commission: Pierre Hausemer, Lison Rabuel and Hans Graux, 'Study on Data in Platform-to-Business Relations : Final Report.' (European Commission 2018) <http://op.europa.eu/en/publication-detail/-/publication/4af6cec1-48fb-11e8-be1d-01aa75ed71a1/language-en> accessed 4 August 2020.
[190] P2B Regulation, Art. 9.
[191] P2B Regulation, Art. 7.
[192] For further details on differentiated treatment, see Inge Graef, 'Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence' (2019) 38 Yearbook of European Law 448.

- Exclusivity obligations imposed by online platforms to businesses, in which case reasons should also be stated;[193]
- Identification of mediators (see sub-section below).[194]

The sanctions in case of non-compliance with the transparency obligations are unevenly governed. The Regulation specifies that clauses of the terms and conditions in violation with some of these transparency obligations, e.g. related to the suspension or termination of the contractual relationship or changes to the terms and conditions, shall be null and void,[195] or in other words would not have the legal binding value (e.g. as a contract) that online platforms would have liked to vest them with. Recital 20 specifies that such clauses shall be deemed to have never existed with effects *erga omnes* and *ex tunc*. A clause in the terms and conditions would therefore be found illegal and deprived of any legal effect not only to the benefit of the complainant but also of the other businesses. With respect to the other transparency obligations, the P2B Regulation does not harmonise sanctions. The default rule, indeed, is that Member States shall "ensure adequate and effective enforcement" and shall "lay down the rules setting out the measures applicable to infringement of [the P2B] Regulation and shall ensure that they are implemented".[196] The diversity of the sanctions has also to do with the fact that the Regulation does not clarify the legal value of the transparency measures in the first place, i.e. whether explanation provided on the ranking system or on preferential treatment would be vested with contractual legally binding value. Depending on the topics, violations with such transparency obligations could result, i.a., in the nullity of related clauses, in the illegitimacy of the said commercial practice and/or in a fine, in the obligation to compensation for subsequent loss, etc.

Beyond transparency obligations, the Regulation also regulates the process for suspension or termination of the contract with businesses, when initiated by the provider of online intermediation services. The latter shall particularly give reasons for such decision and provide the business user swith the opportunity to counter-argue, based on the "internal complaint-handling process" imposed by the Regulation (see below).[197]

b) Ranking

The P2B Regulation particularly governs the widespread practice of 'ranking'. Ranking is broadly defined as the "relative prominence given to the goods or services offered through online intermediation services, or the relevance given to search results by online search engines, as presented, organised or communicated by the providers of online intermediation services or by providers of online search engines, respectively, irrespective of the technological means used for such presentation, organisation or communication".[198] The way the goods or services are presented and offered by platforms constitutes, *per se*, a ranking practice.

[193] P2B Regulation, Art. 10.
[194] P2B Regulation, Art. 12.
[195] P2B Regulation, Art. 3 (3).
[196] P2B Regulation, Art. 15.
[197] P2B Regulation, Art. 4.
[198] P2B Regulation, Art. 2

Online platforms shall bear transparency obligations as per the parameters used to determine ranking and the reasons for the relative importance of the various parameters.[199] Any 'non organic' parameter (e.g. in case ranking can be influenced by sponsoring, or upon third party notification) shall particularly be duly described.[200] These transparency provisions do not go as far as to impose the disclosure of algorithms.[201] The European Commission is further tasked with the duty to clarify the transparency obligations pertaining to ranking, which have not been published at the time of writing.[202]

c) Prohibition of unfair commercial practices

Prohibition of unfair commercial practices are scarce as the Regulation mainly imposes transparency obligations. Yet, Art. 8 prohibits retroactive changes to terms and conditions by online platforms, save where required by law or when beneficial to businesses.[203]

The following sub-sections outline the provisions which aim to provide businesses with appropriate redress mechanisms, e.g. in case of violation of the P2B Regulation by the online platforms.

d) Codes of conduct

Finally, the P2B Regulation tasks the European Commission with the duty to encourage the drawing up and use of codes of conduct by online platforms in line with the substantial provisions of the Regulation and taking into account the specific features of the various sectors in which online platforms are active, as well as "the specific characteristics of SMEs".[204]

5.2.3 Procedural obligations and legal enforcement

The P2B Regulation is based on the observation that business users face to have their rights enforced. The Regulation foresees several options, both judiciary and extra-judiciary, in order to overcome this problem.

a) Internal complaint-handling system

Providers of online intermediation services are requested by the P2B Regulation to provide for an "internal system for handling the complaints of business users".[205] The internal complaint-handling system shall "allow business users to lodge complaints directly with the provider concerned" regarding a range of issues that affect him:

- "Alleged non-compliance by the provider with any obligations laid down in [the P2B] Regulation […];
- "Technological issues which relate directly to the provision of online intermediation services"; and

[199] P2B Regulation, Art. 5 (1) and (2) with respect to, respectively, providers of online intermediation service and providers of online search engines.
[200] P2B Regulation, Art. 5 (3) and (4).
[201] P2B Regulation, Art. 5 (6).
[202] P2B Regulation, Art. 5 (7). See the European Commission's webpage on the elaboration of the guidelines, available here: https://ec.europa.eu/digital-single-market/en/news/ranking-transparency-guidelines-framework-eu-regulation-platform-business-relations-explainer (last visited 4th August 2020).
[203] P2B Regulation, Art. 8 (a).
[204] P2B Regulation, Art. 17.
[205] P2B Regulation, Art. 11 (1).

- Measures from the provider "which relate directly to the provision of the online intermediation services".

The P2B Regulation further governs the process by which the complaints should be handled, e.g. by mandating swift processing of complaints, open communication vis-à-vis the complainant, transparency measures on the process for handling complaints, etc.[206]

The internal complaint-handling system cannot be considered as a form of "alternative dispute resolution" mechanism offered by the online platforms, since the complaints address the very online platforms, party in the dispute. Rather, the internal complaint-handling system shall be considered as an internal department in charge of pre-litigation. The mandatory establishment of such departments is not new in EU law and is particularly common in consumer law, such as for instance with passenger rights regulations of the various transport modes.[207]

The obligation to establish an internal complaint-handling system does not apply to providers of online intermediation services qualifying as "small enterprises" (within the meaning of the Annex to Recommendation 2003/361/EC),[208] which could be the case of the TRUSTS platform.

b) Mediation

The P2B Regulation aims to anticipate the case where disputes between an online platform and a business user cannot be satisfactorily solved through the internal complaint-handling system or where the business would like or feel the need to take its case to an external entity. The Regulation explicitly aims to favour out-of-court dispute resolution (such as mediation) deemed more swift than the judiciary, but does not affect the right of, respectively, online platforms and businesses to take their case to court.

Providers of online intermediation services are requested to identify two or more mediators in their terms and conditions, subject to the conditions laid down in the Regulation (i.a. in terms of independence and impartiality).[209] Recourse to mediators is voluntary, in the sense that "the parties are themselves in charge of the process and can start and terminate it at any time".[210] This being said, both parties shall engage "in good faith" throughout any mediation attempts.

The Regulation does not further clarify or regulate the outcome of the mediation. Because mediations typically result in confidential settlement between the (two) parties in question, it is unlikely that mediations would result in a change in the overall policy of online platforms, e.g. a ban on a commercial practice found illegitimate or the taking down of illegitimate clauses in the terms and conditions, which can be regretted from the perspective of the effective enforcement of the Regulation.

The obligation to identify mediators does not apply to online platforms qualifying as small enterprises.[211]

[206] P2B Regulation, Art. 11 (2) and (3).
[207] See for instance, Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations, OJ L 315/14, Art. 27.
[208] P2B Regulation, Art. 11 (5).
[209] P2B Regulation, Art. 12.
[210] P2B Regulation, Rec. 40 clarifying the expression "voluntary nature".
[211] P2B Regulation, Art. 12 (7).

c) Judicial proceedings by representatives organisations or associations and by public bodies

Finally, the Regulation aims to enlarge the scope *rationae personae* of entities, private associations or public bodies set up by Member States, who can initiate a case before national courts, so as to stop or prohibit "any non-compliance" by online platforms,[212] subject to the conditions laid down in the Regulation (e.g. to ensure that associations are not-for-profit and are not unduly influenced by competing online platforms).[213]

5.2.4 Conclusion: is the P2B Regulation based on the notion of 'economic dependence'?

A concept has gained much traction in the digital environment, as a means to regulate powerful online platforms beyond the mere application of competition law: this of economic dependency or dependence. Competition law, and particularly the regulation of unilateral conducts of undertakings (Art. 102 TFEU), requires the *objective dominant* position of a company on a given market as well as an abuse of such position to the detriment of competition. In contrast, the concept of economic dependency regards the specific relationship between two undertakings, namely a weaker party deemed, subjectively, dependent on the other one. Because markets and market power (often identified by the proxy of market shares) are not easily identifiable in the digital environment and subject to controversy, the concept of (abuse of) economic *dependence*, although as such not specific to the online environment, has gained renewed traction as a "second best" regulatory tool[214] to prevent abuses, i.a. from online platforms. In that respect, the concept of economic dependence is at the crossroads between competition law aiming at protect the functioning of competition and the regulation of unfair commercial practices aiming at protect weaker parties (consumers but also weaker businesses, as discussed in the present section).[215] As well phrased by T. Tombal, the concept of economic dependence "illustrates the core underlying tension between the parties' individual interests and the broader institutional interest in protection the competitive process" as well as it questions the purpose and boundaries of competition law.[216]

No horizontal EU-wide legal framework relies on the concept of economic dependency as such. The P2B Regulation obviously targets online platforms *because of* the "dependence" of businesses on them "particularly SMEs" and reckons the specific role of "data-driven indirect network effects" in creating and maintaining such dependence. "Given that increasing dependence, [online platforms] often have superior bargaining power, which enables them to, in effect, behave unilaterally in a way that can be unfair and that can be harmful to the legitimate interests of their businesses users and, indirectly, also of consumers

[212] P2B Regulation, Art. 14 (1).
[213] P2B Regulation, Art. 14 (3).
[214] As well illustrated by the title of Pranvera Këllezi's paper: Pranvera Këllezi, 'Abuse below the Threshold of Dominance? Market Power, Market Dominance, and Abuse of Economic Dependence' in Mark-Oliver Mackenrodt, Beatriz Conde Gallego and Stefan Enchelmaier (eds), *Abuse of Dominant Position: New Interpretation, New Enforcement Mechanisms?*, vol 5 (Springer Berlin Heidelberg 2008) <http://link.springer.com/10.1007/978-3-540-69965-1_3> accessed 5 August 2020.
[215] See for instance the case of differentiated treatment as a commercial practice in P2B relations, Graef (n 192).
[216] Thomas Tombal, 'Economic Dependence and Data Access' (2020) 51 IIC - International Review of Intellectual Property and Competition Law 70, 77–78.

in the Union. For instance, they might unilaterally impose on business users practices which grossly deviate from good commercial conduct, or are contrary to good faith and fair dealing".[217] The exemptions laid down to the benefit of online platforms qualifying as SMEs are consistent with this rationale.

However, the P2B Regulation addresses only a range of online platforms and not all companies who benefit from economic dependency situations vis-à-vis weaker business counterparts. Second, the concept of economic dependence is not fully deployed in the Regulation, in the sense that certain behaviours, deemed unfair, would be squarely prohibited when on behalf of online platforms. The Regulation mainly mandates transparency requirements, deemed to empower the weaker businesses. This may sound paradoxical. If businesses are indeed dependent on an online platform so that the latter can afford to impose unfair and unbalanced conditions, how would mere transparency requirements prevent them?

Several Member States have legislations that rely, more or less explicitly, on the concept of abuse of 'economic dependency' or on related concepts and that impose stricter behavioural duties on that basis, either generally on undertakings benefiting from economic dependency, or more specifically on online platforms. The regulation of B2B unfair commercial practices may also be based on other premises. Such legal frameworks are outlined in Section 6.

[217] P2B Regulation, Rec. 2.

5.3 Intermediary liability for data sharing platforms

A question that arises in connection to data sharing – or data exchange – platforms and intermediaries is whether and to what extent they can be held liable for the content that their users place on their infrastructure.

The Directive 2000/31/EC on Electronic Commerce ('e-Commerce Directive') is the legal framework for online services in the Internal Market. The Directive establishes harmonised rules on issues such as:

(i) transparency and information requirements for online service providers;
(ii) commercial communications;
(iii) electronic contracts and limitations of liability of intermediary service providers.

The objective of this Directive is to create a legal framework to ensure the free movement of information society services between Member States.[218] Information society services ('ISSs') are defined as services "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service".[219] Some examples of information society services include web shops, on-line information access tools and search engines.[220] What constitutes an "information society service" has been a subject of numerous cases from the CJEU, most notably in judgments concerning *Uber*,[221] *Airbnb*[222] and *Amazon*.[223] Whether or not the TRUST platform falls under this definition is subject to *in concerto* analysis.

The eCommerce Directive introduced a set of special liability rules: it provides for a "safe harbour" regime, under which certain types of ISSs providers are exempted from liability for third party content and activities (infringements on copyright, defamation, content harmful to minors, unfair commercial practices etc.) unless they are aware of the illegality and are not acting adequately to stop it. The exemptions from liability established in this Directive cover only 'technical intermediaries', i.e. when they transmit or host third party information provided by the users of the service.

There are three liability exemptions, namely:

i. "mere conduit"

Article 12 of the e-Commerce Directive provides that a mere conduit consists of the transmission in a communication network of information provided by a recipient of the service ('transmission services'); or the provision of access to a communication network ('access services').

[218] E-Commerce Directive, Rec. 8.
[219] Definition set forth in article 1(2) of Directive 98/34/EC (as amended by Directive 98/48/EC), as referred to by article 2(a) of the E-Commerce Directive.
[220] E-Commerce Directive, Rec. 18.
[221] CJEU 20 December 2017, C-434/15, ECLI:EU:C:2017:981; CJEU 10 April 2018, C-320/16 ECLI:EU:C:2018:221.
[222] CJEU 10 April 2018, C-390/18, ECLI:EU:C:2019:1112 ('Airbnb case').
[223] CJEU 2 April 2020, C-567/18, ECLI:EU:C:2020:267 ('Amazon case').

Recital 42 further stipulates that the exemptions apply only to cases "where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network (…)".[224] Therefore, the mere conduit exemption applies in the situation where the platform: (i) does not initiate the transfer of data; (ii) does not select the recipient of the data; and (iii) does not select or modify the transmitted data;

ii. "caching"

Caching is defined as "the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request".[225] Just as mere conduits, caching service providers are exempted from liability only if they are in no way involved in the data transmitted;

iii. "hosting"

Hosting consists of the storage of information provided by a recipient of the service.[226] The scope of which type of service constitutes "hosting" is subject of discussions.[227] In any case, it has a passive, technical, and automatic role in the storage of data. For hosting platforms, hosting storage is not merely incidental to the provision of the transmission or access services. A hosting service provider should not be held liable for the data stored, if: (i) it is not aware of the facts or circumstances from which the illegal information is apparent or does not have actual knowledge of the illegal information; (ii) upon obtaining such knowledge it acts to remove or disable access to the information in question.[228]

The Directive does however not clarify the details for taking down or blocking access to information.[229] Moreover, Member States are allowed to establish specific procedures governing the removal or disabling of access to information.[230]

The applicability of the exemption of liability will however depend on whether the TRUST platform fulfils the conditions in light of the functions performed. It may well fall within the "hosting" exception.

However, if it performs a more active role and thus somehow controls, selects or determines the data provided, it will most probably not benefit from the liability exemption under the e-Commerce Directive. Such analysis must however be based on the specific set-up of the TRUSTS platform and its architecture.

Richter and Slowinski argue that "in contrast to the conventional sharing economy debate, however, we do not (yet) see a discussion about the liability of data sharing platforms themselves, which might mitigate

[224] E-Commerce Directive, Rec. 42.
[225] E-Commerce Directive, Art. 13(1).
[226] E-Commerce Directive, Art. 14.
[227] Aleksandra Kuczerawy, *Intermediary Liability and Freedom of Expression in the EU: From Concepts to Safeguards* (Intersentia Ltd) 61.
[228] E-Commerce Directive, Art. 14(1)(a) and 14(1)(b).
[229] Aleksandra Kuczerawy (n 227) 63.
[230] E-Commerce Directive, Art. 14(3).

the risks of illicit data use".[231] Since the legal framework is mainly based on a contract between the sharing parties and the platform, it seems even more important to implement the actual technical measures such as certification mechanisms, security measures and blockchain technologies.[232] All that could help to strengthen trust between data sharing partners.

It shall also be noted that the European Commission is currently (re) examining the rules related to intermediaries, as part of its Digital Single Market strategy. The new EU legislation is expected in the forthcoming Digital Services Act package.[233]

[231] Richter and Slowinski (n 167) 13.
[232] ibid.
[233] See more at: https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

6 Economic law applicable to data transactions

At the EU level there is no universally accepted definition for what is called "data sharing", or "shared data". Support Centre for Data Sharing (SCDS)[234], defines "data sharing" as "the collection of practices, technologies, cultural elements and legal frameworks that are relevant to transactions in any kind of information digitally, between different kinds of organisations".

The European Commission refers to "data sharing" as "data supply and (re-)use".[235] It uses the term "data sharing" "in order to describe all possible forms and models underpinning B2B data access or transfer".[236] In this view, we will use a broad definition of data sharing, to cover all types of data flows between data providers, data consumers, and with third parties that may take place within TRUSTS.

In lack of specific EU legislation governing data sharing in B2B setting, data sharing takes place mainly on the basis of contractual terms and conditions agreed upon by the parties, for instance in a form of data sharing agreements. Data sharing agreements may not only be bilateral in nature but may also be concluded between multiple parties.

Despite the contractual freedom, the parties to a data sharing agreement ("DSA") are, however, bound to comply with two sets of obligations:

i. mandatory rules arising from the applicable national (e.g. contract and commercial) laws. Such rules may require, for instance, the data processing agreement between a data controller and a data processor to be in writing. The national legislation may also impose a specific requirements for sharing a special categories of data, such as financial data or health data;

ii. EU legislation, as transposed in national law where applicable, indirectly applicable to data sharing. EU acquis applicable to data sharing consists of general and horizontal legislation (Database Directive, Copyright DSM Directive, Trade Secrets Directive, The Software Directive, the Regulation of B2B unfair commercial practices discussed in section 6.1 and sector-specific rules (the PSI Directive, the PSD2 and the AML discussed in section 8).

This section begins with an outline of the regulation of unfair commercial practices between businesses, mainly at national level. Mostly of horizontal nature (not specific to the digital environment), such regulation may be well-suited to operationalize what it means for data transactions to be conducted in a "fair" manner between businesses. When it comes to the contractual framework for B2B data sharing,

[234] The Support Centre for Data Sharing is an initiative funded by the European Commission to further support the development of the Digital Single Market; See more at: https://eudatasharing.eu/homepage.
[235] European Commission, 'Staff Working Document, Guidance on Sharing Private Sector Data in the European Data Economy Accompanying the Document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a Common European Data Space"' SWD(2018) 125 final, 2.
[236] ibid. 5.

although without legally binding value, the EU (and especially the European Commission) has been active in issuing soft law guidance, which is outlined in the second sub-section.

6.1 Regulation of B2B unfair commercial practices in data-driven ecosystems

Contrary to the regulation of business-to-consumer relationships, and particularly of what should be considered "unfair commercial practices", EU law does not provide for horizontal regulation of business-to-business relationships. Except for *lex specialis* (such as the P2B Regulation introduced in the above section), such regulation is to found in the respective law of the Member States. This section does not aim at providing an exhaustive study on the regulation of unfair commercial practices between businesses in the law of all Member States across the EU, which lies obviously beyond the ambit of this deliverable. Rather, the purpose is to introduce general concepts that should guide the establishment and development of the TRUSTS ecosystem, based on legal traditions in the Member States. Specific attention will be paid to how the regulation of unfair commercial practices between businesses may apply in the case of data markets and data transaction ecosystems. Germany, France and Belgium are respectively discussed as illustrations.

6.1.1 Germany

The concept of economic dependence was introduced in German law (German Act against Restraints of Competition) in the 1970s to the benefit of SMEs depending on undertakings "in such a way that *sufficient and reasonable possibilities of switching* to other undertakings do not exist" (emphasis added), which amounts to a relative market power ('relative' in the sense of related to a given relationship).[237] In such case, any form of discrimination on behalf of the 'relatively dominant' undertaking shall be prohibited. Both the judiciary and the competition authority are respectively competent to enforce this provision. The notion of 'economic dependence' is broad, since it does not go as far as to impose an impossibility for SMEs to switch to another business counterpart, but only a non "sufficient and reasonable possibility".

Prohibition of some commercial practices deemed unfair is also based on the concept of economic dependence or similar notions in other Member States, such as France and, more recently, Belgium.

6.1.2 France

In France, the Code of Commerce prohibits the abusive exploitation of the condition of economic dependence in which a company finds itself vis-à-vis another company, whenever it is susceptible to affect the functioning or structure of competition ("dès lors qu'elle est susceptible d'affecter le fonctionnement ou la structure de la concurrence").[238] Although its analysis shall focus on the bilateral relationship

[237] Section 20 of the German Act against Restraints of Competition. For a commentary, see i.a. Këllezi (n 214) 63.
[238] Code of Commerce, Art. L420-2, al. 2. For a commentary, see ibid 63–65.

between the two companies, the condition that the functioning or structure of competition shall be likely to be affected brings the provision closer to competition law and makes its application less likely. In case of such economic dependence, any "abusive exploitation" of it shall be prohibited, which includes not only discriminatory practices but also the refusal of sale, tied sales (such practices being explicitly mentioned) or any other practice found abusive. The victim does not have to qualify as an SME.

While the concept of 'economic dependence' is strictly defined and of practical little use, *other provisions of the French Code of Commerce* otherwise aim to restore balance in contractual relationships between businesses. For instance and similar to consumer law, commercial law prohibits a range of contractual clauses deemed unfair between businesses in any case, e.g. contractual clauses allowing one party to benefit retroactively from discounts or to benefit automatically from the most favourable conditions granted to competing undertakings by the counterpart.[239] Of specific relevance for contracts between businesses and online platforms is also the prohibition for an undertaking to abruptly cut off an established commercial relationship.[240] Other contractual clauses and commercial practices are similarly regulated. A provision of the French Code is particularly relevant for the online business environment. The Code of Commerce deems unfair the fact for an undertaking to (a) (attempt to) obtain from the other party a benefit without consideration or manifestly disproportionate, or to (b) (attempt to) impose to the other party obligations creating a **'significant unbalance'** between the rights and obligations of the parties.[241] Unlike the concept of economic dependency, this provision does not directly regard the *economic* unbalance (and dependence), but the *legal* unbalance between the parties. Both are obviously related, since a stronger economic position allows one to impose uneven contractual clauses. Not only the victim but also the French Competition Authority, the prosecutor and the Minister for the economy can bring an action to Court. Available sanctions include compensation for loss, a fine but also ban on the unfair practice or clause and the victim can have the unfair clauses found null and void.[242]

When it comes to online platforms, Amazon was sentenced by the Commercial Court of Paris to a 4 million € fine in 2019, for having *imposed* contractual clauses (and for the way they are implemented by Amazon) to business users which create a significant unbalance between their respective rights and obligations.[243] The case was brought to Court by the Minister for the economy. In its judgement, the Court refers i.a. to the proposal for a P2B Regulation and to the data-driven indirect network effects of online platforms which contribute to increase the [economic] dependency of businesses vis-à-vis them. The Court argues that it is the situation of economic unbalance and dependency between Amazon on the one hand and the business users on the other which justifies that Amazon did indeed "impose" unfair contractual clauses on them. The Court notably found that, *inter alia,* the following contractual clauses imposed by Amazon in its terms and conditions were unfair:

[239] Code of Commerce, Art. 442-3.
[240] Code of Commerce, Art. 442-1, II.
[241] Code of Commerce, Art. L442-1,I.
[242] Code of Commerce, Art. 442-4,I.
[243] Tribunal de commerce de Paris, 1ère ch., jugement du 2 septembre 2019, M. Le Ministre de l'Economie et des Finances / Amazon.

i. The 'modification' clause, for absence of notice period and individual notification by Amazon in case of modification of the terms and conditions;

ii. The 'termination' clause, which afforded Amazon to terminate a commercial relationship for any reason, without any statement of reasons, without prior notice and without consideration for the nature of the potential breach of the business user;

iii. The regime of 'performance drivers', for lack of transparent and stable indicators, the latter being subject to the entire discretion of Amazon;

iv. An unclear clause allowing Amazon to automatically claim the best conditions afforded by a business user to any other distributor, without any specific consideration.

In 2018, the French Minister for the economy also filed a suit before the Commercial Court of Paris based on the same legal basis against Apple and Google with respect to the conditions that they impose to business users for the use of their app stores.[244] The Minister for the economy (and the public administration DGCCRF) considers that a number of their standard terms and conditions characterise a 'significant unbalance', such as the following ones: the one-sided setting of a price range between the businesses *and their own customers (consumers)*; the unilateral possibility for Apple / Google to modify or suspend the contract; the one-sided right for Google / Apple to make use of (e.g. technological) information from the businesses. The cases are still pending at the time of writing. It should be noted in this respect that, following complaints by alleged victims (Spotify and an e-book distributor) the European Commission also opened investigations into Apple's app store in June 2020, based on general competition law (Art. 102 TFEU). The European Commission will look into the terms and conditions of Apple, viewed as a "gatekeeper" when it comes to the distribution of apps and content.[245]

In addition to these *lex generalis* provisions, specific provisions have also been introduced into French law with respect to online platforms.[246] However, such provisions are mainly aimed at protecting consumers and do not apply to B2B relationships.

[244] Direction Générale de la Concurrence, de la Consommation et de la Répression des fraudes ('DCCRF'), Assignation de Google et Apple pour des pratiques commerciales abusives (press release), Paris, le 14 mars 2018 N°391. The press release is available here : https://www.economie.gouv.fr/files/files/directions_services/dgccrf/presse/communique/2018/cp-google-apple.pdf (last visited 7th August 2020).

[245] European Commission, press release, Antitrust: Commission opens investigations into Apple's App Store rules Brussels, 16 June 2020. The press release is available here: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073 (last visited 7th August 2020).

[246] See LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique. Online platforms are defined in Art. 49.

6.1.3 Belgium

Another example of a Member State regulation of unfair commercial practices between businesses, in addition to EU law-based competition law, is this of Belgium. The Belgium Code of Economic Law ('Code de Droit Economique' or 'Wetboek van Economisch Recht') was again revised in 2019 to strengthen the regulation of B2B unfair commercial practices.[247] The 2019 revision expressly introduces the concept of 'economic dependence' into Belgian law. The state of economic dependence ("sujétion") is characterised by the absence of reasonably equivalent alternative within a reasonable time limit and at a reasonable cost, vis-à-vis a company, which allows the latter to impose conditions which would not be obtained under normal market conditions.[248] The 2019 revision prohibits the abusive exploitation of such state of economic dependence, when competition is likely to be harmed. While 'abuse' is not defined, a non-exhaustive list is provided of practices that *could* constitute such an abuse: refusal to deal, direct or indirect price setting under non fair transaction conditions, production cap prejudicing consumers, uneven contractual conditions between economic partners or tying.[249] The regulation of economic dependence makes part of Belgian competition law. I.e. the Belgian Competition Authority is competent to investigate such cases, on its own initiative or following a complaint. Fines can be imposed. Just like in French law, the notion of 'economic dependence' is associated with the harm to competition, which brings this legal regime very close to 'regular' competition law. However, and again just like in French law, victims do not have to be SMEs so that the scope *rationae personae* is broader than the German regime with this respect. The new concept of economic dependence shall however not be viewed in isolation: not only does the 2019 revision create new provisions regulating B2B commercial practices; Belgium also revises its Civil Code, with new provisions resonating with the notion of economic dependence.

Subject to approval by the Parliament, a bill aiming to revise the law of obligations introduces the notion (well-known in the Belgian legal scholarship and already somehow developed by the case law) of the 'abuse of circumstances' ('abus de circonstances' or 'misbruik van omstandigheden', otherwise called 'lésion qualifiée' or 'gekwalificeerde benadeling'). The abuse of circumstances refers to a situation of manifest unbalance between the respective performances of the parties when concluding a contract, due to the abuse by one party of the weaker position of the other party. In such case, the victim can obtain adjustments to his / her obligations. The obligation may also be declared null and void by a judge (n.b. not by the Belgian Competition Authoritity).[250] The provision applies to all contractual relationships, irrespective of the nature of the parties (i.e. whether consumers or businesses, with respect to

[247] 4 AVRIL 2019. - Loi modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises.
[248] Law of 4 April 2019, Art. 2, modifying the Code of Economic Law, Art. I.6.
[249] Law of 4 April 2019, Art. 4, creating a new Art. IV.2/1. in the Code of Economic Law.
[250] Proposition de loi portant insertion du livre 5 « Les obligations » dans le nouveau Code civil, 3 Avril 2019, DOC 54 3709/001, Art. 5.41. The link between the two legal regimes is notably made by Olivier Vanden Berghe, in a blog post: Olivier Vanden Berghe, 'Relations B2B – L'abus de dépendance économique et les clauses abusives entre entreprises, nouveautés insérées dans le Code de droit économique par la loi du 21 mars 2019' (21 March 2019) <https://www.rdc-tbh.be/news/relations-b2b-labus-de-dependance-economique-et-les-clauses-abusives-entre-entreprises-nouveautes-inserees-dans-le-code-de-droit-economique-par-la-loi-du-21-mars-2019/> accessed 6 August 2020.

relationships governed by economic law). The preparatory works in Parliament clarify that the weaker position of the party can relate not only to personal characteristics (e.g. state of physical necessity) but also to the condition of economic or functional superiority of the abusing party (e.g. monopoly or power position).[251] The latter circumstance, related to the relative strength of the parties, could for instance apply to P2B contractual relationships, similar to the French legal notion of 'significant unbalance' (see above).

While the 'abuse of circumstances' relates to the major obligations of the contract or its 'raison d'être' (by its reference to the 'performance'), the 2019 revision of the Code of Economic Law also strengthens the regulation of unfair contractual clauses between businesses. In this case, the identification of the unfair nature of the clauses shall relate neither to the main subject of the contract, nor to the appropriateness between the product or services on the one hand and the remuneration on the other.[252] The legislator thereby prohibits contractual clauses between businesses which create a manifest unbalance between the rights and obligations of the parties, similar to the French legal regime of 'significant unbalance' (see above).[253] Unfair clauses are prohibited and shall be null and void.[254] Actions may be brought to Court not only by the victim but also, i.a. by the federal public administration. Inspired by consumer law, the 2019 revision includes a 'black list', namely a list of clauses which are abusive, irrespective of the context, e.g.: clauses whose purpose is to:

i. Provide for an irrevocable commitment of one party while the performance of the other party is subject to self-determined condition;

ii. Grant an undertaking the one-sided right to interpret (part of) the contract;

iii. In case of dispute, have the other party renounce any redress;

iv. Irrevocably acknowledge that the other party has read or adhered to clauses that this party has not had the occasion to take note of.[255]

The 2019 revision also includes a 'grey list', namely a list of clauses presumed to be abusive, in the absence of evidence to the contrary, e.g. clauses whose purpose is to:

i. Allow the undertaking to unilaterally modify the price, features, or contractual conditions without good reason;

ii. Extend tacitly a fixed-term contract without reasonable notice period;

iii. Shift the economic risk on a party while it should normally lie with the(an) other party;

[251] Proposition de loi portant insertion du livre 5 « Les obligations » dans le nouveau Code civil, 3 Avril 2019, DOC 54 3709/001, p. 48.
[252] Code of Economic Law, Art. VI.91/3(2).
[253] Code of Economic Law, Art. VI.91/3(1).
[254] Code of Economic Law, Art. IV.91/6.
[255] Code of Economic Law, Art. VI.91/4.

iv. Rule out or improperly limit the legal entitlements of a party in case of (whole or partial) failure to perform by the other party;

v. Waive the undertaking from liability in case of fraud, gross misconduct or, save in the event of *force majeure*, in case of non-performance of the main contractual obligations;

vi. Limit the means of evidence that the other party can use;

vii. Set disproportionate amounts of damage in case of non-performance by the other party.[256]

The 2019 revision also introduces the prohibition of unfair commercial practices between businesses, and particularly deceiving and aggressive practices. Aggressive practices are characterised by the significant alteration of freedom of choice of the contracting business, because of harassment, duress or undue influence, which lead the business to make a decision he / she would not have made otherwise. Undue influence is defined as the use of a position of power by an undertaking vis-à-vis the other so as to pressure him / her. The use of physical force is not required. Several elements shall be taken into account, *i.a.* the contractual position of an undertaking vis-à-vis the other.[257]

6.1.4 Intermediary conclusion: towards EU regulation of B2B unfair commercial practices?

This overview of national legal frameworks is far from exhaustive. However, not only does it give a taste of how B2B contractual relationships may be regulated. It also shows that *lex generalis,* namely legal frameworks applicable to *any type* of business transactions may be well-fitted to the challenged encountered in the digital environment, as illustrated by the French case law.

Although they provide interesting provisions for the regulation of unfair commercial practices, it remains to be seen whether national legal frameworks are sufficient to deal with the specific challenges encountered in data transactions. Two types of challenges are expected. First, national legislations are by nature fragmented. The willingness of the European Commission to have EU-wide data market ecosystems flourish may be confronted to this lack of harmonization. This challenge is further emphasized by the horizontal nature of most national provisions. They do indeed not tackle data or data transactions as such but, much more generally, transactions between businesses. It creates uncertainties as for how general principles do apply to concrete data-related cases. This also means that some data-specific challenges may not be tackled by the law in force. For this reason, some have suggested more targeted provisions, such as the European Law Institute (ELI) and the American Law Institute (ALI), who are elaborating "Principles for the Data Economy".[258] According to the contribution made to the public consultation of the European Commission on the Data Strategy by the rapporteur of the project - Christiane Wendehorst – and by a

[256] Code of Economic Law, Art. VI.91/5.
[257] Code of Economic Law, Art. VI.104/1(2), Art. VI.109/1, Art. VI.109/2.
[258] See the webpage of the project on ELI's website: https://www.europeanlawinstitute.eu/projects-publications/current-projects-feasibility-studies-and-other-activities/current-projects/data-economy/ (last visited 26th October 2020).

working member – John Thomas - (with the help of Sebastian Schwamberger),[259] the challenges related to the absence of clear rights on data and to the unbalance of power in data transactions could be best solved by data-specific regulation of B2B unfair commercial practices, possibly at EU level. They propose in particular the creation of 'data rights in co-generated data', that 'co-generators of data' could enforced against the 'data controller' (this figure being inspired by personal data protection law).

[259] The contributions to the public consultation are publicly available, see https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-european-strategy-data (last visited 26th October 2020).

6.2 B2B data sharing principles and contractual terms

For absence of a horizontal legal framework regulating B2B transactions, the EU has been active in elaborating soft law guidelines for businesses.

In the Commission Communication "Towards a common European data space", the stakeholder dialogue and replies to the online survey showed that stakeholders take the view that, at this stage of the development of the data economy, the existing regulatory framework is fit for purpose and that it is too early for horizontal legislation on data sharing in business-to-business relations".[260] The prevailing view is that the freedom of contract should be a cornerstone for data sharing and that "in general, businesses should be free to decide to whom and under what conditions access can be granted to their non-personal data".[261] Moreover, the stakeholders supported "non-regulatory measures, such as (i) fostering the use of APIs for simpler and more automated access to and use of datasets; (ii) developing recommended standard contract terms; and (iii) the provision of EU level guidance".[262] That approach has been to a large extent followed by the EU legislator, by encouraging the development of codes of conduct (see Section X 4.1.2 above) and non-binding guidance issued by the European Commission. Although without legal value, they can provide practical guidance.

This section begins with general guiding principles for B2B data sharing provided in the "Guidance on sharing private sector data in the European data economy" (European Commission Staff Working Document) of 2018. The second subsection offers an overview of considerations which may be included in data sharing agreements.

6.2.1 B2B data sharing principles

On 25 April 2018, the European Commission published a series of communications related to data and artificial intelligence. One of them called "Towards a Common European Data Space", came with a non-binding European Commission Staff Working Document "Guidance on sharing private sector data in the European data economy". In the Document, the Commission defines a series of key principles for data transactions in business-to-business (B2B) and business-to-government (B2G) relations. The B2G situations will not be analysed in this report.

In what follows we elaborate upon these general guiding principles to be considered by B2B data sharing, namely:

i. **Transparency**: The relevant contractual arrangements (including data usage agreements) should *"identify in a transparent and understandable manner (i) the persons or entities that will have*

[260] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Towards a Common European Data Space"' COM/2018/232 final/2, 9.
[261] ibid.
[262] ibid.

access to the data that the product or service generates, the type of such data, and at which level of detail; and (ii) the purposes for using such data".[263]

The requirement to identify who is given access to the data is essential to determine liability for accuracy of data and to ensure clear responsibility for each shared dataset and possible damages arising from (mis)use of the dataset. It also enables the identification of potential risks of data sharing. Determining the purpose of using data also helps to determine liability in case of unlawful disclosure of trade secrets.[264]

ii. **Shared value creation**: *"The relevant contractual agreements should recognise that, where data is generated as a by-product of using a product or service, several parties have contributed to creating the data".*[265]

iii. **Respect for each other's commercial interests**: *"The relevant contractual agreements should address the need to protect both the commercial interests and secrets of data holders and data users".*[266]

It is essential to contractually recognize the co-creation of data. Data providers and data customers should carefully assess the datasets and their "ownership" before sharing the data. Similar reasons fall under the respect for each other's interest's principle.

iv. **Ensure undistorted competition**: *"The relevant contractual agreements should address the need to ensure undistorted competition when exchanging commercially sensitive data".*[267]

The contractual arrangements should not distort competition and be in line with Art. 101 and 102 TFEU, in particular when exchanging sensitive and/or strategic data. For competition law concerns of data sharing we refer to Section 5.1.3 of this document.

v. **Minimized data lock-in:** *"Companies offering a product or service that generates data as a by-product should allow and enable data portability as much as possible*[268]*. They should also consider, where possible and in line with the characteristics of the market they operate on, offering the same product or service without or with only limited data transfers alongside products or services that include such data transfers".*[269]

[263] European Commission (n 2) 3.
[264] Begoña Gonzalez Otero, 'Evaluating the EC Private Data Sharing Principles' [2019] 10 (2019) JIPITEC 66 para 1 19, 77.
[265] European Commission (n 2) 3.
[266] ibid.
[267] ibid.
[268] E.g. data produced by robots in the context of industrial processes, relevant for provision of after-sales services (e.g. repair and maintenance), or data on the rating of services providers.
[269] European Commission (n 2) 3.

> This mirrors Article 6 of the Free Flow of Non-Personal Data Regulation discussed in Section 4.1.2. In certain cases, the porting of non-personal data would be covered by both the Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation.

The Commission Staff Working Document then provides a "How to" guide on “legal, business and technical aspects of data sharing”. First, it elaborates on three main models of B2B data sharing, namely (1) an Open Data approach; (2) Data monetization on a data marketplace; and (3) Data exchange in a closed platform. Variations and combinations of these models are possible and need to be adapted to each concrete business need.

When it comes to the data monetization on a data marketplace, the Document specifies that “this mechanism appears suitable when either (1) there are limited risks of illicit use of the data in question, (2) the data supplier has grounds to trusts the (re-)user, or (3) the data supplier has technical mechanisms to prevent or identify illicit use. Model contract terms can lower the costs of drawing up data usage agreements”.[270]

Second, the Staff Working Document explains the legal aspects of data sharing. Third, it provides guidance on the technical aspects of data sharing which fall outside the scope of this analysis.

6.2.2 Terms of data sharing agreements

At the EU level, there is yet no comprehensive EU law or guidance on the drafting of contractual agreements for data sharing. However, “model contract terms for different types of data sharing agreements and for some sectors or types of data sharing are already being developed”.[271] The Staff Working Document does not however specify what specific measures are being developed. One may assume that the EU Code of conduct on agricultural data sharing by contractual agreement[272] or the documents of the Support Centre for data sharing may be considered as such. The aim of this Support Centre is to provide practical advice, best practices, and methodologies for both data sharing and data analytics. In view that “there is no single “right” way for sharing data”[273], in the Report on collected model contract terms of 26 July 2019, the Support Centre for Data Sharing provides a range of model contracts, which can be used as templates by relevant stakeholders to license data.[274] The document identifies existing licences and analyses their characteristics, such as: (i) provisions relating to the content or nature of the data; (ii) commercial / business related provisions; (iii) provisions relating to control, “ownership” and usage rights; (iv) general legal provisions; (v) provisions related to the service providing the data. The

[270] ibid. 5.
[271] ibid. 6.
[272] EU Code of conduct on agricultural data sharing by contractual agreement. The code is available at: https://copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf (last visited 6 October 2020).
[273] Support Centre for Data Sharing website, https://eudatasharing.eu/homepage.
[274] Support Centre for Data Sharing, B.1 – Report on collected model contract terms Support Centre for data sharing. The report is available at: https://eudatasharing.eu/sites/default/files/2019-10/EN_Report%20on%20Model%20Contract%20Terms.pdf (last visited 5 October 2020).

document suggests that this "can be considered as a soft and non-regulatory form of intervention, which comprises elements of best practice identification and dissemination, but also of pragmatic support".[275] It can therefore be used as a reference point to develop a tailor-made data sharing and/or data licensing agreement for TRUSTS partners.

The European Commission Staff Working Document provides a set of non-binding considerations which may help companies in the preparation and/or negotiation of data usage agreements. Taking the Commission Staff Working Document as a starting point, the data usage agreement may include the following aspects (not exhaustive):

a) Data specification and quality

Companies are advised to describe the data they share as concretely and precisely as possible. A data asset may include a single data sets, a combination of individual or multiple datasets and elements of several datasets, data items databases, unstructured data quantities etc.

There is no strict legal definition of what "data" is. In practice, it proves extremely difficult to clearly define the concept. Nevertheless, it has to be contractually clarified whether the data transaction is:

i. a data asset purchase (one-off release of data or granted for an agreed period);
ii. a data stream (access to data source);
iii. a data as a service (alternative cloud computing service model where data are made available to users as a service through network).[276]

As for the TRUSTS platform, the requirements of data sharing agreement are, in principle, the same as for the bilateral data sharing agreements between data providers and data customers. However, depending on the specificities of the TRUSTS platform acting as (an) intermediary(ies), the service component may have to be considered.

It should also be clarified whether the data will be updated and how often. Importantly, the character of the data can change with time: the nature of data is sometimes uncertain at the moment of the trade, for example it may not always be clear whether some data are really anonymous. A party processing anonymous data could *ex post* obtain information which allows to identify the individual, making anonymous data personal data.[277] Proper anonymisation of data requires that the data no longer identifies or enables identification of the data subject "either by the controller or by another person to identify the natural person directly or indirectly".[278] The question raises what if party B processing anonymous data re-identifies data subject based on wrongly "anonymised" data provided by party A. Art. 79 GDPR provides

[275] ibid.
[276] The roll-out of the EC data strategy will set up the foundation for enabling modern data management and the provisioning of services, including Data as a Service (DaaS), through the data platform. The European Commission Cloud Strategy is available at: https://ec.europa.eu/info/sites/info/files/ec_cloud_strategy.pdf (last visited 11 October 2020).
[277] Václav Janeček and Gianclaudio Malgieri, 'Commerce in Data and the Dynamically Limited Alienability Rule' (2020) 21(5) German Law Journal 924-943 20, 5.
[278] GDPR, Rec. 26.

data subjects a right to an effective judicial remedy against a controller or processor. It does not, however protects against third parties unlawfully exploiting data. There seems to be a gap for in the liability[279] for unlawful processing of data "re-identified" after failed anonymisation. For more on privacy-preserving technique, see Section 3.4 of this document.

Shared data should be of good quality, i.e. accurate, reliable, up-to-date and ideally it should not have incomplete, duplicated or unstructured data. It is also advised to set up a mechanism for reporting error in the data. The source/origin of data and how it was collected/constructed should be specified (such as personal data collected directly from the data subject with his or her consent).

b) Data access

Contract should define in a transparent, clear and understandable way who has a right to access, right to (re-)use, and right to distribute data and under which conditions. Sub-licensing should also be considered; it may either be expressly excluded, or the conditions under which it is allowed should be clearly stipulated.

c) Data usage

The parties gaining access to data should be as open and clear as possible about how the data will be used, including by other parties downstream. This includes considering whether and to what extent use of the data is allowed (including additions, modifications, updates, deletion of data, combinations with other data assets, etc.). Contracts should also specify the exact usage that can be made of data, including applications developed on the basis of the data assets or intellectual property rights on derivatives of the data. This includes the authorization for commercial or exclusively non-commercial purposes.

In the context of TRUSTS, a data provider can also have an interest in allowing only uses for research purposes. These are considered non-commercial if they do not pursue a profit-making aim.

The non-disclosure and confidentiality rules regarding downstream parties should also be defined.

d) Technical measures for data access and sharing

The technical and security aspects for the data access and/or exchange, such as frequency of data access and maximum loads, IT security requirements, service levels for support should also be included.

e) Security measures

Contractual parties should ensure that the shared data is protected from any foreseen and unforeseen circumstances, including theft, misuse, technical problem and human error. Failure to provide the necessary level of security measures may lead to liability concerns.

f) Liability

[279] As regards criminal and penal sanctions for wrongful re-identification of "anonymized" data see: Phillips Mark, Dove Edward S., Knopper Bartha M., 'Criminal Prohibition of Wrongful Re-identification: Legal Solution or Minefield for Big Data?' (2017) 14 Journal of Bioethical Inquiry 527.

Rules on liability provisions for supply of erroneous data, disruptions in the data transmission, low quality interpretative work, if shared with datasets, or for destruction/loss or alteration of data (if it is unlawful or accidental) should be covered.

It is also important to consider the contractual liability rules as regards different actors of the data value chain, including end-users. "Liability" may be defined as the responsibility of one party for harm or damage caused to another party, which may be a cause for compensation, financially or otherwise, by the former to the latter.[280]

The general principle is that the parties to data sharing agreement may freely agree on liability limitations or exclusions, except, however mandatory national provisions on liability. In certain cases, clauses agreed in the B2B context may be declared invalid in case the limitation of liability clauses will be considered contrary to national law. That, however, is subject to country to country analysis.

g) Parties' rights

Others' rights on the data should be respected. That includes in particular intellectual and industrial property rights. Contracts should also ensure the protection of trade secrets, sensitive commercial information, licenses, patents, intellectual property rights. Rights of both parties to perform audits on the respect of the mutual obligations should be defined.

h) Renumeration and terms of service

Parties should also agree on whether the data is shared in return for remuneration, and, if so, on payment modalities. The open data approach is followed e.g. when the data supplier has a strong interest in the data re-use. The Commission provides as an example providers of services that would like to make use of an ecosystem of third party application developers in order to reach the final customers.[281] They should determine the due date (e.g. upon conclusion of the contract or only after acceptance by the data customer). In practice, the value of data and the appropriate price to be paid for access proves difficult to assess.

i) Duration and termination of a contract

Parties should agree on the intended duration of the contract, conditions and circumstances to terminate the contract, and on the notice period.

j) Dispute resolution

[280] European Commission, 'Commission Staff Working Document Liability for Emerging Digital Technologies Accompanying the Document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe' SWD/2018/137 final, 2 footnote 1.

[281] European Commission, 'Staff Working Document, Guidance on Sharing Private Sector Data in the European Data Economy Accompanying the Document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a Common European Data Space"' (n 2) 5.

It is important to specify the law applicable to the contract. Moreover, the parties should specify which dispute resolution mechanism is selected in case a conflict arises. It may take the form of a litigation or of an alternative dispute resolution mechanisms, e.g. mediation and/or arbitration.

While describing the economic aspect of data transaction, one cannot forget about the competition law aspect of data sharing agreements. This will be discussed in the next Section.

7 Competition law and access to data

As discussed above, contractual framework remains the main legal regime governing data sharing. However, one of the guiding principles for data sharing is to ensure undistorted competition. As put in the "Competition policy for digital era" report, "while laws and institutions may emerge under data protection, national (or possibly EU) contract law or in other policy fields that may help to promote efficient data access in many contexts, competition law remains an important background regime".[282] At EU level, competition law is principally regulated by the Article 101 and 102 of the Treaty on the Functioning of the European Union ('TFEU'). In case of established infringements of Article 101 or 102, the European Commission may impose fines based on the gravity and the duration of the infringement, at a maximum of 10% of an infringing company's turnover, as well as structural and behavioral remedies. In some merger cases, the European Commission ordered the merged entities to limit data sharing or keep their datasets separate.[283] Mandatory data sharing as a remedy to restore competition in the affected market is also been subject of academic debate.[284]

First, the role of data for competition law analysis needs to be underlined (first sub-section). The two following sub-sections overview the two main legal frameworks in EU competition law, namely Article 101 and article 102 TFEU, with a focus on specific applications closely connected to data market ecosystems such as this of TRUSTS. Finally, the third and last sub-section outlines the increasing connection between competition law and data protection law.

7.1 Introduction - the role of data for competition law analysis

Data is a core input factor many business, products, applications and services, as well as Artificial Intelligence ('AI'). As the European Commission puts it in its "European Data Strategy", "over the last few years, digital technologies have transformed the economy and society, affecting all sectors of activity and the daily lives of all Europeans. Data is at the centre of this transformation and more is to come".[285] The competitiveness and efficiency of businesses increasingly depends on access to relevant data and the ability to use and apply it. Thus, the competitive relevance of data is constantly growing and data has in recent years become the relevant factor in competition law analysis.

[282] Jacques Crémer and others, *Competition Policy for the Digital Era.* (2019) <http://publications.europa.eu/publication/manifestation_identifier/PUB_KD0419345ENN> accessed 17 July 2020 96.
[283] *Thomson Corporation/Reuters Group* (Case M.4726) Commission Decision C (2008) 654 final [2008].
[284] See: Vikas Kathuria and Jure Globocnik, 'Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy' Journal of Antitrust Enforcement, 2020, 0, 1–24 <https://academic.oup.com/antitrust/advance-article/doi/10.1093/jaenfo/jnz036/5699250> accessed 14 October 2020.
[285] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM(2020) 66 final.

On the one hand, data sharing provides many opportunities for pro-competitive exchange of data. Access to pooled data may also allow firms to offer better products and services to customers than they could have based on their "own" data alone. The "Competition policy for the digital era" report concludes that "to the extent that data is the "raw material" for quality competition and innovation, enhancing data access will frequently promote, rather than impede competition".[286]

On the other hand, there are the possible anti-competitive aspects of data sharing, e.g.:

i. the data sharing arrangements may amount to an exclusionary practice such as denying or granting less favourable terms to competitors;

ii. the data sharing arrangements may amount to exploitative practices such as imposing an excessive or unfair purchase or selling prices or other unfair trading conditions;

iii. the data sharing arrangements may amount to an anti-competitive information exchange where it includes sensitive information;

iv. concentration of data may raise barriers to entry and be a source of market power.

As discussed below, the refusal of the dominant undertaking to grant other firms access to data may lead to anticompetitive foreclosure.

Importantly, not only restrictions on data access per se, but also restrictions on data use can have anti-competitive consequences.[287]

The heterogeneity of data, the diversity of the concept of data and of possible data access scenarios, make it difficult to apply "one fits all" solution. According to the "Competition policy for digital era" report data can be categorised as volunteered, observed, and inferred data. The type of data has implications on the capacity of competitors to gather or obtain the same information independently. It can be collected and used in different forms: individual-level data, anonymized data, aggregated-level data, historical or real-time data. Finally, data can be personal or non-personal. "The significance of data and data access for competition will thus always depend on an analysis of the specificities of a given market, the type of data, and data usage in a given case".[288]

[286] Crémer and others (n 27) 94.
[287] ibid. 93.
[288] ibid. 8.

7.2 Article 101 TFEU

7.2.1 General outline of Article 101 TFEU

Article 101 of the TFEU contains a general prohibition against agreements between undertakings which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which:

i. "directly or indirectly fix purchase or selling prices or any other trading conditions;

ii. limit or control production, markets, technical development, or investment;

iii. share markets or sources of supply;

iv. apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

v. make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts".[289]

Such agreements are automatically void according to Art. 101(2) of the TFEU.

Article 101 TFEU is relevant to any party (data provider, data consumer or data sharing platform itself), to the agreement, decisions or concerted practices in relation to data sharing. Data sharing agreements may be found anti-competitive, and therefore contrary to Article 101 "where companies in the data economy share data on terms that exclude fair competition, are discriminatory, or make market entry for third parties prohibitively impractical"[290], as long as they affect the trade between Member States. As a consequence, when defining terms under which data is shared, a party to the agreement must assess whether it does not infringe Article 101.

Moreover, in the Notice on agreements of minor importance which do not appreciably restrict competition under Article 101(1) of the Treaty on the Functioning of the European Union (De Minimis Notice), certain agreements between parties with low "aggregated market share" fall outside Article 101(1) of the

[289] TFEU, Article 101(1).

[290] Support Centre for data sharing, B2 – Analytical report on EU law applicable to sharing of non-personal data , 24 January 2020, available at: https://eudatasharing.eu/sites/default/files/2020-02/EN_AR%20on%20EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf (last visited 11 October 2020) 17.

Treaty.[291] The threshold depends on whether or not parties to the agreement are (potential) competitors or not.[292]

Article 101(3) TFEU exempts some agreements from this general prohibition when the following cumulative conditions are met:

i. the agreement contributes to improving the production or distribution of goods or contributes to promoting technical or economic progress, that is to say, lead to efficiency gains;

ii. consumers receive a fair share of the resulting benefits; and;

iii. the restrictions are indispensable to the attainment of those objectives;

iv. the agreement does not afford the parties the possibility of eliminating competition in respect of a substantial part of the products in question.[293]The assessment whether data sharing agreements are potentially anticompetitive is, however, always required. Possible efficiency gains within the meaning of Article 101(3) need to be analysed on a case-by-case basis.

There are two main types of cooperation agreements: (i) agreements that are entered into between companies at a different level of the production or distribution chain (vertical agreements), and (ii) agreements between actual or potential competitors (horizontal agreements).

The European Commission Regulation (EU) No 330/2010 ('the VBER')[294] exempts vertical agreements that meet certain conditions from the prohibition in Article 101(1) TFEU. Together with the VBER, the Commission also adopted the Guidelines on Vertical Restraints.[295] Direct information exchange between competitors is not, however, covered by the VBER.[296]

[291] Communication from the Commission — Notice on agreements of minor importance which do not appreciably restrict competition under Article 101(1) of the Treaty on the Functioning of the European Union (De Minimis Notice), OJ C 291, 30.8.2014, p. 1–4.

[292] The Commission holds the view that agreements between undertakings which may affect trade between Member States and which may have as their effect the prevention, restriction or distortion of competition within the internal market, do not appreciably restrict competition within the meaning of Article 101(1) of the Treaty:

(a) if the aggregate market share held by the parties to the agreement does not exceed 10 % on any of the relevant markets affected by the agreement, where the agreement is made between undertakings which are actual or potential competitors on any of those markets (agreements between competitors); or

(b) if the market share held by each of the parties to the agreement does not exceed 15 % on any of the relevant markets affected by the agreement, where the agreement is made between undertakings which are not actual or potential competitors on any of those markets (agreements between non-competitors).

[293] TFEU, Article 101(3).

[294] Commission Regulation (EU) No 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices, OJ L 102, 23.4.2010, p. 1–7.

[295] Guidelines on Vertical Restraints, OJ C 130, 19.5.2010, p. 1–46.

[296] The VBER, Article 2(4).

The European Commission Regulation (EU) No 1217/2010 ('R&D BER')[297] and No 1218/2010 ('Specialisation BER')[298], together referred to as the 'Horizontal block exemption regulations' (or 'HBERs'), exempt from the prohibition contained in Article 101(1) of the Treaty certain horizontal R&D and specialisation agreements. Moreover, the European Commission Guidelines on horizontal cooperation agreements provide binding guidance on the Commission for the interpretation of the HBERs.[299]

7.2.2 Information exchange

One of the examples of the data sharing agreement may give rise to restrictive effects, is the exchange of information, and in particular sensitive information. Information exchange can take various forms and can be shared either directly between competitors or indirectly through a common agency (e.g. platform).[300]

The European Commission Horizontal Guidelines find that information exchange is a common feature of many competitive markets and may generate various types of efficiency gains.[301] Sharing information may solve problems of information asymmetries and make markets more efficient. Companies may also improve their internal efficiency through benchmarking against each other's best practices. As a result, information exchanges may directly benefit consumers by reducing their search costs and improving choice.[302]

Some exchanges of commercially sensitive information may however constitute restrictions of competition under Article 101(1). It is a case for example in situations when information exchange enables undertakings to be aware of market strategies of their competitors. Communication of information on companies' individualised data regarding future prices or quantities is particularly likely to lead to a collusive outcome.

Asnef-Equifax case[303] concerned an agreement between competing financial institutions to create a register to share consumer solvency and credit data to evaluate credit risks. The CJEU held that the information sharing arrangement must not reveal the market position or commercial strategy of competitors. As a result, individual credit (pricing) decisions should not be shared, whilst information regarding, e.g., income and credit history may very well be shared. Moreover, such the register should be accessible on equal, non-discriminatory terms to all companies active in the relevant market.[304]

[297] Commission Regulation (EU) No 1217/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of research and development agreements, OJ L 335, 18.12.2010, p. 36–42.
[298] Commission Regulation (EU) No 1218/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of specialisation agreements, OJ L 335, 18.12.2010, p. 43–47.
[299] Communication from the Commission — Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, OJ C 11, 14.1.2011, p. 1–72.
[300] ibid., para 55.
[301] ibid., para 57.
[302] ibid.
[303] CJEU 23 November 2006, C-238/05, ECLI:EU:C:2006:734 ('Asnef-Equifax case').
[304] ibid., paras 58-60.

The likely effects of an information exchange on competition must be analysed on a case-by-case basis as the results of the assessment of various factors. The (anti) competitive outcome of information exchange depends on the characteristics of the market (such as concentration, transparency, complexity, stability) and which type of data is exchanged between competitors. The exchange of strategic data (e.g. individualized data, younger data) is much more likely to be anti-competitive under Art. 101 TFEU than the exchange of other type of data. In particular exchanges of genuinely aggregated data, where the recognition of individualised company level information is sufficiently difficult, are much less likely to lead to restrictive effects on competition than exchanges of company level data. Similarly, the exchange of historic data is unlikely to lead to a collusive outcome.[305] What constitutes ”historic” data depends on the data's nature, aggregation, frequency of the exchange, and the characteristics of the relevant market. Some counter factors to the risks of anti-competitive agreements are therefore to ensure that data is limited in scope or aggregated and anonymised.[306] Additionally, protocol and data interoperability are another mitigating components to take into consideration when sharing data.

Finally, the online platform operator which facilitates interactions between undertakings using their platform may act “as a hub coordinating the horizontal anticompetitive practice” and “could also be held responsible for the conduct as a facilitator”.[307] Both the decision practice by the European Commission and the CJEU case law established the liability of third-party service providers as cartel facilitators. Most notably, in the *AC Treuhand* case[308], the CJEU held that the company violated EU cartel rules by directly helping to facilitate anti-competitive exchange of commercially sensitive information, including data on customers, production and sales. The CJEU found that “AC-Treuhand played an essential and similar role in both the infringements at issue by organising a number of meetings which it attended and in which it actively participated, collecting and supplying to the producers of heat stabilisers data on sales on the relevant markets, offering to act as a moderator in the event of tensions between those producers and encouraging the latter to find compromises, for which it received remuneration”.[309] According to the judgement, facilitators can be sanctioned for horizontal coordination even if they do not operate on the affected market.[310]

Whether the TRUSTS platform could face liability for the infringement of Article 101 TFEU requires detailed *in concerto* analysis and will very much depend on the platform’s architecture.

[305] ibid, para 89.
[306] Crémer and others (n 27) 96.
[307] OECD, Hub-and-spoke arrangements – Note by the European Union, DAF/COMP/WD(2019)89, 4.12.2019, available at: https://one.oecd.org/document/DAF/COMP/WD(2019)89/en/pdf (last visited 11 October 2020), 7.; See also: Hartnett Brian N., Sparks Will, ‘The service provider as carter facilitator: assessing ‘third party’ liability under Article 101 TFEU’, CLPD Issue 1, Volume 2 - 2.
[308] CJEU 22 October 2015, C-194/14 P, ECLI:EU:C:2015:717 (‘AC-Treuhand case’).
[309] ibid. para 37.
[310] ibid. para 36.

7.3 Article 102 TFEU

7.3.1 Article 102 TFEU – general outline

Article 102 prohibits firms that hold a dominant position on a given market to abuse that position,

specifically, by:

i. "directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;

ii. limiting production, markets or technical development to the prejudice of consumers;

iii. applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

iv. making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts".[311]

The essential questions under Article 102 TFEU to determine abuse of a dominant position, are:

i. what is a relevant market;

To determine whether a company is dominant, one must first define the relevant product market and the relevant geographic market in which the company is active.[312]

According to Bruc, if data is directly sold to customers, this service could constitute a relevant market.[313] In some merger decisions, the European Commission has distinguished a market for marketing data services, further segmented into marketing information services, market research services and media measurement services.[314]

ii. whether an undertaking is in a position of dominance on that market;

Traditionally, dominance is not likely if the undertaking's market share is below 40 % in the relevant market.[315] However, market shares cannot always be the main indicator to measure market power. Market shares provide a useful, but not an exclusive, indication for the Commission whether an undertaking has a dominant position on the market. In Microsoft/Skype merger decision, the Commission indicated that

[311] TFEU, Art. 102(2).
[312] See the European Commission Notice on the definition of relevant market for the purposes of Community competition law, OJ C 372, 9.12.1997, 5–13.
[313] Édouard Bruc, 'Data as an Essential Facility in European Law: How to Define the "Target" Market and Divert the Data Pipeline?' (2019) 15 European Competition Journal 177, 187.
[314] *Publicis / Omnicom* (Case M.7023) Commission Decision C(2014) 89 final [2014] para 618; *Telefónica UK/ Vodafone UK/ Everything Everywhere/ JV* (Case M.6314) Commission Decision [2012] paras 197–98.
[315] See Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, OJ C 45, 24.2.2009, 7–20.

"market shares only provide a limited evidence of competitive strength.[316] In the context of a data marketplace, the simple fact that a platform has access to large amount of data does not automatically provide it with a dominant market position.

Graef provides the following non-exhaustive conditions which may point towards a potential market power in a data-related market: "(1) data is a significant input into the end products or services delivered on online platforms; (2) the incumbent relies on contracts or on intellectual property and trade secret law to protect its dataset as a result of which competitors cannot freely access the necessary data; (3) there are few or no actual substitutes readily available on the market for the specific information needed to compete on equal footing with an incumbent; (4) it is not viable for a potential competitor to collect data itself in order to develop a new dataset with a comparable scope to that of the incumbent (for example due to network effects or economies of scale and scope)".[317]

At this stage, it is beyond our competences to assess whether the TRUSTS platform is a dominant player in the (data) market. One cannot yet speculate on the potential abuse of dominant position.

iii. whether this position is abused;

To be dominant is not illegal per se. However, according to the CJEU case-law[318], holding a dominant position confers a special responsibility on that undertaking not to act in a manner that could abuse the dominant and distort competition.

There are various forms of abuse that can take place under Article 102 TFEU.[319] Specifically, with regards to data sharing, the potential infringements of Article 102 may take the form of a refusal to share, abusive discrimination and exploitation by unlawful processing or unfair term. One could consider the situation where a company A would like to access and use particular data held company B. However, the company B holding the commercially important information may be a direct competitor of company A, and therefore not interested in granting the other company access to the information. This becomes problematic if the company holding the information enjoys dominant position under Article 102, and abuses its position to refuse the other company access to data and the market by allowing data sharing only under unequal or discriminatory terms.

7.3.2 Article 102 TFEU – the refusal to give access to data

One particular issue that is being discussed when it comes to data sharing is the refusal to give access to data which may constitute an abuse of dominant position under Article 102 TFEU. In certain circumstances

[316] *Microsoft / Skype* (Case M.6281) Commission Decision C(2011)7279 [2011] para 78.
[317] Inge Graef, 'Data as Essential Facility. Competition and Innovation on Online Platforms', 261.
[318] See: CJEU 9 November 1983, C-322/81, ECLI :EU:C:1983:313 ('Michelin case') para 57; CJEU 6 October 1994, T-83/91, ECLI:EU:T:1994:246 ('Tetra Pak case') para 114; CJEU 7 October 1999, T-228/97, ECLI:EU:T:1999:246 ('Irish Sugar case') para 112.
[319] For more detailed information Section IV of the Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings OJ C 45, 24.2.2009.

national competition authorities may impose on a dominant undertaking an obligation to provide access to its data under the so-called essential facilities doctrine.

In a number of cases,[320] the CJEU has established the following requirements for the 'essential facility' doctrine:

i. the facility is indispensable in that no real or potential alternatives exist;

As has been said above, the first requirement to apply the essential facility doctrine under Article 102 TFEU is for an undertaking to be found "dominant". In the context of data-(with)holding undertakings, "dominance can be created through a database in exceptional circumstances: if the data is very unique in terms of quantity and quality and is used quasi-exclusively for captive purposes in the relevant market".[321]

The owner of a facility has a duty to deal when its facility is 'indispensable' for competition. The requirement of indispensability consists of two different elements: (1) the objective necessity of the input for being able to compete on the downstream market and (2) the absence of economically viable substitutes for the input.[322] A facility is deemed indispensable when no alternative exists and there are no technical, legal, or economic obstacles that make it impossible or unreasonably difficult to create an alternative facility.[323]

To meet these conditions, database must be indispensable in the sense that it must be necessary to carry the business at stake, it must be at the core of the business structure and a requirement in order to compete effectively on the market.[324] Whether or not that is the case, is subject to case-by-case analysis. In many European Commission's decisions it has been said that the non-rivalry and wide availability of data will often render a dataset non-indispensable.[325]

ii. the refusal of access to a facility must be liable or likely to eliminate all effective competition on the downstream market;

As Graef puts it "the requirement of exclusion of effective competition aims to target the situation in which an essential facility holder is already active on the downstream market and tries to reserve that market to itself by refusing to deal".[326]

This presupposes that the dominant undertaking is also active as a competitor in the secondary market. This, however, will frequently not be the case when firms refuse access to data as the platform which

[320] See: CJEU 6 March 1974, joined cases 6 and 7-73, ECLI:EU:C:1974:18 ('Commercial Solvents case'); CJEU 6 April 1995, joined cases C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98 ('Magill case'); CJEU 29 April 2004, C-418/01, ECLI:EU:C:2004:257 ('IMS Health case'); CJEU 26 November 1998, C-7/97, ECLI:EU:C:1998:569 ('Bronner case').
[321] Édouard Bruc, 'Data as an Essential Facility in European Law: How to Define the "Target" Market and Divert the Data Pipeline?' (2019) 15 European Competition Journal 177, 187.
[322] Graef (n 62) 215.
[323] *Bronner* case, para 44.
[324] ibid., para 41.
[325] See among others: *Google/DoubleClick* (Case M.4731) Commission Decision C(2008) 927 final [2008]; *Facebook/Whatsapp* (Case M.7217) Commission Decision C(2014) 7239 final [2014]; *Apple/Shazam* (Case M.8777) Commission Decision C(2018) 5748 final [2018].
[326] Graef (n 62) 218.

collects and/or facilitates access to data (such as data marketplace), is rarely active on the data provider's market. Drexl[327] provides an example of a big data analytics service provider who seeks access to data for purposes of data mining. It is unlikely for the holders of such data to be active as competitors in the market of providing new information generated through big data analyses.

iii. there is no objective justification for the refusal;

Microsoft was the first case in which the notion of objective justification has been analysed in detail in a refusal to deal context. Microsoft argued that its refusal to supply was objectively justified by: (i) the intellectual property rights, (ii) the fact that the technology which it was required to disclose to its competitors was secret, (iii) the circumstance that forced disclosure of the necessary protocols would adversely affect its incentives to innovate.[328] None of these reasons have succeeded before the Court of Justice.

If the intellectual property rights are involved, an additional condition appears: the refusal to supply prevents technical development, previously known as the "new product conditions" for which there is a potential demand. The key issue here is also to determine whether the benefits of compulsory data sharing outweigh its costs. As the report "Competition policy for the digital era" puts it, "a thorough analysis will be required whether such access is truly indispensable, and in addition, the legitimate interests of both parties need to be considered".[329] The conditions of the 'essential facility doctrine' are still evolving. The application of the doctrine to data has been a topic of a much broader discussion. However, despite the attention for the issue, no decision has been issued so far at EU level to force access to data in order to open up data markets.

[327] Josef Drexl, 'Designing Competitive Markets for Industrial Data - Between Propertisation and Access' [2016] SSRN Electronic Journal <https://www.ssrn.com/abstract=2862975> accessed 12 October 2020, 46.
[328] CJEU 17 September 2007, T-201/04, ECLI:EU:T:2007:289 ('Microsoft case'), par. 666.
[329] Crémer and others (n 27) 107.

7.4 Connections to data protection law

In many recent proceedings, competition authorities have analyzed the competition issues arising from the possession and use of data.[330] The European Commission report "Competition Policy for the Digital Era", and the joint paper on data and its implications for competition law by the French Autorité de la concurrence and the German the German Competition Authority ('Bundeskartellamt')[331] shows that there is a notable interdependency between competition law and data protection law.

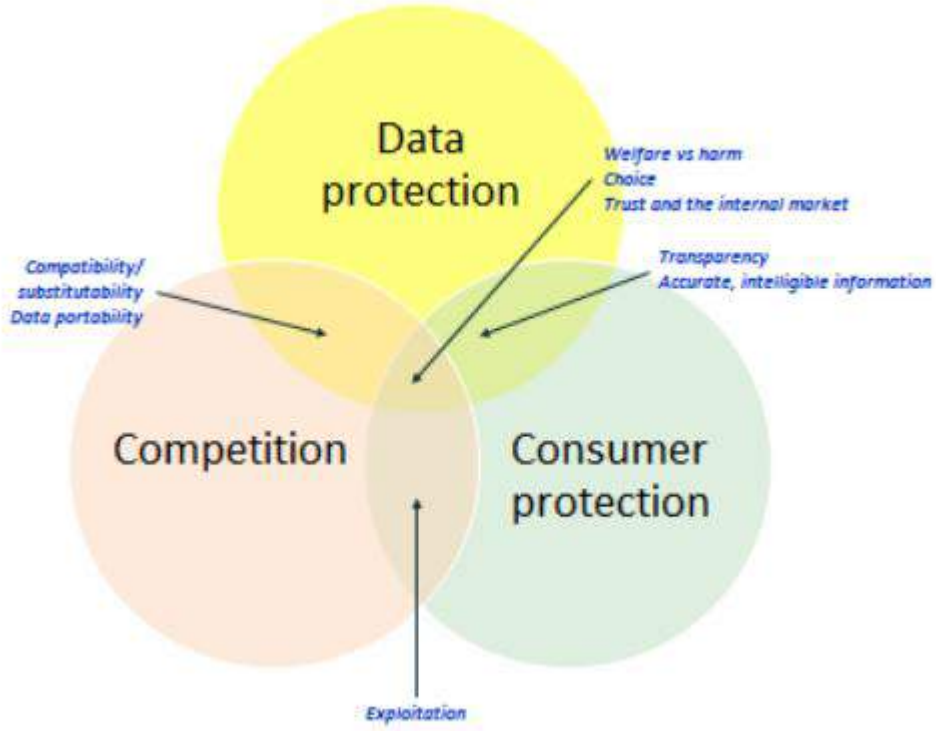

Figure 2: The interplay between data protection, competition law and consumer protection in the Digital Economy.[332]

[330] See: *Google/ DoubleClick* decision, para 359-366; *Facebook / Whatsapp* decision para 180-189; Bundeskartellamt, B6-22/16, 6.02.2019.

[331] Bundeskartellamt and Autorité de la concurrence, 'Competition Law and Data' (2016) <https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2> accessed 14 October 2020.

[332] EDPS, 'Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' March 2014, available at: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf (last visited 11 October 2020).

It is beyond the ambit of this sub-section to provide an exhaustive analysis of the intersections between competition law and other branches of the law in the digital environment. A well-known intersection is this between competition law and personal data protection law (such as the GDPR), when personal data are at stake.

Competition law and personal data protection law are sometimes complementary to each other or supportive one of the other. On the other hand, they may also contradict each other. This sub-section provides illustrations of the two situations.

First, competition law and personal data protection can complement each other or be supportive one of the other. A first example can be found in the new right for data subjects inserted in the GDPR, namely the right to data portability (Art. 20 GDPR), by which data subjects can obtain personal data concerning him or her that he or she has provided to a controller. They can also transmit such data to another controller, directly from controller to controller should the data subject choose for such option. This right is applicable in the case where the data where initially collected based on the consent of the data subject and provided the personal data processing is carried out by automated means. The right to portability is expressly aimed at empowering data subjects with respect to 'their' personal data.[333] The right to data portability is also expected, *inter alia,* to turn data subjects into active customers, who would thereby be able to put service providers in competition.[334] The right to data portability is therefore expected to be pro-competition, at least when the initial controller has a dominant position (e.g. Facebook), in which case portability would prevent lock-in.

Another example is illustrated by the recent 'Facebook saga' triggered by the German Competition Authority ('Bundeskartellamt'). In 2019, the German Competition Authority issued a final decision prohibiting Facebook from combining user data from different sources.[335] Without going into the details of the case, it should be underlined that its groundbreaking character lies in the non-compliance with data protection obligations being used as a benchmark for qualifying exploitative behavior on behalf of Facebook. This is especially relevant in the case of digital markets where services are provided "for free". On a request from Facebook, the Düsseldorf Higher Regional Court ordered the suspensive effect of the Bundeskartellamt decision until the Court rules on the substance of the appeal. And then, in summary proceedings, the Federal Supreme Court overturned that order in June 2020. In essence, the Federal

[333] GDPR, Rec. 68.

[334] Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' [2017] Computer Law & Security Review s 7 <http://www.sciencedirect.com/science/article/pii/S0267364917303333> accessed 15 March 2018; Inge Graef, Jeroen Verschakelen and Peggy Valcke, 'Putting the Right to Data Portability into a Competition Law Perspective' (2013) Annual Review The Journal of the Higher School of Economics 53.

[335] Bundeskartellamt, Press Release 'Bundeskartellamt prohibits Facebook from combining user data from different sources', 07.02.2019, available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (last visited 13th October 2020). The decision is available here: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/AktuelleMeldungen/2019/11_07_2019_decisionFacebook.html (last visited 13th October 2020).

Supreme Court backed the Bundeskartellamt arguments that data protection law could be used as a benchmark to qualify exploitative abuses.[336] This case was however ruled based on national legal provisions, not based on EU competition law. It remains to be seen whether the same reasoning could be imported into EU competition law *mutatis mutandis.*

On the other hand, personal data protection can trump the operation of competition law, particularly when it comes to data sharing. Increased attention has been paid to data sharing as a competition law remedy (see above), i.e. in response to undue denial to share data. However, when personal data are at stake, such a data sharing remedy would constitute a further processing of data and would obviously result in *more* processing of data while data protection traditionally aims to limit the processing of personal data to what is strictly necessary. The legal scholarship has therefore investigated under which conditions competition law authorities could impose data sharing remedies where personal data are involved.[337] The main issue seems to consist in the absence of a clear and specific legal basis for imposing such remedies. Competition law is indeed mainly based on a few principled provisions, which are further complemented by secondary legislation or – more often – soft law guidelines. While this regulatory approach provides much-needed flexibility to competition law authorities, it may find its limit with personal data protection. It remains therefore to be seen whether secondary legislation could constitute an appropriate legal basis for that purpose.

7.5 Conclusion – relevance for TRUSTS

Current data sharing models vary significantly regarding the type of data in question, partners involved and the business interest behind data sharing. In the context of TRUSTS, the relevant questions for legal analysis are, *inter alia*: how will the data flows be designed? Which function(s) will the TRUST platform perform? How will the responsibility and liability be allocated between different partners and the TRUST platform itself? The wide variety of possible answers to these questions make it impossible to provide a "one size fits all" guidance for data sharing.

B2B data sharing is generally done on a contractual basis. The principle of contractual freedom generally governs contractual arrangements. This freedom, however, may be limited by mandatory legislative provisions, such as national contract law provisions, trade secret legislation, IP rights, GDPR or competition law restrictions. Each of these legal frameworks needs to be carefully assessed before data is shared.

The role of data to establish a competitive advantage is one of the elements which must be taken into account when assessing the competitive position of companies involved in trading practices. Data sharing may lead to potentially anti-competitive behaviors (i.e., risk of exclusionary practices, exclusive contracts, tying and bundling practices) which need to be assessed on a case-by-case basis. In particular, TRUSTS partners should ensure that they do not discriminate other competitors and preventing them from

[336] Bundesgerichtshof, KVR 69/19 (Facebook v Bundeskartellamt) 23 June 2020.
[337] Vikas Kathuria and Jure Globocnik, 'Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy', *EU Competition Law Remedies in Data Economy, forthcoming* (Marco Botta, Springer 2019).

accessing the data (especially strategic), if they hold a dominant position on the relevant market. The collaboration on a platform may also hold risks in terms of exclusion, i.e. of competitors not involved in the platform. It is important to make sure that the TRUST platform does not facilitate exclusion of, or discrimination against, certain companies by preventing their effective access to data. Thorough analysis of these factors with regard to the specific dataset will therefore be required.

8 Financial law applicable to data transactions

As follows from the TRUSTS research objectives, in particular Use Case 1, the processing of personal data is necessary for the assessment of anti-money laundering ('AML') risks by a future TRUSTS platform participants (financial institution, fiduciary etc.) prior to entering into a contract with a customer. Here, a distinction shall be made between a research context and a real-world situation. While no real business relationship is foreseen within the TRUSTS research project, this deliverable still provides some practical insights into the real-life deployment of the platform in order to anticipate eventual risks by the consortium partners. Financial institutions and similar entities perform an assessment of AML risks as part of their AML legal compliance obligations.

This section provides an insight into the financial law applicable to data transactions. The first sub-section will start with the insight into the scope of the 4th Anti-money laundering Directive ('4th AML Directive' or '4th AML'), its main definitions, concepts, and reporting obligations (section 8.1). At the same time, this section sheds light on the main changes brought by the 5th Anti-money laundering Directive ('5th AML Directive' or '5th AML'), which was designed to improve and facilitate the implementation of the AML framework in the EU. The second sub-section covers the Second Payment Services Directive ('PSD2') as a legal framework which governs new digital payment services. This part of the deliverable is meant to inform in an anticipatory manner the TRUSTS partners on the EU legal framework on payment instruments, its updates and main challenges.

8.1 The Anti-Money laundering (AML) Directive

The EU AML framework has rapidly evolved during the last years. Recent developments in legislation have aimed to strengthen the EU anti-money laundering and countering the financing of terrorism ('AML/CFT') framework. These include amendments to the 4th Anti-Money Laundering Directive[338] introduced by the 5th Anti-Money Laundering Directive.[339] The 5th Anti-Money Laundering Directive was adopted on 9 July 2018. By 10 January 2020 Member States had to implement these new rules into their national legislation. It shall be noticed that the 5th AML Directive only amended some points, but did not change the AML framework under the 4th AML Directive. More tightened rules were upgraded following the wave of terrorist attacks.

[338] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141 ('4th AML Directive').
[339] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156 ('5th AML Directive').

The work on the rules improvement will continue with the 6th Anti-Money Laundering (AML) Directive,[340] which is meant to be transposed by 2021.[341] The 6th AML Directive was published in the Official Journal of the European Union on 12 November 2018. This is just four months after the 5th AML came into force. The 6th AML Directive is intended to complement and reinforce the AML rules by laying down minimum rules on criminal liability for money laundering. Some key changes envisaged in the 6th AML Directive are meant to enhance international cooperation, apply targeted approach by obliging investigating or prosecuting authorities to use targeted investigative tools, to follow a risk-based approach and to take into account the principle of proportionality and the nature and seriousness of the offences under investigation.[342]

In May 2020, the European Commission's Communication issued an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (C(2020)2800 final) which set a road map for the achievement of its objectives in this area.[343] In its Opinion 5/2020 issued in July 2020, the EDPS assessed the European Commission's Communication. While acknowledging the importance of the fight against money laundering and terrorism financing as an objective of general interest, it calls for the legislation to strike a balance between the interference with the fundamental rights of privacy and personal data protection and the measures that are necessary to effectively achieve the general interest goals on anti-money laundering and countering the financing of terrorism (AML/CFT).[344]

8.1.1 The scope of application

'*Money laundering*' is defined in article 1(3) of the 4th AML Directive, and is kept unchanged in the 5th AML Directive and reads as follows:

"(1) the conversion or transfer of property, *knowing that* such property is derived from criminal activity or from an act of participation in such activity, for the purpose

1. of concealing or disguising the illicit origin of the property or

2. of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action.

[340] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law PE/30/2018/REV/1 OJ L 284 ('6th AML Directive').
[341] Member States are required to transpose the AMLD 6 into national law by 3 December 2020, after which, firms within Member States will have to implement the relevant regulations by 3 June 2021.
[342] Sanctions scanner, Expected Changes For Sixth Anti-Money Laundering Directive available at: <https://sanctionscanner.com/blog/expected-changes-for-sixth-anti-money-laundering-directive-6amld-187> (last visited 20 September 2020).
[343] European Commission, Communication on an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (C(2020)2800 final) 7 May 2020.
[344] EDPS, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 23 July 2020.

(2) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, *knowing that* such property is derived from criminal activity or from an act of participation in such activity;

(3) the acquisition, possession or use of property, *knowing*, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

(4) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points."

The definition of money laundering refers to '*property*', which is defined as: "assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets."[345]

The following entities are bound by the AML legal rules, regardless of their status (legal or natural person), as long as they are acting in their professional activities:

i. auditors, external accountants and tax advisors;
ii. notaries and other independent legal professionals, regarding certain financial transactions;
iii. trust or company service providers;
iv. estate agents;
v. other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
vi. providers of gambling services.

The 5th AML Directive has extended the scope of entities bound by the AML legal rules. Now they also apply to the following subjects:[346]

i. providers engaged in exchange services between virtual currencies and fiat currencies; virtual currencies are defined as a "digital representation of value that can be digitally transferred, stored or traded and is accepted… as a medium of exchange"
ii. custodian wallet providers;
iii. persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more;
iv. persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more.

[345] 4th AML Directive, Art. 3(3).
[346] 5th AML Directive, Art. 1.

8.1.2 Obligations under the AML framework

The AML legal framework contains different levels of customer due diligence obligations (simplified, enhanced). A risk-based approach is used to determine the necessary level of due diligence and the extent of the measures undertaken. Furthermore, the AML legal framework requires the responsible entities to inform the Financial Intelligence Unit ('FIU') on their own initiative when they know, suspect or have reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing.

a) Due diligence

In order to comply with due diligence requirements, the obliged entities must be able to identify the holders of bank accounts. Due diligence makes part of the so-called know your customer (KYC) procedures. This an umbrella term for different AML obligations which include performing of a customer due diligence, carrying out ongoing monitoring of the established business relationship, reporting suspicious activities to the FIUs etc.

Both 4th and 5th AML Directives prohibit the keeping of anonymous accounts. More specifically, 4th AML Directive requires credit and financial institutions to refrain from keeping anonymous accounts or anonymous passbooks.[347] The owners and beneficiaries of existing anonymous accounts or anonymous passbooks must be subject to customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.[348]

Due diligence must be carried out at least in the following circumstances:[349]

i. when establishing a business relationship;
ii. when carrying out an occasional transaction that:
    - amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or
    - constitutes a transfer of funds, as defined in point (9) of article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council (30), exceeding EUR 1 000;
iii. in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
iv. for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
v. when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

[347] 5th AML Directive, Art. 10.
[348] 4th AML Directive, Art. 10.
[349] 4th AML Directive, Art. 11.

vi. when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Derogations are possible if appropriate mitigation measures are taken, such as having a good monitoring system in place to detect unusual or suspicious payment patterns, as per article 12 of the 4th AML Directive. Pre-paid cards must not exceed EUR 250 (in the 5th AML Directive: EUR 150) to be exempt from the due diligence requirement. Likewise, due diligence is triggered by cash redemptions or withdrawals and remote payments above EUR 50.

According to article 13 of the 4th AML Directive (EU) 2015/849, due diligence must comprise of:

i. identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source[350]; identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;[351]
ii. assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
iii. conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

The 5th AML Directive adds an additional nuance to the verification obligation – it must likewise be carried out "whenever entering into a new business relationship with a corporate or other legal entity, or a trust or a legal arrangement having a structure or functions similar to trusts ("similar legal arrangement") which are subject to the registration of beneficial ownership information."[352]

Obliged entities must apply each of the customer due diligence requirements. However, they may determine the extent of such measures on a risk-sensitive basis. At least the variables set out in Annex I must be taken into account when assessing the risks of money laundering and terrorist financing:

i. the purpose of an account or relationship;
ii. the level of assets to be deposited by a customer or the size of transactions undertaken;

[350] In the 5th AML Directive, this is replaced by: identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services.
[351] 5th AML Directive, Art. 13(1)(b) also requires that, if the beneficial owner is identified as the senior managing official, obliged entities must take the necessary reasonable measures to verify the identity of the natural person who holds the position of senior managing official and shall keep records of the actions taken as well as any difficulties encountered during the verification process.
[352] 5th AML Directive, Art. 14(a).

iii. the regularity or duration of the business relationship.

Due diligence means that entities are able to demonstrate to competent authorities or self-regulatory bodies that the measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified. Self-regulatory body means a "body that represents members of a profession and has a role in regulating them, in performing certain supervisory or monitoring type functions and in ensuring the enforcement of the rules relating to them".[353]

Due diligence obligations can be divided into two groups: **simplified due diligence** and **enhanced due diligence**. Simplified due diligence measures can apply to situations identified as lower risk. For this, the obliged entities must ascertain that the business relationship or the transaction presents a lower degree of risk. A sufficient monitoring of the transactions and business relationships is required to enable the detection of unusual or suspicious transactions.[354] **Enhanced due diligence** refers to the cases, when dealing with PEPs or natural persons or legal entities established in the third countries identified by the Commission as high-risk third countries, as well as in other cases of higher risk that are identified by Member States. In this case, obliged entities shall apply enhanced customer due diligence measures to manage and mitigate those risks appropriately. A special attention shall be paid to the background and purpose of all complex and unusually large suspicious transactions which have no apparent economic or lawful purpose. (Article 18 of the 4th AML Directive).

b) Reporting obligations

The responsible entities are required to inform the Financial Intelligence Unit ('FIU') on their own initiative when they know, suspect or have reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing.[355] They must also provide necessary information when requested by the FIU.[356] Such a disclosure of information in good faith shall not constitute a breach of any restriction imposed by contract or by legislative, regulatory, or administrative provisions, and shall also not result in liability.[357] The obliged entities shall also not tip-off the customer or other third parties about the fact that information is disclosed.[358]

The 5th AML Directive goes further than the 4th AML Directive in its reporting obligations. More specifically, it gives the FIU a mandate to obtain the addresses and identities of owners of virtual currency – and so push back against the anonymity associated with the use of cryptocurrency.[359]

Alongside the due diligence requirements, reporting obligations constitute a wide-ranging exercise in data retention, which has implications for human rights and privacy. More on those in the section 8.1.2.

[353] 4th AML Directive, Art. 3(5).
[354] 4th AML Directive, Art. 18.
[355] 4th AML Directive, Art. 33.
[356] ibid.
[357] 4th AML Directive, Art. 37.
[358] 4th AML Directive, Art. 39.
[359] Comply Advantage, 5AMLD – 5th EU Anti-Money Laundering Directive: What You Need to Know, available at: <https://complyadvantage.com/blog/5mld-fifth-anti-money-laundering-directive> (last visited 20 August 2020).

8.1.3 Politically exposed persons

Anti-money laundering regulation is based on the assumption that individuals holding high political office may be at larger risk of bribery or corruption by virtue of the office entrusted to them. Financial Action Task Force on Money Laundering ('FATF') defines a politically exposed person ('PEP') as an "individual who is or has been entrusted with a prominent public function". Potential risks associated with PEPs justify the application of additional preventive measures in scrutinising business relationships and addressing abuses, if they occur.[360] Business relationships shall be understood as "business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration" (Article 3(13) of the 4th AML).

In the 4th AML and 5th AML Directives, a PEP is defined as a natural person who is or who has been entrusted with prominent public functions and includes the following:[361]

i. heads of state, heads of government, ministers and deputy or assistant ministers;
ii. members of parliament or of similar legislative bodies;
iii. members of the governing bodies of political parties;
iv. members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
v. members of courts of auditors or of the boards of central banks;
vi. ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
vii. members of the administrative, management or supervisory bodies of state-owned enterprises;
viii. directors, deputy directors and members of the board or equivalent function of an international organisation.

Due to heightened risks where PEPs are concerned, both the 4th and the 5th AML Directives prescribe obliged entities to carry out an enhanced due diligence procedure, described in the section 8.1.2. Moreover, those entities are required to:[362]

i. have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a politically exposed person. Risk-based procedures are used for determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action (Art. 12 of the Regulation (EU) 2015/847 on information accompanying transfers of funds);[363]
ii. apply the following measures in cases of business relationships with politically exposed persons:

[360] FATF Guidance, Politically exposed persons (Recommendations 12 and 22), para. 1, available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-pep-rec12-22.pdf> (last visited 13 July 2020).
[361] 4th AML Directive, Art. 3(9).
[362] 4th AML Directive, Art. 20.
[363] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance) OJ L 141.

- obtain senior management approval for establishing or continuing business relationships with such persons;
- take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;
- conduct enhanced, ongoing monitoring of those business relationships.

The 5th AML Directive adds a new article 20a, requiring Member States to issue and keep up to date a list indicating the exact functions which qualify as prominent public functions for the purposes of the AML Directive. The lists of prominent public functions shall be sent to the European Commission and may be made public. The European Commission is likewise authorised to compile such a list of the exact functions which qualify as prominent public functions at the level of Union institutions and bodies. That list shall also include any function which may be entrusted to representatives of third countries and of international bodies accredited at Union level. Moreover, the European Commission is empowered to assemble a make public, based on these data, a single list of all prominent public functions which qualify as PEPs.

In accordance with Article 18a of the 5th AML Directive, Member States shall require obliged entities to apply the enhanced customer due diligence measures, such as obtaining additional information on the customer and the beneficial owner, the nature of their business relationship, their source of wealth, the reasons behind intended or performed transactions etc.

8.1.4 High-risk third countries

According to Article 9 of the 4th AML Directive, high-risk third countries shall be understood as third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union. Those countries shall be identified in order to protect the proper functioning of the internal market. The European Commission is empowered to adopt delegated acts in accordance with Article 64 of the 4th AML in order to identify high-risk third countries. Relevant criteria for the European Commission's assessment include the following: the legal and institutional AML/CFT framework, the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing, the effectiveness of the AML/CFT system in addressing money laundering or terrorist financing risks of the third country.[364]

Recital 29 and Article 9 of the 4th AMLD prescribe that Member States should require enhanced customer due diligence measures when dealing with natural persons or legal entities established in high-risk third countries identified by the Commission. Countries not included in the list should not be automatically considered to have effective AML/CFT systems and the assessment on the risk-sensitive basis is required.

According to Article 18 of the 4th AMLD, when dealing with natural persons or legal entities established in the third countries identified as high-risk third countries, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate AML risks.

[364] 4th AML Directive, Art. 9.

8.1.5 Between the GDPR and the AML legal framework

As said above, the 4th AML Directive requires obliged entities to identify and verify the identity of clients, perform customer due diligence, monitor transactions and report suspicious transactions. The majority of these actions require the collection, analysis, storage and sharing by the obliged entities of personal data from their customers. It does not come as a surprise then that the 4th AMLD has several touch points with the GDPR. Moreover, the increased transparency and easiness of access to personal data held in public registries of beneficial ownership information[365] is not easily compatible with the enhanced protection of personal data promised under the GDPR. It is clear that both legal instruments do not share the same objectives. While the AML is aimed at maximising the use of personal data to fight money laundering and terrorism financing (i.e. a general or public interest), the GDPR is precisely aimed at limiting the collection and the use of personal data in order to put individuals in better control of their data (i.e. a private interest).

The 5th AML Directive refers to the GDPR on multiple occasions and commits to ensuring the fundamental right to the protection of personal data, as well as the observance and application of the proportionality principle. The processing of personal data for AML purposes is therefore subject to both pieces of legislation, namely data protection instruments, especially the GDPR, and the AML Directives. While the GDPR rules apply to the "broader" matter of personal data processing operations, the AML framework lays out more specific rule for preventing money laundering. Therefore, we can reasonably assume that the GDPR serves as *legi generali*, and the AML Directive as *lex specialis*, and apply the rule of "*lex specialis derogate legi generalis*". In other words: the obligations laid out in the GDPR apply unless the AML Directives contain a more specific rule.

In practice, complying with both legal frameworks is easier said (or written) than done. While pursuing a good cause, the European Commission, which has an initiative prerogative and a better access to impact assessment practices, found itself between the GDPR rock and the AML Directive hard place.

8.1.6 Convergences between the GDPR and the AML framework

The current section will look at the risk-based nature of the GDPR and the AML framework in order to identify how compliance obligation are tackled by both legal frameworks. This section will inform Use Case 1 partners on their compliance obligations within the TRUSTS project and also provide a broader overview of the interaction between two legal acts (GDPR and AML legal framework).

a) **Risk based nature of the GDPR**

At the time of its inception, data protection was seen as an attempt to tame and regulate risks posed by computers.[366] The GDPR embraces a risk-based approach (as vague as it may sound) to data protection by

[365] 5th AML Directive, Rec. 28.
[366] Raphael Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5(1) International Data Privacy Law, 5.

encouraging controllers to perform the assessment of personal data processing operations in order to identify activities posing a high risk to data subjects and adopt tailored responses. In other words, compliance measures shall be tailored to the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.[367]

The promoters of a risk-based approach argued that legal compliance should shift to the framing of responsible data use based on risk management.[368] Article 35 of the GDPR is the first risk management method enshrined in European data protection law.[369] It provides for an obligation for the controller to carry out an evaluation of the impact of the envisaged processing operations on the rights and freedoms of natural persons, prior to the processing ('data protection impact assessment' or 'DPIA'). The rights and freedoms of the data subjects primarily concern the right to privacy and data protection, but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.[370]

Moreover, the risk-based nature of the GDPR is translated through the requirement of a higher standard of protection with regard to some specific cases, such as the processing of special categories of data or children's personal data. In addition, many provisions of the GDPR require the assessment of the likelihood and severity of the risk in the sense that technical and organisational measures are adjusted in a scalable manner to risk levels of controllers' activities (this will be substantiated in the table below).

Such a risk-based approach ensures the flexibility necessary to encompass a wide variety of different situations. The risk-based approach "provides a way to carry out the shift to accountability that underlies much of the data protection reform, using the notion of risk as a reference point in light of which we can assess whether the organisational and technical measures taken by the controller offer a sufficient level of protection".[371] The cornerstone of any compliance exercise grounded in risks-based scalability culminates with the obligation to conduct a DPIA.[372] Article 35 GDPR established minimum requirements for riskier processing operations rather than a provision limiting DPIA to only a subset of activities.[373]

Two major aspects with respect to the risk-based approach are worth highlighting. First of all, data protection compliance obligations and compliance should depend upon the risks that data processing activities present for individuals. Second, the analysis of the level of risks (and the subsequent compliance

[367] GDPR, Rec. 74.

[368] Article 29 Working Party, Statement on the role of a risk-based approach in data protection legal framework, 30 May 2014 available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (last access on 18 April 2019, 2-3).

[369] Raphael Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34(2) Computer Law & Security Review 279–88.

[370] Article 29 Working Party, Statement on the role of a risk-based approach in data protection legal framework.

[371] Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9(3) *European Journal of Risk Regulation*, 502–526. https://doi.org/10.1017/err.2018.47.

[372] Athena Christofi et al, 'Erosion by Standardisation: Is ISO/IEC 29134:2017 on Privacy Impact Assessment Up to (GDPR) Standard?. Personal Data Protection and Legal Developments in the European Union' (2020) 140 - 167 *Publisher: IGI Global.*

[373] ibid.

measures) should in certain cases be left for the controller to decide (cf. DPIA as a prime example). This allows for a better compliance flexibility.

The table below summarizes the scalable nature of the GDPR compliance obligations depending on several factors, such as data categories, data subjects categories, likelihood and severity of the risk to the rights and freedoms of data subjects.

Risk level (high or not) based on	Risk-based compliance obligation
Categories of data (sensitive) (Recital 51, 53)	Personal data which are, by their nature, particularly **sensitive** in relation to fundamental rights and freedoms **merit specific protection** as the context of their processing could create significant risks to the fundamental rights and freedoms.
Categories of data subjects (children) (Recital 38)	**Children merit specific protection**, as they may be less aware of the risks.
Likelihood and severity of the risk for rights and freedoms of natural persons	**The higher the risk, the stricter the compliance obligation:** • the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures (Article 25) • the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security (Article 32) • the controller must notify the personal data breach to the supervisory authority (Article 33) • the controller shall communicate the personal data breach to the data subject without undue delay (Article 34, Recital 86) • obligation to perform the DPIA (Article 35, Recital 84, 90, 91, 94) • obligation to notify the processing of personal data to the supervisory authorities (Recital 89) • obligation to keep records of processing activities (Article 30) • obligation to appoint a data protection officer (Articles 37-39)

Table 1 Description of risk-based provisions in the GDPR

b) **Risk-based nature of the AML Directive**

At the time of its inception, the AML framework adopted a static approach and imposed standard reporting obligations on regulated entities for transactions over a certain threshold.[374] The inflexibility and rigidity of purely such a rules-based system required an alternative solution for identifying and mitigating the risks of money laundering and terrorist financing. Traditional regulatory approach mandating either specific behaviours in a command-control way or particular measurable outcomes was ill-fitted for the rapidly evolving context with the increasing role of firms themselves in identifying, assessing, and mitigating risks.[375]

The AML legal framework, thus, advocates for the risk-based approach for the review of existing clients. In this context, risk refers to measuring the impact and likelihood of money laundering and terrorist financing ('ML/TF') taking place and adopting appropriate measures proportionate to those risks.[376] Risk means an inherent risk that exists before mitigation; it does not refer to residual risk that remains after mitigation.

In this context, 'risk' shall be understood as likelihood of ML/TF taking place. And 'risk factors' means variables that may increase or decrease the ML/TF likelihood of a business relationship or occasional transaction.[377] Several risk factors shall be taken into account for AML detection purposes:[378]

i. the customer's and the customer's beneficial owner's reputation. Beneficial owner means any natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted[379];
ii. the customer's and the customer's beneficial owner's nature and behaviour;
iii. the customer's and the customer's beneficial owner's business or professional activity;
iv. the customer or beneficial owner's links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement;
v. beneficial owner's links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals;
vi. The customer or beneficial owner's links to sectors that involve significant amounts of cash;

[374] Carsten Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet: Adopting the Anti-Money Laundering Framework to Online Platforms' (2018) 26(3) *International Journal of Law and Information Technology* 226–51, https://doi.org/10.1093/ijlit/eay008. For instance, for any transaction involving a sum amounting to ECU 15 000 or more, whether the transaction is carried out in a single operation or in several operations which seem to be linked.

[375] Lishan Ai and Jun Tang, 'Risk-based Approach for Designing Enterprise-wide AML Information System Solution' (2011) 18 Journal of Financial Crime 268.

[376] Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (2018).

[377] ibid.

[378] ibid.

[379] 4th AML Directive, Art. 3(6).

vii. existence of adverse media reports or other relevant sources of information about the customer, such as any allegations of criminality or terrorism against the customer or the beneficial owner.
viii. The credibility of these reports shall be also analysed;
ix. Some further aspects might also be relevant, such as the nature of the business, political connections, whether they are a Politically Exposed Person ('PEP');
x. It is also relevant to check whether the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain.

The 5th AML Directive foresees a range of exceptions for certain categories of high risk clients that shall be monitored regularly. For instance, the 5th AML Directive reads as follows: "the approach for the review of existing customers in the current framework is risk-based. Article 4 of the 4th AML Directive also refers to a risk-based approach. However, given the higher risk of money laundering, terrorist financing and associated predicate offences associated with certain intermediary structures, that approach might not allow for the timely detection and assessment of risks. It is therefore important to ensure that certain clearly specified categories of existing customers are also monitored on a regular basis".[380] The wording of this recital suggests that several risk can be identified for an enhanced scrutiny in order to avoid money laundering or terrorist financing.

8.1.7 Divergences between the GDPR and the 4th AML Directive

Complying with both data protection and AML requirements is not straight-forward task as the combination of both legal instruments creates a number of tension points. The 4th AML Directive seems to acknowledge this problem and devotes an entire chapter on the relationship between the AML and the GDPR requirements (Chapter V on Data Protection, Record Retention and Statistical Data).

This section will look on certain divergences between the 4th AML and the GDPR.

a) Lawfulness of processing

In cases where the obliged entities would process personal data in the framework of *'fighting money laundering and terrorist financing'* the legal basis for such processing would be the necessity to comply with a legal obligation under Art. 6(1)(c) of the GDPR.

However, the question raises what is the legal basis for processing personal data under the AML legislation for other reasons then complying with the 'legal obligation' (e.g. to outsource the performance of the KYC exercise or transferring data to the financial institution). One of the possible basis under the GDPR could be "the performance of a contract".[381] However, this legal basis applies when the processing is necessary in the framework of the 'normal performance' of a contract between the customer (data subject) and the obliged entity (data controller). The 29WP has excluded the possibility of data processing for fraud prevention under this legal basis: "fraud prevention - which may include, among others, monitoring and

[380] 5th AML Directive, Rec. 24.
[381] GDPR, Art. 6(1)(b)

profiling customers - is another typical area, which is likely to be considered as going beyond what is necessary for the performance of a contract. Such processing could then still be legitimate under another ground of Article [6], for instance, consent where appropriate, a legal obligation or the legitimate interest of the controller (…)".[382]

As suggested by the 29WP, it would be possible to argue that the data transfer is necessary for the purposes of the legitimate interest pursued by a third party (i.e. the financial institution). As has been said before, relying on the "legitimate interest" requires to meet a high threshold of the 'balancing test' between the legitimate interests of the third party and the need for protection of customers' data protection rights. It could also be argued that the transfer of data from the obliged entity to a third part (e.g. to the financial institution) might fall under a task carried out in the 'public interest' (cfr. Article 6(1), e) GDPR). Indeed, Article 43 of the 4th AML Directive provides that "the processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing (…) shall be considered to be a matter of public interest".

Although, in our view, the 'public interest' ground is likely to be found as a legitimate, transferring personal data gathered while complying with the AML obligations is subject to case-by-case analysis and requires a thorough analysis on whether such 'public interest' exists.

b) Information rights

Article 12 GDPR sets out the modalities for the exercise of the rights of data subjects, including the right to be informed of certain particulars regarding the processing of their personal data. Among others, any communication issued by the controller in that context must be phrased in a concise, transparent, intelligible and easily accessible form, using clear and plain language. [383] The controller must also facilitate the whole procedure.[384] The Regulation introduces a one-month time limit to react to any request made by the data subject, which may be extended by two further months when justified by the complexity or number of requests.[385] As an important improvement to the current *status quo*, the Regulation also empowers data subjects to exercise their rights free of charge.[386] Before answering a request, the controller may also seek the provision of additional information to confirm the identity of the data subject.[387]

Article 15 GDPR grants the data subject the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where this is the case, access to

[382] Opinion 06/2014 of 29WP on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, 844/14/EN WP 217 17. This is confirmed in point 47 of the Guidelines 2/2019 of the EDPB on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subject, adopted on 9 April 2019.
[383] GDPR, Art. 12(1).
[384] GDPR, Art. 12(2).
[385] GDPR, Art. 12(3).
[386] GDPR, Art. 12(5).
[387] GDPR, Art. 12(6).

these data. Article 15(1) GDPR provides a list of all the information the data subject is entitled to receive, such as:

i. the purposes of the processing;
ii. the categories of personal data concerned;
iii. the recipients or categories of recipients to whom the personal data have been or will be disclosed;
iv. the retention period;
v. the existence of the right to rectification or erasure;
vi. the right to lodge a complaint with a supervisory authority;
vii. the source of the personal data;
viii. the existence of automated decision-making.

The right of access is the essential first step toward the exercise of the other prerogatives granted to data subjects. Neither rectification nor erasure of personal data, nor blocking or objecting to their processing, seem easy or even possible unless the data subject knows exactly what data the controller processes and how. Additionally, it plays a crucial role in assessing controllers' compliance with data protection rules. Therefore, it is extremely important that controllers take all the necessary steps to adequately comply with Article 15 GDPR.

However, under Article 41(4) of the 4th AML Directive, Member States may adopt legislative measures restricting the data subject's right of access to personal data (as foreseen under Article 15 GDPR). The 4th AML Directive allows Member States to restrict the right of access if necessary and proportionate to enable undertakings to fulfil their tasks properly or to avoid that investigations of money laundering and terrorist financing are jeopardised.[388]

It is possible that the activation of the rights of access and right to information provided for by Articles 12-15 of the GDPR could have the effect of impairing attempts, for example by a financial institution, to combat money laundering and terrorist financing. Informing individuals of the peculiarities of the data that is being held and/ or collected could have the unintended consequence on the institution's investigation.

Therefore, the tension raises, between, on the one hand, individuals' right to privacy, on the other, the sensitivity of investigations into anti-money laundering issues. In that regard, the obliged entity should in every case check whether the national legislation provides for an exception to the right of the data subject to get access to his/her personal data. As a general rule, data subject request should be answered within 1 month deadline. The Article 23(1) of the GDPR allows restrictions on the data subject's rights only in specific circumstances, when such a restriction would be necessary and proportionate to protect the public interest such as prevention, investigation, detection or prosecution of criminal offences.[389]

c) Transfer of personal data to third countries

Articles 39, 42 and 45 of the 4th AML Directive require obliged entities to:

[388] ibid.
[389] GDPR, Art. 23(1).

(i) share data with foreign regulators in accordance with the 4MLD's newly extended reporting obligations; and

(ii) put in place policies for data sharing across group-companies located in third countries for AML/CIT purposes. Article 39(3) and 39(5) of 4MLD set out the circumstances in which obliged entities may share with other obliged entities in a third country provided that: i. the other entity is in a third country with equivalent AML laws; ii. the entities are in the same professional category; and iii. the entities are subject to data protection obligations in their jurisdiction.

However, Article 44 of the GDPR prohibits transfers of personal data to third countries, unless specific circumstances are met such as adequacy decisions, data protection clauses and additional safeguards to demonstrate the adequate level of protection of personal data (binding corporate rules, approved industry codes with binding and enforceable commitments).

At the same time, Article 49(1)(d) of the GDPR sets out a mechanism for transfers which are necessary for *"important reasons of public interest"*. However, it is not known yet whether this clause operates to capture actions undertaken to deter money laundering and terrorist financing.

Article 49(4) GDPR states that such public interest needs to be 'recognised' by the law of the relevant Member State. In addition, Article 49(1) also allows non-repetitive transfers of personal data of limited numbers of individuals if those transfers are necessary for the purposes of compelling legitimate interests pursued by the obliged entities, and those interests are not overridden by the interests or rights and freedoms of individuals.[390] To determine whether this is the case, obliged entities will need to undertake *"legitimate interests*" assessments, weighing up and balancing the interests of both parties.

d) Transparency of the beneficial ownership information

In response to the 'Panama Papers' revelations of April 2016, the European Commission started the revision process of the 4th AML Directive in order to tackle tax evasion as well as anti-money laundering practices and terrorist financing in a more efficient manner. The proposed amendments included, *inter alia*, increasing transparency of the beneficial ownership[391] information, enhancing information sharing between financial supervisory authorities, applying stricter monitoring to transactions with high-risk third countries. Furthermore, the new AML rules were extended to apply to virtual currencies[392] by restricting their anonymous use.

[390] Article 29 Working Party, Guidelines on Article 49 of Regulation 2016/679 WP262, 6 February 2018.

[391] 'Beneficial owner' means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted. In the case of corporate entities: the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. In the case of trusts: (i) the settlor; (ii) the trustee(s); (iii) the protector, if any; For more information see 4th AML Directive, Art. 3(6).

[392] 'Virtual currencies' means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically. For more information see 5th AML Directive, Art. 3(18).

The 5th Anti-Money laundering directive broadened access to beneficial ownership information by both competent authorities and the public. In the Opinion 1/2017, the EDPS expressed a number of concerns relating to the respect of the principles of purpose limitation and proportionality by the amendments introduced by the 5th AML Directive.[393] In particular, lack of safeguards to avoid that personal data collected for the purpose of AML/CFT are used for other purposes, such as countering tax evasion or enhancing corporate transparency. Moreover, the EDPS insisted on a proper assessment of the proportionality of the policy measures with regard to the access to information on financial transactions by FIUs, and the broadening of the access to beneficial ownership information to both competent authorities and the public.

Under the 5th AML Directive, Member States are required to set up centralised mechanisms or central registries containing all the necessary data for the identification of holders of bank accounts.[394] National FIUs and AML/CFT competent authorities shall be granted full and swift access on a "need to know" basis to the information kept in the registry for a faster detection of suspicious transactions. In order to comply with data protection rules, such registries shall only include the minimum data. Data subjects must be informed of their rights and must be given a contact point[395] for exercising their rights of access and rectification. Data shall not be stored for longer than necessary and shall be deleted once no longer needed in accordance with the national rules.

The 5th AML Directive introduced the reinforced rules on access to beneficial ownership information. Granting public access to beneficial ownership information allows greater scrutiny of information by civil society, including by the press or civil society organisations. However, the amendments proposed shall strike a balance between the rights privacy and to the protection of personal data and the need for more transparency in financial and economic activities. The data made available to the public must be strictly limited to economic activities of beneficial owners and must be *"adequate, accurate and up-to-date"*.[396] With regard to trusts or similar legal arrangements, the access to beneficial ownership information should be granted to any person demonstrating a *"legitimate interest"* or to any person filing a written request.[397] It is for the Member States to determine whether those requests are in line with the objectives of the Directive.

e) Purpose limitation

Under the GDPR data may only be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with these purposes. [398] Under the AML Directive, all data collected in the framework of the AML Directive should fit within “fight against money laundering and terrorist financing” purpose.[399] However, such purpose is quite broad. The AML Directive itself explains

[393] EDPS, Opinion 1/2017 on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC Access to beneficial ownership information and data protection implications.
[394] 4th AML Directive, Art. 9(2).
[395] 4th AML Directive, Art. 48(a).
[396] 5th AML Directive, Rec. 25.
[397] 5th AML Directive, Rec. 28.
[398] GDPR, Art. 5(1)(b).
[399] 4th AML Directive, Art. 1(1) and Art. 41(2).

that processing of personal data within the purposes of the AML Directive means that data can only be processed "for the activities required under this Directive such as carrying out customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person, sharing of information by competent authorities and sharing of information by credit institutions and financial institutions and other obliged entities".[400] As has been said above in the section relating to the transparency of the beneficial ownership information, the 5th AMLD also introduced combatting of tax evasion as a purpose of the AML Directive. What it means is that when personal data is collected to in order to "fight money laundering or terrorist financing", but it does not fall within the specific activity mentioned above, such processing of personal data could infringe the purpose limitation principle under the GDPR.

f) Data retention

The 4th AML Directive provides for a fixed data retention period of 5 years after the end of the business relationship with the customer or after the date of an occasional transaction. After 5 years, the personal data must be deleted. Member States may however allow further retention for a period of 5 years where the necessity and proportionality of such further retention has been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing.[401]

The 5th AMLD explicitly provides that the additional retention period of 5 years is without prejudice to national law which allows in certain circumstances longer retention periods to facilitate criminal or administrative proceedings.[402] Under the GDPR, the storage limitation principle does not allow for identifiable personal data to be processed and stored "for longer than necessary for the purposes for which the data are processed".[403] However, the GDPR allows for further retention of the personal data in cases it is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest.[404]

The question raises whether the general 5-year retention period mentioned in the AML Directive should be interpreted strictly. If the AML Directive is to be regarded as *lex specialis* to the general rules of the GDPR, that would indeed be the case. One must also remember about the national rules, especially these dealing with personal data of a suspect being under pending investigation (which might exceed the 5 years).

[400] 4th AML Directive, Rec. 43.
[401] 4th AML Directive, Art. 40(2).
[402] 5th AML Directive, Recital 21.
[403] GDPR, Art. 5(1)(e).
[404] GDPR, Recital 65.

8.2 The Second Payment Services Directive (PSD2)

This section covers the legal framework with regards to the EU rules for electronic payments (Payment Services Directives). It is meant to inform the partners involved mostly Use Case 2 which have as their main purpose to verify that TRUSTS services can be used to advance current marketing activities in a GDPR compliant manner, through correlating anonymized banking and telecommunications data. The first sub-section provides insights into the requirements for payment services, and the rights and obligations of users and providers of payment services. The second sub-section discusses the relationship between the PSD2 and the GDPR.

8.2.1 Introduction

In 2007 the First Payment Services Directive ('PSD1')[405] provided the legal basis for the creation of an EU-wide single market for payment services across the European Economic Area, covering all types of electronic and non-cash payments, such as credit transfers, direct debits, card payments, mobile and online payments. The directive laid down rules about the information that payment services providers have to give to consumers and about the rights and obligations linked to the use of payment services.

In 2015, the EU adopted the Second Payment Services Directive ('PSD2')[406] to improve the existing rules so that they cover the new digital payment services. The PSD2 applies to '*payment services*' provided by payment service providers ('PSPs'). Payment services are listed in Annex I of the Directive. The list is exhaustive, which means that any kind of monetary transaction or transfer that is not mentioned in it, cannot be considered a payment service and does therefore not fall under the scope of the Directive. Payment services providers are entities that fall into any of the following six categories: (1) credit institutions,[407] (2) electronic money institutions, (3) post office giro institutions, (4) payment institutions, (5) the European Central Bank and national central banks (when not acting in their capacity as monetary authority or other public authorities), and (6) Member States or their regional or local authorities (when not acting in their capacity as public authorities).[408]

The PSD2 aims to:

i. Tackle fraud and abuse in online payments

The PSD2 introduces strict security requirements for the initiation and processing of electronic payments. Payment service providers must apply the so-called "strong customer authentication" ('SCA') when a payer

[405] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, p. 1–36.
[406] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35–127 ('PSD2').
[407] As defined in point (1) of article 4, (1) of Regulation (EU) No 575/2013.
[408] PSD2, Art. 1(1).

initiates an electronic payment transaction.[409] "Strong customer authentication" means an authentication based on the use of two or more elements: the breach of one does not compromise the reliability of the other(s). It is designed in such a way as to protect the confidentiality of the '*authentication data*', namely data which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials.[410] "Personalised security credentials**"** are personalised features provided by the payment service provider to a payment service user for the purposes of authentication.[411]

The PSD2 also introduces the category of "sensitive payment data", namely data, including personalised security credentials which can be used to carry out fraud.[412]

ii. Open the EU payment market to competition and enhance consumers' choice

The PSD2 rules apply equally to traditional banks and to new digital payment services and service providers (so called FinTechs). The PSD2 also aims to facilitates customer mobility: should they want to use such new FinTech services, they cannot be prevented by their banks from doing so. Any bank that offers online access to accounts must cooperate with FinTech companies or with other banks providing such services. Consumers and companies using these services have to grant access to their payment data to third parties providing payments-related services ('TPPs'). These are, for example, payment initiation service providers ('PISPs') and account information service providers ('AISPs'). The "open banking" concept offers consumers more freedom, but also allows third parties to access the data traditionally held by banks, and build applications and services around this data.

iii. Better protect consumers and improve complaints procedure;
iv. Prohibit surcharging (additional charges for payments with consumer credit or debit cards);
v. Strengthen the role of the European Banking Authority (EBA) to coordinate supervisory authorities and draft technical standards.

8.2.2 Interaction between the PSD2 and the GDPR

As said above, the PSD2 requires financial institutions to open up their infrastructure and give access to data (including personal data) to third party providers ('TPPs'). On the other hand, the GDPR protects personal data and restricts sharing of personal data if none of the legal basis of the GDPR applies. As a result, the tensions between the two pieces of legislation may arise.

The preamble to the PSD2 recognizes that "provision of payment services by the payment services providers may entail processing of personal data".[413] While there are many provisions, especially those on

[409] PSD2, Art. 97.
[410] PSD2, Art. 4(29), Art. 4(30).
[411] PSD2, Art. 4(31).
[412] PSD2, Art. 4(32).
[413] PSD2, Rec. 89.

access to information by payment services providers, which arguably contain a broad link to data protection law, Article 94 of the PSD2 is the only explicit provision on the subject-matter.

The Directive only allows for processing of personal data by payment systems and payment service providers "when necessary to safeguard the prevention, investigation and detection of payment fraud."[414] It then continues by stating that the Directive 95/46/EC (now replaced by the GDPR) and the national rules which transpose it, are applicable to the processing of personal data for the purposes of the Directive.[415] In practice, payment service providers must comply with the requirements of the GDPR, namely inform their customers about how their data will be processed, comply with other customers' rights of access, the right to be forgotten, etc. This has been confirmed by the European Data Protection Board Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR: "[t]hus, controllers acting in the field covered by the PSD2 must always ensure compliance with the requirements of the GDPR, including the principles of data protection set out in Article 5 of the GDPR, as well as the relevant provisions of the ePrivacy Directive".[416]

Finally, Art. 94(2) of the PSD2 provides that "payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user".[417]

a) Lawful grounds for processing

Under the PSD2 account holders can exercise control over the transmission of their personal data and no data processing can take place without the "*explicit consent"* of the consumer. Under the GDPR however, data may be processed based exclusively on an exhaustive list of legal bases mentioned in Article 6(1). The question raises which legal ground for processing personal data applies.

The EDPB Guidelines clarifies that "the consent of Article 94 (2) of the PSD2 is not a legal ground for the processing of personal data".[418] It also explains that "[p]ayment services are always provided on a contractual basis between the payment services user and the payment services provider. As stated in recital 87 of the PSD2, "[t]his Directive should concern only contractual obligations and responsibilities between the payment service user and the payment service provider."[419] It follows from there that there is no *lex specialis* relationship between the two legal acts. The payment service provider has to comply with both Article 94 of the PSD2 (the explicit consent requirement) and the GDPR provisions (requiring a lawful basis for data processing e.g. consent, compliance with legal obligation, legitimate interests, contractual necessity, etc.).

[414] PSD2, Art. 94(1).
[415] PSD2, Rec. 89.; PSD2 Art. 94(1).
[416] European Data Protection Board, 'Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR' (2020), para 1.
[417] PSD2, Art. 94(2).
[418] European Data Protection Board (n 12) para 38.
[419] ibid para 14.

b) "Explicit consent"

Customer's consent mentioned in the PSD2 has to be "*explicit*". The question raises whether or not this is the GDPR consent. Or rather, is it specific, *explicit* PSD2 consent that should not be read as 'GDPR consent'? Consent under the GDPR shall be freely given, specific, informed and unambiguous. Also, it shall be given by a clear affirmative act.[420]

The GDPR mentions "explicit consent" in several places. Processing of special categories of personal data may be allowed if "the data subject has given explicit consent".[421] Similarly, automated individual decision-making, including profiling is allowed when it "is based on the data subject's explicit consent".[422] However, there is no definition of explicit consent under the GDPR.

There has been much discussion over the notion of "explicit consent" under the GDPR. The UK Information Commissioner's Office ('ICO') stated that "explicit consent is not defined in the GDPR, but it is not likely to be very different from the usual high standard of consent".[423] The ICO finds that the key difference is likely to be that 'explicit' consent must be affirmed in a clear statement (whether oral or written).

According to the EDPB Guidelines 05/2020 on consent under Regulation 2016/679, "the term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future".[424] Under no circumstances can consent be inferred from potentially ambiguous statements or actions. A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service.[425]

The EDPB Guidelines clarify that when it comes to the explicit consent under the PSD2, referred to in Article 94(2) PSD2, the "explicit consent" is a "contractual consent".[426] Data subjects must be made fully aware of the specific categories of personal data that will be processed and of the specific (payment service) purpose for which their personal data will be processed and have to explicitly agree to these clauses. The object of the explicit consent under Article 94 (2) PSD2 is the permission to obtain access to those personal data, to be able to process and store these personal data that are necessary for the purpose of providing the payment service.[427] In conclusion, explicit consent under the PSD2 is different from (explicit) consent under the GDPR. "Explicit consent" under PSD2 is an additional requirement of a contractual nature.

[420] GDPR, Art. 4(11).
[421] GDPR, Art. 9(2)(a).
[422] GDPR, Art. 22(1)(c).
[423] See Information Commissioner's Office; Document available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/
[424] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679', para 93.
[425] European Data Protection Board (n 12) para 32.
[426] ibid. para 36.
[427] ibid.

Moreover, there are some points, which, even if not contradictory, should be carefully considered when processing personal data under the PSD2 is concerned.

c) Transparency and information requirements

Under Title III, Transparency of conditions and information requirements for payment services, PSPs are required to provide users with certain information, on principle free of charge.[428] The payment service provider must be able to prove that it has supplied the user with the necessary information and carries the '*burden of proof*'.[429] Transparency and accountability are also two fundamental principles of the GDPR. Both legal frameworks are therefore complementary.

In practice, Article 13 of the GDPR lists the information which must be provided where personal data are collected from the data subject, and Article 14 provides which information has to be provided where personal data have not been obtained from the data subject. Both lists include, inter alia, the following information:

i. the identity and the contact details of the controller and, where applicable, of the controller's representative;
ii. the contact details of the data protection officer, where applicable;
iii. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
iv. the categories of personal data concerned;
v. the recipients or categories of recipients of the personal data, if any.[430]

Moreover, data controller must provide information necessary to ensure fair and transparent processing, including the period for which the personal data will be stored, the legitimate interest, if any, the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability, etc.

The EDPB Guidelines operationalizes these requirements by encouraging "a layered approach". In order to avoid information fatigue, and ensure the effectiveness of the information, all information should not be displayed in a single notice on a screen. Rather, the *'layered privacy statements/ notices'* should be used to link to the various categories of information which must be provided to the data subject. Data controllers may also choose additional tools to provide information to the individual data subject, such as privacy dashboards.

d) Silent party data processing

"Silent party data" are personal data concerning a data subject who is not the user of a specific payment service provider, but whose personal data are processed by that specific payment service provider for the

[428] PSD2, Art. 40.
[429] PSD2, Art. 41.
[430] GDPR, Art. 13-14.

performance of a contract between the provider and the payment service user.[431] When payment services are provided by a "silent party", measures should be taken not to unduly disclose personal data. In that regard, the question of legitimate interests (carrying out payments/enabling account information services) as legal grounds, and may we add – also questions of data minimisation and purpose limitation, arise.

e) Profiling, automated decision-making and processing of sensitive data/special categories of data

GDPR rules that apply to special categories of data and automated decision-making, including profiling, are highly relevant to and fully apply in the PSD2 context. A person's bank account may reveal different kinds of behavioural patterns, and personal data concerning health may be gathered from analysing medical bills paid by a data subject. In such cases, only explicit consent may be legal grounds for their processing, and consumers should be able to select which data they wish to share with payment services providers.

f) Data minimisation and data security

Different actors (traditional payment services providers, such as banks; account information services and payment information services) should have access to different amounts and types of data based on the (strict) necessity of access. The TPP accessing payment account data in order to provide the requested services must also take the principle of data minimisation into account and must only collect personal data necessary to provide the specific payment services requested by the payment service user. In this respect, the EDPB recommends the use of "digital filters" in order to support account information service providers in their obligation to only collect personal data that are necessary for the purposes for which they are processed.[432]

Moreover, where a data breach involves financial data, the data subject may be exposed to considerable risks. The higher the risk associated with the processing, the higher the security standards that need to be applied.

[431] European Data Protection Board (n 12) para 44.
[432] ibid para 63.

9 Blockchain and law

The blockchain technology is contemplated to be used in TRUSTS data market ecosystem, including smart contracts which could automate data transactions. This section introduces the blockchain technology and smart contracts and outlines the points of contact of such technologies with the law. The first sub-section defines the blockchain technology and smart contracts and undertakes to understand why they are often contemplated as supporting technologies for data markets. In a second sub-section, we will outline the EU policies towards blockchain legal and regulatory framework. At this stage of development of the TRUSTS research project, we do not have sufficient information over the concrete expected use of the blockchain technology. Therefore, this deliverable cannot provide a detailed and exhaustive analysis of the legal challenges arising from the use of the blockchain technology in TRUSTS. Additionally, the legal analysis of smart contracts makes part of the scope of Task 3.2. In this context, the third and last sub-section will outline in general terms potential points of contact between the blockchain technology and the operation of the law.

9.1 Why are the blockchain technology and smart contracts considered for data markets?

9.1.1 The blockchain technology

The blockchain technology can be defined as a digital decentralised ledger technology. According to Wright and De Filippi, the blockchain technology is a "distributed, shared and encrypted database that serves as an irreversible and incorruptible public repository of information".[433] Blockchain has two main characteristics: first, it is a distributed database that is stored on various 'nodes' (the server or computer that store a copy of the database). As a result, the ledger's data is resilient as it is simultaneously stored on many nodes so that even if one or several nodes fail, that does not affect the data. Second, the database is modified chronologically, by the addition of new blocks, leading to a chronological chain of blocks, hence the name. The blocks are added to the database following a dedicated procedure called the 'consensus' by which a decision can be made which 'miner' is allowed to add the following block, which is then duplicated by all the nodes. The blockchain technology is not a groundbreaking technology. Its innovation rather lies in the "combination of existing technologies: peer-to-peer networks, cryptographic algorithms, distributed data storage and decentralised consensus mechanisms".[434] The blockchain technology is disruptive in that it allows distributed coordination of people by technically performing authentication of data as well as timestamping transactions when being processed and stored, without the need to resort to a certifying or trusted intermediary. This is deemed as the "trustless trust" feature of the blockchain

[433] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2580664 2.
[434] ibid 4–5.

technology.[435] Blockchain users could "trust the technology, which dispenses from the need to trust human counterparties or institutions".[436]

This is why the blockchain technology is often advocated for in no trust environments. The blockchain technology is for instance expected to bring its "trustless trust" to emerging data markets. At the extreme, it would allow data market users to do away with trust in the other parties in the data market ecosystem, such as the other party to the data transaction (data provider and data user) but also the intermediaries supporting the data transaction. The blockchain technology is all about the circumvention of intermediaries traditionally necessary to bring trust between parties,[437] by computed decentralisation and distribution.[438] In that sense, the blockchain technology is about "resolv[ing] the problem of how coordination of individuals' activity could be ensured without a central authority guaranteeing the validity of transactions".[439] In sum, looking at the blockchain technology implies to try and do away with centralised intermediaries (such as the model of a centralised online platform), because of the fear that such intermediaries would end up abusing this strong position.

Not all blockchain networks are the same. Every blockchain is subject to specific governance rules, which significantly affect the legal analysis. Although many typologies exist, blockchain networks are often categorised as either 'public' or 'private' ones.

9.1.2 Public v private blockchains

Public blockchains are also 'permissionless'. They are the archetype of the blockchain. They can be accessed and used by anyone, without restriction. Any user can theoretically play any role in the blockchain ecosystem (i.e. any 'node' can become a 'miner' and participate in the consensus mechanism).[440] Public blockchains have a high level of transparency. They are 'immutable' (in the blockchain parlance), such that in principle no node is able to prevent or suspend the continued operation of the blockchain. Public blockchains are very often fuelled by cryptocurrencies, the tokens of which are created as a result of the 'mining' of new blocks in order to incentivise 'miners' to operate the blockchain.

Private blockchains – Private blockchains are often described as closed blockchains. They may be run by a single entity or a group of entities. They are accessible only to a predetermined set of actors. Private blockchains are however not decentralised, so that the ('centralised') actors operating the blockchain may make decisions on the blockchain network. A private blockchain may incorporate cryptographic elements (i.e. security elements) but does not have the main characteristics of a (public) blockchain as decentralised

[435] Wulf A Kaal and Craig Calcaterra, 'Crypto Transaction Dispute Resolution' (2017) 73 The Business Lawyer 109.
[436] Michèle Finck, 'Blockchains: Regulating the Unknown' (2018) 19 German Law Journal 28, 669.
[437] Wright and De Filippi (n 433).
[438] Marcella Atzori, 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' (2017) 6 Journal of Governance and Regulation 45.
[439] Helen Eenmaa-Dimitrieva and Maria José Schmidt-Kessen, 'Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts' (2019) 35 Computer Law & Security Review 69, 71.
[440] See for instance ibid 72.

and distributed networks.[441] On the flip side, running a private blockchain enables one to have control over the data inserted on the ledger, and especially to conduct quality checks. Because the decision-making power lies with well-identified entities, the operation of a private blockchain may be suspended, terminated or rectified. In other words, a private blockchain is not 'immutable'. Private blockchains may but do not have to be based on cryptocurrencies.[442]

This categorisation as public or private does not exhaust qualification questions. The public v private nature of the blockchain networks should not be viewed as a block or white option, but rather as two extreme points of a great spectrum. The overall point is that the less the blockchain is permissionless and public, the less 'ambitious' it is from the perspective of decentralisation and distribution and therefore the less challenging it is for the legal analysis. It is therefore crucial to qualify the nature of the blockchain at stake before going into any legal analysis. Additionally, blockchain users should receive a fair information on the type of blockchain that they are dealing with. Managers of private blockchains could indeed easily 'hide' their responsibilities by alleging the use of (public) blockchain, thereby deceiving users.[443] With respect to TRUSTS, questions as for the governance of the blockchain are expected to be closely related to questions on the architecture of the TRUSTS data market ecosystem (who are the intermediaries? What do they do? Etc.).

9.1.3 Smart contracts

Another feature of the blockchain is often considered for data markets: smart contracts. Technically, smart contracts are computer messages comprised of "if x then y" statements where "y" executes automatically on a blockchain when "x" happens. Functionally, smart contracts can be designed to automate (part of) an agreement where automation refers to the computer-based execution without direct human intervention. Smart contracts may obviously perform other functions, with no legal significance. Contract automation is not something new. Most contracts concluded online are, at least partly, executed automatically online. Another famous example of contract automation is vending machines delivering cans or other goods in exchange for a coin. What is truly new smart contracts is the fact that they are executed on a blockchain. This entails that the automation is neither up to the parties nor up to a third party. Smart contracts are expected to enable parties to place their agreement in a smart contract (or in other words to code it and have the code run on a blockchain network) and entrust the "disinterested blockchain"[444] to execute it. The ground-breaking character of smart contracts is that both sides of the agreement's obligations can be subject to automation.[445] Because of the self-executing feature of the smart contract, parties can trust that

[441] ibid 73–74.
[442] Some authors would add to that "consortium blockchains". However, the definition of consortium blockchains is unclear and often overlaps to a great extent with this of private blockchains, see ibid 73. For further elaboration on the different types of blockchain networks and their respective pros and cons, see Spigolon and others (n 160).
[443] Charlotte Ducuing, 'How to Make Sure My Cryptokitties Are Here Forever? The Complementary Roles of Blockchain and the Law to Bring Trust' (2019) 10 European Journal of Risk Regulation 315.
[444] Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1 Georgetown Law Technology Review 37, 319.
[445] Guido Governatori and others, 'On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain Systems' [2018] Artificial Intelligence and Law 377.

their agreement will be executed as planned. It is therefore the blockchain technology which makes smart contracts specific.

Against this background, blockchain-based smart contracts ('smart contracts') are expected to automate data transactions in data market ecosystems. Smart contracts are expected to decrease transaction costs, such as litigation costs and risk of non-compliance and to increase efficiency in contracting.[446] More generally, smart contracts are expected to provide an "alternative mechanism of contract governance", namely alternative to this of the law.[447] This already gives an idea of the relationship between the blockchain and smart contracts on the one hand, and the law on the other. On the one hand, smart contracts are expected to substitute or complement legal tools (especially legal enforcement). On the other, participants expect that the data transactions be recognised by the law or in simpler terms that they will not 'have problems' with it.

9.1.4 What to expect from the blockchain?

The blockchain technology is particularly subject to political fantasies and ideologies. This may not only obscure scientific analysis but it may also lead to over-expectations of what the blockchain technology can deliver. A now famous example is the (often implicit) belief that the blockchain would be able to verify the accuracy of information placed on the blockchain. This misbelief can be seen i.e. in the law of Arizona, which defines blockchain technology as "distributed ledger technology that uses a distributed, decentralised, shared and replicated ledger". From that, the law derives that data stored on such blockchain would "provide an unensored truth".[448] As hightlined by Walch, "if a false piece of data is put on a blockchain ledger, it remains false, regardless of the fact that it appears on the ledger […]".[449] In the case of a data market, the fact that a catalogue of data 'for sale' would be placed on a blockchain would for instance provide no guarantee as for the accuracy or even nature of the data. Similarly, the blockchain cannot assess the professional quality of a given intermediary in the data market ecosystem.

Awareness of the limits of the blockchain capabilities is crucial so as to build the right ecosystem. The blockchain technology can be viewed as a building block, but cannot solve all the problems. Other technological tools need to be attached to the blockchain. Trusted intermediaries also have to play a role in the overall data market ecosystem, i.e. to verify the accuracy of the data placed on the platform or to identify and authenticate the platform users. Finally, the legal scholarship has made clear that the blockchain can certainly not substitute the law, the question being how they could complement each other.[450]

[446] Eenmaa-Dimitrieva and Schmidt-Kessen (n 439).
[447] ibid 70.
[448] Act of September 21 2006, ch 26, Ariz. Rev. Stat. Ann. § 44-7003 (2006) (amended by 2017 Ariz Sess Laws 2417).
[449] Angela Walch, 'Blockchain's Treacherous Vocabulary: One More Challenge for Regulators' (2017) 21 Journal of Internet Law 1,10, 10.
[450] On this, see Kevin Werbach, 'Trust, but Verify: Why the Blockchain Needs the Law' (2018) 33 Berkeley Technology Law Journal 487; Ducuing (n 443).

9.2 EU policies towards blockchain legal and regulatory framework

At the EU level, there are some blockchain-related policy initiatives rather than legal instruments. The most significant elements of the European Blockchain Strategy include: developing joint visions and initiatives through a European Blockchain Partnership launched in April 2018, increasing funding for blockchain innovation, supporting interoperability and standards and setting up European Union Blockchain Observatory and Forum in February 2018.[451] On 24 September 2020, the European Commission adopted also a comprehensive package of legislative proposals for the regulation of crypto-assets.[452] It also proposed to create a legal framework for Pan-European blockchain regulatory sandbox for using blockchains in the trading and post trading of securities. The sandbox is expected to become operational by 2021/22.[453] However, these legislative initiatives are expected not to have an influence on the use of the blockchain technology in TRUSTS, which does not directly concern crypto-assets. In the public sphere, the European Blockchain Services Infrastructure (EBSI), a joint initiative from the European Commission and the European Blockchain Partnership (EBP) will be deployed in 2021 to deliver EU-wide cross-border public services using blockchain technology. [454]

The full realisation of blockchain potential is, however hindered by a lack of harmonisation and interoperability.[455] The absence of a harmonised legal regime at EU level may lead to legal fragmentation, as some Member States have also enacted legislative provisions dedicated to the blockchain technology, and more specifically to *specific applications* thereof. Following two studies commissioned by the Government and the Parliament, France adopted, as part of the so-called 'PACTE' Act,[456] a provision specifically dedicated to creating a legal framework for 'Initial Coin Offerings' (ICOs). France also revised its Tax Code in order to clarify the taxation (the sale of) cryptoassets.[457] Another example is Italy, where the law no.12/19[458] recognises the same legal effect to the storage of computerised document based on distributed ledger technologies as "electronic time stamp" (as defined in the eIDAS Regulation).

[451] Available at: https://ec.europa.eu/digital-single-market/en/news/european-blockchain-strategy-brochure
[452] See more at: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en
[453] ibid.
[454] See more at: https://ec.europa.eu/digital-single-market/en/european-blockchain-services-infrastructure
[455] See also CEN-CENELEC White Paper 'Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies' available at: https://www.cencenelec.eu/news/brief_news/Pages/TN-2018-085.aspx (last visited 13 October 2020).
[456] LOI n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises.
[457] Nicolas Boring, 'Regulatory Approaches to Cryptoassets' (April 2019) <https://www.loc.gov/law/help/cryptoassets/france.php> accessed 13 October 2020.
[458] Law n° 12.19, available here: http://www.senato.it/leg/18/BGT/Schede/Ddliter/51070.htm (last visited 13th October 2020).

9.3 Overview of legal issues related to blockchain technology

In lack of a blockchain-specific regulation at the EU level, there is a number of points of attention in relation to blockchain, which have to be analysed against *lex generalis* legal frameworks. The remainder of this section provides a non-exhaustive list of such points. Questions arising specifically from the use of smart contracts are not included in this section, as they are dealt with in task 3.2. Legal issues related to cryptocurrencies and ICOs are also not included in this section, because they relate to very specific applications of the blockchain technology, unrelated to the TRUSTS research project.

9.3.1 Responsibility for legal compliance and liability

Decentralised digital environments are tricky from a legal perspective. As there is no one who 'owns' a blockchain, it is equally difficult to determine who is 'responsible' for it. This question runs through all legal frameworks. Who is liable to comply with the said legal obligations, in such a decentralised and distributed environment?

Finck points out that in decentralized blockchain-based applications it is more burdensome to share responsibility than in centralized regimes.[459] One of the main difficulties lies with the fact that when it comes to blockchain regulatory access points are harder to define.[460] Should Internet Service Providers ('ISPs') become focal points of blockchain regulation? Finck explains that "when governments wish to prevent their citizens from using blockchains or specific blockchain-based applications, they could order ISPs to block encrypted data that passes through their network or prevent ISPs from transmitting data to and from decentralized applications".[461] Or should it be miners, the nodes in the network that add new data to a blockchain? Core Software Developers have an equally key role as they "are not just software architects but also policy-makers shaping the world we live in."[462] Finally, end users, although (pseudo)anonymised, could however be identified for law enforcement purposes. Should they be the one responsible for legal compliance of blockchain? Last but not least, online intermediaries are attractive regulatory access points.[463]

As the European Commission 'Study on Blockchains Legal, governance and interoperability aspects (SMART 2018/0038)'[464] points out, the degree of difficulty differs depending on whether the blockchain in

[459] Michèle Finck, 'Blockchains as a Regulatable Technology' (*Blockchain Regulation and Governance in Europe*, December 2018) </core/books/blockchain-regulation-and-governance-in-europe/blockchains-as-a-regulatable-technology/D4102531C0FC1821B45D6E7E231BE07E/core-reader> accessed 13 October 2020.46.
[460] ibid.
[461] ibid.
[462] ibid.
[463] ibid.
[464] European Commission DG Communications Networks, Content & Technology, 'Study on Blockchains: Legal, Governance and Interoperability Aspects.' (Publications Office 2020) <https://data.europa.eu/doi/10.2759/4240> accessed 14 October 2020.

question is permissioned (private) or permissionless (public). [465] The later, as discussed above, are not governed by a single legal entity accessed and may be used by anyone, without restriction.

In all likelihood, managers of private blockchains should be held responsible for 'their' blockchain and should not be deemed to escape such responsibility and liability behind false allegations over the governance regime of the blockchain (e.g. pretending to deal with public blockchains).

These considerations raise problems in relation to liability. It is unclear who, to whom, for what and based on what liability standard (negligence, strict liability etc.) is liable for compliance in contexts of decentralised blockchain.

9.3.2 Potential tensions with data protection rules

Just like for the responsibility for legal compliance and liability, the questions mostly arise from the use of public blockchains.

There are many of the points of tension between blockchain and the GDPR. First, in blockchain it is difficult to identify data (joint) controllers and processors as defined under the GDPR. As a result, it is equally difficult to enforce their obligations. Second, there is much debate whether data on blockchain is pseudo- or fully- anonymized and therefore whether the personal data placed on the blockchain, and subject to such safeguards, should still qualify as personal data or not Third, blockchains can make it difficult for data subjects to exercise some of their rights, most notably the "right to be forgotten".

9.3.3 Blockchain and law evasion - The protection of fundamental legal principles and mandatory rules

Blockchain can be used to infringe fundamental legal principles or mandatory rules (such as the prohibition of child abuse materials or of money laundering, etc.). Due to the fact that data on blockchain cannot easily be changed, it can be difficult to remove related content from the database.[466] Moreover, a pseudonymous nature of blockchain (and, in some cases, a full anonymity) makes it more burdensome to track down the identity of the specific individuals responsible for infringements. Because of its decentralised and distributed nature, a (especially, public) blockchain raises also jurisdictional issues, which add to the law enforcement challenges.

9.3.4 Tension between blockchain reality and legal reality

As put by the European Union Blockchain Observatory Study, 'Legal and regulatory framework of blockchains and smart contracts', "just because we can prove mathematically that transactions on a blockchain are valid, know who "owns" the data saved in a blockchain based ledger and demonstrate that

[465] ibid.

[466] European Commission DG Communications Networks, Content & Technology (n 33) 54.

that data has not been tampered with, does not however mean that blockchain-based transactions or registration of ownership is by itself legally binding."[467]

To recognize the legal status of blockchain transactions, one would need to analyse the eIDAS Regulation[468] with regard to the recognition of blockchain-based signatures, timestamps and validations, but also property law and contract law provisions laid down in the national law of the respective member States. As indicated by the European Commission 'Study on Blockchains Legal, governance and interoperability aspects', the problem raises when ownership of digital or real-world assets changes but this is not reflected on blockchain.[469] In such a case the tension arises because data is not up to date or does not correspond to legal reality.[470]

9.3.5 Risk to fair competition

The blockchain technology was also found to disrupt competition law. Schrepel considers that the decentralisation, anonymity and immutability that characterise a public blockchain challenge the "ability to detect anticompetitive practices and their perpetrators". They are also likely to hinder the effects of competition law remedies. Schrepel goes as far as to suggest that some changes to competition law are required to tackle these issues.[471]

In any case, blockchain is context-specific, and further research will be needed to determine its applicability to TRUSTS as well as the specific legal aspects thereof.

[467] The European Union Blockchain Observatory & Forum 'Legal and Regulatory Framework of Blockchains and Smart Contracts' <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> accessed 14 October 2020.
[468] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.
[469] European Commission DG Communications Networks, Content & Technology (n 33) 54.
[470] The relationship between blockchain and property law is discussed in more details in Ducuing (n 159).
[471] Thibault Schrepel, 'Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox' (2019) 3 Georgetown Law Technology Review 281, 285.

10 Ethical challenges in data sharing

The concept of "data ethics" used by ethicists Floridi and Taddeo describes "ethical problems posed by the collection and analysis of large dataset".[472] Such ethical problems range from risks of reidentification of individuals, re-using of large datasets and data-driven discrimination (e.g. ageism, ethnicism, sexism).[473] Trust and transparency are equally important topics in the ethics of data. Regardless of a size of a dataset, the extensive use of data of various types (personal, sensitive, big data) also raises questions of fairness, responsibility, accountability and bias. The successful use of supervised and unsupervised artificial intelligence (AI) and machine learning (ML) depends on access to (big) data as necessary inputs for training algorithms.[474] As put by Hand, "the ubiquity of the impact of data technologies on all aspects of modern life means that those concerned with data and their use must engage with the ethical issues".[475] He then lists various characteristics of modern data and the use of such data which require careful consideration of ethical issues: (i) the pervasiveness of data technology; (ii) the interconnectedness of data; (iii) the dynamic nature of data; (iv) real-time online analysis and decision-making; (v) synergistic analysis through merging and combination of data sets; (vi) lack of space, time, and social context limitation on scope of data; (vii) ability to use for unexpected purposes and to reveal unexpected information; (viii) risk of exceptional intrusiveness since it is impossible to avoid having data about individuals stored in multiple databases; (ix) potential for misuse, privacy breach, blackmail, and other crimes; (x) ownership issues.[476]

Misusing data and overlooking ethical data sharing principles may lead to negative social consequences and public outcry (e.g. the 'Cambridge Analytica' leak). On the other hand, there are many positive outcomes of data sharing. Ethical data sharing is therefore a balancing exercise. As the European Commission President Ursula von der Leyen explains, in order to fully release the potential of data "we have to find our European way, balancing the flow and wide use of data while preserving high privacy, security, safety and ethical standards".[477]

Finally, there is a lively debate concerning bias, discrimination, and fairness in AI and machine learning. AI-driven decision-making can lead to discrimination in several ways. An algorithm can contribute to discriminatory decision making if it uses biased data or can discriminate against specific subgroups for whom representative data is not available. A use of artificial intelligence in human-computer interaction (HCI) may affect consumers psychological wellbeing.[478]

[472] Luciano Floridi and Mariarosaria Taddeo, 'What Is Data Ethics?' (2016) 374 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20160360.
[473] ibid. 3.
[474] Bertin Martens, 'The Impact of Data Access Regimes on Artificial Intelligence and Machine Learning' (JRC Digital Economy Working Paper 2018).
[475] David J Hand, 'Aspects of Data Ethics in a Changing World: Where Are We Now?' (2018) 6 Big Data 176.
[476] ibid. 178.
[477] President of the European Commission Ursula von der Leyen, 'A Union that strives for more: My agenda for Europe', available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf (last visited 12 October 2020).
[478] Gary M Olson and Judith S Olson, 'Human-Computer Interaction: Psychological Aspects of the Human Use of Computing' (2003) 54 Annual Review of Psychology 491.

This section begins with the ethics requirements for Trustworthy AI as defined by the High-Level Expert Group (HLEG). The second subsection elaborates on data-driven discrimination and data bias.

10.1 Ethics requirements for Trustworthy AI

On 8 of April 2019, the EU's High-Level Expert Group (HLEG), a multi-stakeholder group of fifty-two experts, published the "Ethics Guidelines for Trustworthy AI".[479] The Guidelines are not legally binding. They do, however, pave the way for the future "AI regulation". The stakeholders are moreover encouraged to voluntarily opt to use these Guidelines. In order to help operationalise the ethical requirements HLEG has also published the "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment"[480] and an on-line tool.[481]

The Guidelines are centred around the concept of "trustworthy AI". Trustworthiness is defined "a prerequisite for people and societies to develop, deploy and use AI systems".[482] Without AI systems being trustworthy, unwanted consequences may arise and prevent the realisation of the social and economic benefits of AI.

According to the Guidelines, the three pillars of trustworthy AI are:

i. Lawfulness – compliance with all applicable laws and regulations; those include: EU primary law (the Treaties of the European Union and its Charter of Fundamental Rights), EU secondary law (such as the General Data Protection Regulation, the Product Liability Directive, the Regulation on the Free Flow of Non-Personal Data, anti-discrimination Directives, consumer law and Safety and Health at Work Directives), the UN Human Rights treaties and the Council of Europe conventions (such as the European Convention on Human Rights), and EU Member State laws. Various sector-specific rules that apply to particular AI applications should also be taken into consideration.

ii. Ethics – respect for ethical principles and values; and

iii. Robustness - both from a technical and social perspective individuals and society must also be confident that AI systems will not cause any unintentional harm. AI should perform in a safe, secure and reliable manner, and safeguards prevent any unintended adverse impacts of AI applications should be put in place.[483]

[479] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019).
[480] High-Level Expert Group on AI, 'Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment' (European Commission 2019)'.
[481] Available at : https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence.
[482] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) (n 8) 4.
[483] ibid. 7.

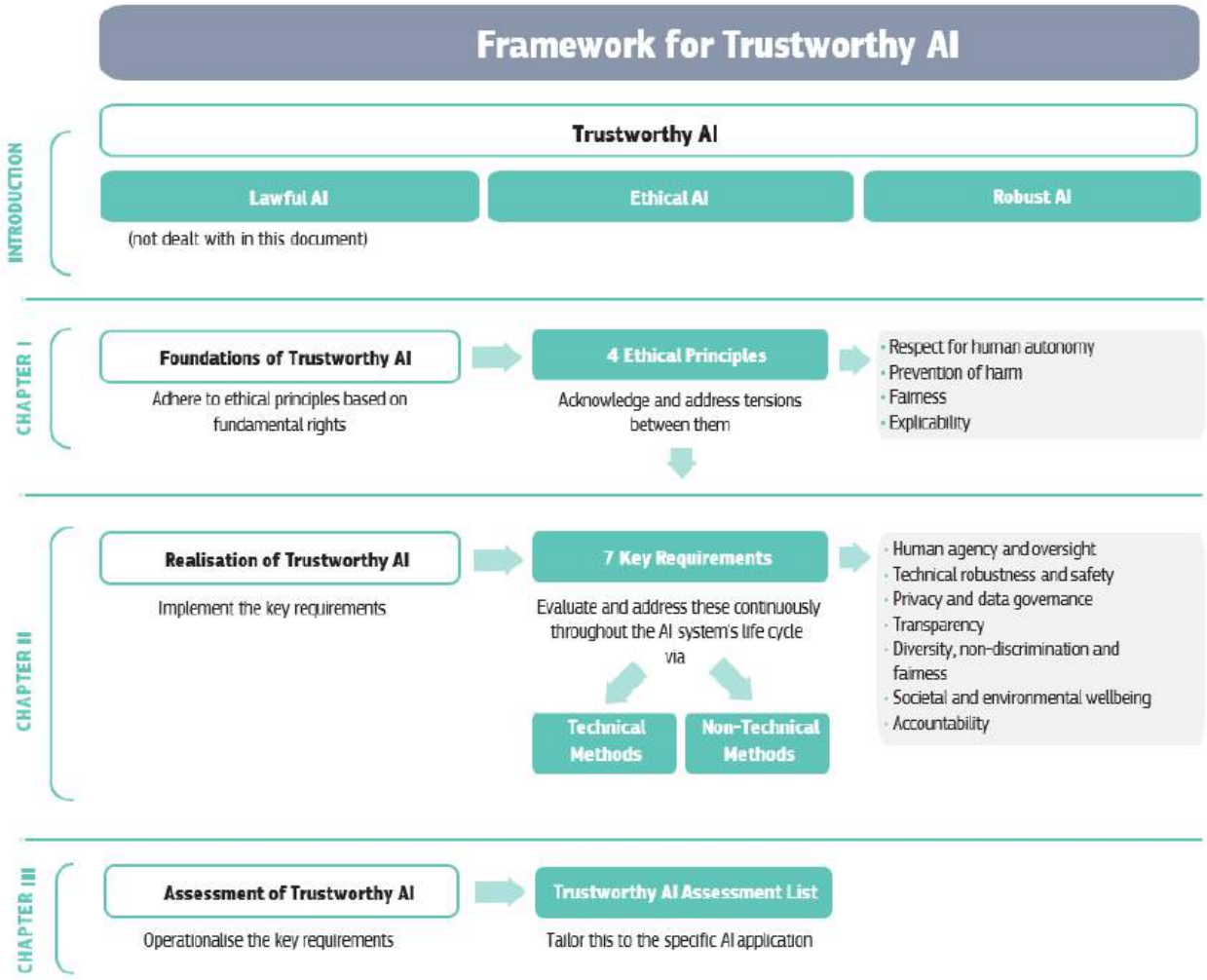

Figure 3: Framework for Trustworthy AI.[484]

According to the HLEG, the foundations of Trustworthy AI are the fundamental rights enshrined in the EU Treaties, the EU Charter and international human rights law:

i. Respect for human dignity which should never be diminished, compromised or repressed by others – nor by new technologies like AI systems;[485]
ii. Freedom of the individual, including freedom from (in)direct illegitimate coercion, unjustified surveillance, deception and unfair manipulation;
iii. Respect for democracy, justice and the rule of law. In particular, AI systems must not undermine democratic processes, human deliberation or democratic voting systems.[486]

[484] ibid. 8
[485] ibid. 10.
[486] ibid. 11.

iv. Equality, non-discrimination and solidarity - including the rights of persons at risk of exclusion. AI systems should generate unfairly biased outputs, meaning that the data used to train AI systems should be as inclusive as possible, representing different population groups.[487]

v. Citizens' rights. In particular AI systems should not negatively impact citizens' rights, including the right to vote.

Importantly, many of these rights are, to some extent, legally enforceable in the EU so that compliance with their terms is legally obligatory. Besides legally enforceable rules, ethical guidelines can help to "identify what we should do rather than what we (currently) can do with technology".[488] This is why the HLEG proposes the following four ethical principles ("imperatives") "which must be respected in order to ensure that AI systems are developed, deployed and used in a trustworthy manner"[489]: (i) the principle of respect for human autonomy; (ii) the principle of prevention of harm; (iii) fairness; (iv) the principle of explicability.

The HLEG notes that "tensions may arise between the above principles, for which there is no fixed solution".[490] Using machine learning and big data improves the quality of various services to the benefit of citizens, but requires large amounts of personal data, raising concerns about privacy and especially meaningful consent. Use of AI systems for "predictive policing" may help to reduce crime, but it often entails surveillance activities. Some authors[491] suggest that the next steps for AI ethics should indeed focus on bridging the gap between different sets of principles, acknowledge differences in values and identify ambiguities and knowledge gaps. The Guidelines propose that AI practitioners approach these ethical dilemmas and trade-offs 'via reasoned, evidence-based reflection'.[492]

In chapter II of the guidelines, the abovementioned principles are translated into a list of seven requirements to achieve Trustworthy AI:

i. Human agency and oversight

AI systems should support human autonomy and decision-making, as prescribed by the principle of respect for human autonomy. On the notion of autonomy, the following characteristics for a conceptualization of autonomy of AI systems have been developed. Human autonomy within technology systems requires:

- "A feeling of willingness, volition and endorsement;
- The lack of pressure, compulsion or feeling controlled;

[487] ibid. 11.
[488] ibid. 10.
[489] ibid. 11.
[490] ibid. 13.
[491] Jess Whittlestone and others, 'The Role and Limits of Principles in AI Ethics: Towards a Focus on Tensions', *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (ACM 2019) <https://dl.acm.org/doi/10.1145/3306618.3314289> accessed 12 October 2020.
[492] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) (n 8) 13.

- The lack of deception or deliberate misinformation".493

The Guidelines point out that when there is a risk that the AI system may negatively affect fundamental rights, an impact assessment should be undertaken. This should be done prior to the system's development. Users should also be able to make informed autonomous decisions regarding AI systems and have the knowledge and tools to understand and interact with AI systems. A central place of users in the AI system's functionality means that it must respect users' right not to be subject to a decision based solely on automated processing when this produces legal effects on users or similarly significantly affects them.[494]

As regards the human-to-computer interactions (HCI) the assessment list offers a series of questions that may be asked to make sure that human perception is not deceived when confronted with AI systems that "act" like humans. Such questions include: "Could the AI system generate confusion for some or all end-users or subjects on whether they are interacting with a human or AI system? Are end-users or subjects informed that they are interacting with an AI system? Does the AI system risk creating human attachment, stimulating addictive behaviour, or manipulating user behaviour?"[495]

Finally, human oversight may be achieved through governance mechanisms such as a human-in-the-loop (HITL), human-on-the-loop (HOTL), or human-in-command (HIC) approach. HITL refers to the capability for human intervention in every decision cycle of the system. Such approach is however neither possible nor desirable.[496] HOTL refers to the capability for human intervention during the design cycle of the system and monitoring the system's operation. HIC refers to the capability to oversee the overall activity of the AI system and the ability to decide when and how to use the system in any particular situation.[497]

ii. Technical robustness and safety

This requirement deals with four main issues: 1) security; 2) safety; 3) accuracy; and 4) reliability, fall-back plans and reproducibility.

Technical robustness, closely linked to the principle of prevention of harm requires that AI systems are developed with a preventative approach to risks. They should behave reliably while minimising unintentional and unexpected harm, and preventing unacceptable harm. For AI systems to be considered secure, possible unintended applications of the AI system (e.g. dual-use applications) and potential abuse of the system by malicious actors such as data-targeted attacks (data poisoning), model-targeted attacks (model leakage) or software and hardware attacks should be taken into account. The steps should be taken to prevent and mitigate these risks. [498]

[493] Rafael A Calvo and others, 'Supporting Human Autonomy in AI Systems: A Framework for Ethical Enquiry' in Christopher Burr and Luciano Floridi (eds), *Ethics of Digital Well-Being: A Multidisciplinary Approach* (Springer International Publishing 2020) <https://doi.org/10.1007/978-3-030-50585-1_2> accessed 12 October 2020.
[494] See also GDPR, Art. 22.
[495] High-Level Expert Group on AI (n 9) 7.
[496] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) (n 8) 16.
[497] ibid.
[498] ibid.

AI systems should also have safeguards that enable a fallback plan. It must be ensured that the system will do what it is supposed to do without harming humans or the environment.

Accuracy pertains to an AI system's ability to make correct judgements, predictions, recommendations, or decisions based on data or models. It is important that the system can indicate how likely these errors are.

Reliability requires to scrutinise an AI system and to prevent unintended harms. Reproducibility describes whether an AI experiment exhibits the same behaviour when repeated under the same conditions. The self-assessment list suggests that AI developers should ask themselves the following questions: "Did you put in place a well-defined process to monitor if the AI system is meeting the intended goals? Did you put in place verification and validation methods and documentation (e.g. logging) to evaluate and ensure different aspects of the AI system's reliability and reproducibility? Did you put in place a proper procedure for handling the cases where the AI system yields results with a low confidence score?"[499]

iii. Privacy and data governance

AI systems must guarantee privacy and data protection throughout a system's entire lifecycle. This includes both the information provided by the user, and the information generated about the user over the course of their interaction with the system (e.g. outputs that the AI system generated for specific users or how users responded to particular recommendations).[500] It must also be ensured users' data will not be used to unlawfully or unfairly discriminate against them. Quality and integrity of data must be ensured. Finally, organisation that handles individuals' data should make data protocols governing data access accessible.

To adhere to data protection legislation, one may ask himself if the AI system is trained, or was developed, by using or processing personal data (including special categories of personal data). If so, mandatory GDPR measures must be put in place, such as: perform a Data Protection Impact Assessment, designate a Data Protection Office, comply with privacy-by-design and default measures e.g. encryption, pseudonymisation, aggregation, anonymisation; adhere to data minimisation principle, in particular with regard to the special categories of personal data etc.[501]

iv. Transparency

The guidelines propose the three-fold approach to transparency. First, traceability means that datasets and processes that lead to the AI system's decision should be documented to the best possible standard. AI developers should be able to trace back which data, models and rules were used by the AI system to make a certain decisions or recommendations.

Second, explainability concerns the ability to explain both the technical processes of an AI system and the related human decisions. "Whenever an AI system has a significant impact on people's lives, it should be possible to demand a suitable explanation of the AI system's decision-making process".[502]

[499] High-Level Expert Group on AI (n 9) 11.
[500] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) (n 8) 17.
[501] High-Level Expert Group on AI (n 9) 13.
[502] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) (n 8) 16.

Renda finds the principle of explicability of AI systems "perhaps the most controversial imperative".[503] He argues that in certain circumstances "invoking the full explicability of AI systems and decisions could jeopardize the use of AI techniques". To this end, the HLEG clarified that "the degree to which explicability is needed is highly dependent on the context and the severity of the consequences if that output is erroneous or otherwise inaccurate".[504]

Third, humans should be informed that they are interacting with an AI system. They should also have the option to have a human interaction instead.

v. Diversity, non-discrimination and fairness

Biased data could lead to unintended (in)direct prejudice and discrimination against certain groups or people, potentially exacerbating prejudice and marginalisation. Discrimination and data bias will be further discussed in Section 10.2 below.

The concept of 'fairness' is in particular highly-debated one. The notion of 'fairness' refers to the various concepts, such as "the need for equal and just distribution of both benefits and costs; providing equal opportunity; protecting individuals' freedom of choice; respecting the principle of proportionality as well as offering the possibility for effective redress against decisions made by AI systems and by the humans operating them".[505] Moreover, the research is done on statistical measures of fairness among the data science and machine learning specialists.

Accessibility and universal design[506] mean that AI systems should be user-centric and designed in a way that allows all people to use AI products or services, regardless of their age, gender, or abilities. Finally, the Guidelines highlight the importance of stakeholder participation throughout the whole process of implementing AI systems.

vi. Societal and environmental well-being

The Guidelines encourage sustainability and ecological responsibility of AI systems and the environmental friendliness. The societal impact, such as its effect on institutions, democracy, society and individuals' well-being should be given careful consideration.

vii. Accountability

The requirement of accountability "necessitates that mechanisms be put in place to ensure responsibility and accountability for AI systems and their outcomes, both before and after their development, deployment and use."[507] The requirement of accountability also includes auditability

[503] Andrea Renda, 'Europe: Toward a Policy Framework for Trustworthy AI' in Markus D Dubber, Frank Pasquale and Sunit Das (eds), Andrea Renda, *The Oxford Handbook of Ethics of AI* (Oxford University Press 2020) <https://oxfordhandbooks.com/view/10.1093/oxfordhb/9780190067397.001.0001/oxfordhb-9780190067397-e-41> accessed 12 October 2020.
[504] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) (n 8) 13.
[505] Renda (n 31) 656.
[506] Terms such as "Design for All", "Universal Design", "accessible design", "barrier-free design", "inclusive design" and "transgenerational design" are often used interchangeably with the same meaning.
[507] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) (n 8) 19.

(the enablement of the assessment of algorithms, data and design processes through e.g. evaluation reports) and the use of impact assessments (e.g. red teaming or forms of Algorithmic Impact Assessment) proportionate to the risk that the AI systems pose. Trade-offs should be explicitly acknowledged and evaluated in terms of their risk to ethical principles, including fundamental rights. When unjust adverse impact occurs, accessible mechanisms should be foreseen that ensure adequate redress.[508]

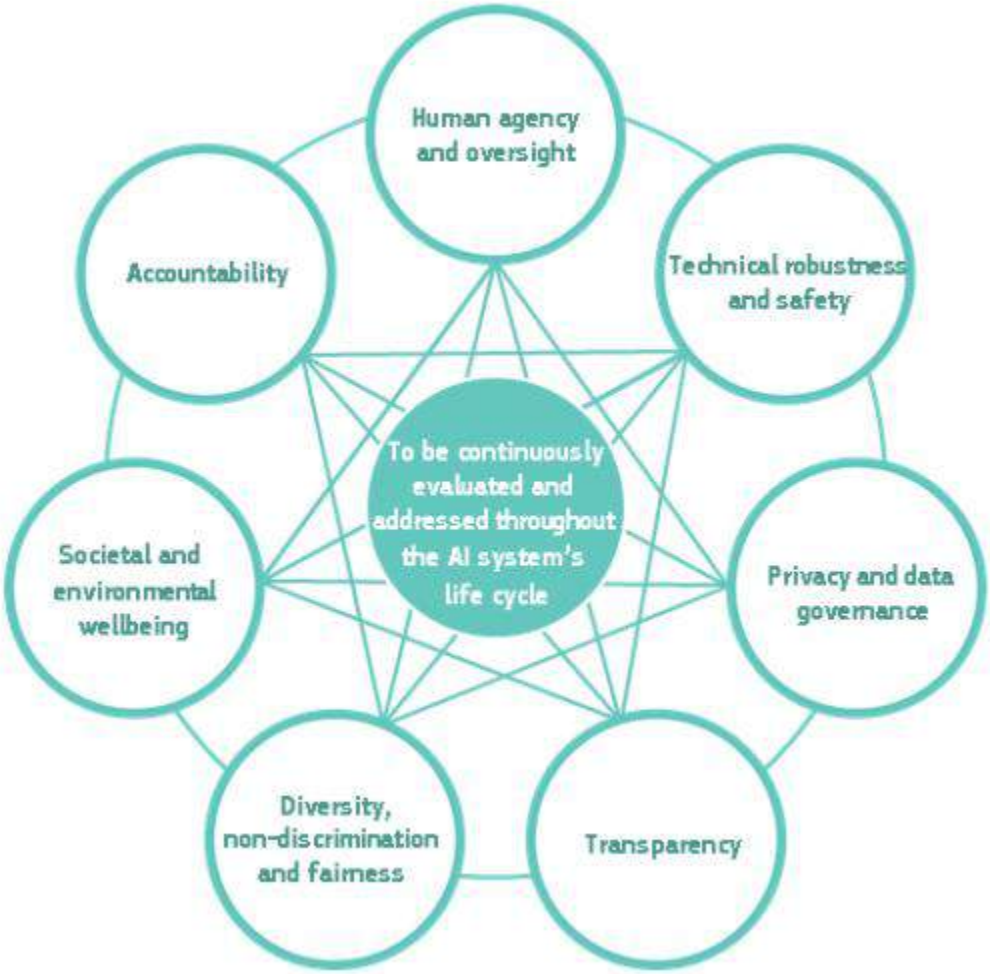

Figure 4: Interrelationship of the seven requirements: all are of equal importance, support each other, and should be implemented and evaluated throughout the AI system's lifecycle. [509]

[508] ibid. 19.
[509] ibid. 15.

The Guidelines point out that the realisation of Trustworthy AI is not a one-off exercise but a continuous process. Any changes to the implementation processes should occur on an ongoing basis. The Guidelines then lists a series of technical[510] and non-technical[511] methods to ensure Trustworthy AI.

[510] These include: Architectures for Trustworthy AI, Ethics and rule of law by design (X-by-design), Explanation methods, Testing and validating, Quality of Service Indicators.

[511] Such as Regulation, Codes of conduct, Standardisation, Certification, Accountability via governance frameworks, Education and awareness to foster an ethical mind-set, Stakeholder participation and social dialogue, Diversity and inclusive design teams.

10.2 Data-driven discrimination and data bias

According to the online Oxford English Dictionary, the term 'discrimination' is defined as “treating one or more members of a specified group unfairly as compared with other people. Discrimination may be illegal on the ground of sex, sexual orientation, race, religion, disability, or nationality”.[512]

European non-discrimination law exists in both primary and secondary law. The principle of non-discrimination is enshrined in the Charter of Fundamental Rights of the European Union (EU).[513] Article 21 of the Charter establishes that “[a]ny discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.” Under EU secondary legislation, there are the four main non-discrimination directives: the Racial Equality Directive (2000/43/EC)[514], the Gender Equality Directive (2006/54/EC)[515], the Gender Access Directive (2004/113/EC)[516], and the Employment Directive (2000/78/EC).[517] The Directives establish a minimal standard which needs to be transposed into national law by the Member States.

Wachter points out that to bring a case alleging direct or indirect discrimination under EU non-discrimination law, one must demonstrate that: “(1) a particular harm has occurred or is likely to occur; (2) the harm manifests or is likely to manifest significantly within a protected group of people; and (3) the harm is disproportionate when compared with others in a similar situation”.[518]

When data and algorithms are used for decision making purposes, there is potential for discrimination against individuals. The Council of Europe “Study on discrimination, artificial intelligence and algorithmic decision-making” points out that AI systems are often "black boxes". It is often unclear why a system makes a certain decision. Because of the opaqueness of such decisions, it is difficult for people to assess whether they were discriminated against.[519]

[512] See the online Oxford dictionary, https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095721450#:~:text=Treating%20one%20or%20more%20members,A%20Dictionary%20of%20Law%20Enforcement%20%C2%BB (last visited 12 October 2020).
[513] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407, Art. 21.
[514] Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180, 19.7.2000, p. 22–26.
[515] Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation, OJ L 204, 26.7.2006, p. 23–36.
[516] Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services, OJ L 373, 21.12.2004, p. 37–43.
[517] Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, OJ L 303, 2.12.2000, p. 16–22.
[518] Sandra Wachter, Brent Mittelstadt and Chris Russell, ‘Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI’ [2020] SSRN Electronic Journal 15.
[519] Council of Europe, Directorate General of Democracy, ‘Discrimination, Artificial Intelligence, and Algorithmic Decision-Making’ (2018).

AI-driven decision-making can lead to discrimination in several ways. Barocas and Selbst[520] offer the following taxonomy of AI-driven discrimination:

i. Discrimination based on how the "target variable" and the "class labels" are defined;

In machine learning, the algorithm "learns" which attributes or activities (previously identified as fraud, spam, etc.) can serve as potential proxies for those qualities or outcomes of interest. Such an outcome of interest is called a "target variable".[521] "Class labels" divide all possible values of the target variable into mutually exclusive categories".[522] Importantly, "insofar the data scientist needs to translate a problem into formal computer coding, deciding on the target variable and the class labels is a subjective process".[523] The discrimination may take place depending on how an organisation defines the target variables and class labels.

ii. Discrimination based on labelling and collection of the training data;

AI decision-making can also have discriminatory results if the system uses biased training data. If data is poorly labelled, inaccurate, incomplete or if it reflects human prejudices, then the AI model will reproduce those same biases.

iii. Discrimination based on feature selection;

By selecting only certain features that an AI system uses for prediction, the organisation might introduce bias against certain groups.

iv. Proxy discrimination;

The so-called indirect discrimination concerns "an apparently neutral practice or policy which puts persons belonging to a protected group at a particular disadvantage".[524] Indirect discrimination does not focus on a particular individual but rather deals with rules or patterns of behavior. It may be fair in form, but discriminatory in outcome. In machine learning contexts, indirect discrimination is considered the most relevant type of discrimination.[525]

The Council of Europe study gives the example of a bank using AI system trained on 20-years old data to predict which loan applicants will have problems repaying the loan. The training data do not however, contain information about protected characteristics such as skin colour. The AI system learns that people

[520] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' [2016] SSRN Electronic Journal <https://www.ssrn.com/abstract=2477899> accessed 12 October 2020.
[521] ibid. 678.
[522] ibid.
[523] Maddalena Favaretto, Eva De Clercq and Bernice Simone Elger, 'Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review' (2019) 6 Journal of Big Data 12.
[524] Tarunabh Khaitan, *The Architecture of Discrimination Law* (Oxford University Press) <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199656967.001.0001/acprof-9780199656967-chapter-3> accessed 12 October 2020, 69.
[525] Philipp Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law' (2018) 55 Common Market Law Review <https://kluwerlawonline.com/JournalArticle/Common+Market+Law+Review/55.4/COLA2018095> accessed 14 October 2020 11.

from a particular postal code were likely to default on their loans. The correlation is made to predict defaulting in repaying the loans. However, one may suppose that the postcode correlates with racial origin. In that case, the prediction made by a bank based on *prima facie* neutral characteristic (a postcode), would discriminate against people from a certain racial origin.[526]

v. Intentional discrimination.

This so-called direct discrimination entails unfavourable or less favourable treatment 'on the ground of' or 'because of' a protected characteristic (such as race, sex, gender, religion) or, sometimes, a combination of such characteristics (intersectional discrimination).[527]

According to all of EU anti-discrimination directives "direct discrimination shall be taken to occur where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of (…)".[528] Importantly, the focus in direct discrimination is on the individual. As Hacker points out this is "certainly the easiest, and most blatant, case of algorithmic discrimination"[529] and "in machine learning contexts, direct discrimination will be rather rare."[530]

The European Union Agency for Fundamental Rights Study "#BigData: Discrimination in data-supported decision making"[531] offers the following solutions towards fundamental rights compliance in the development and use of data-driven AI:

i. Being as transparent as possible about how algorithms are built and used;
ii. Conducting fundamental rights impact assessments which include among others, an assessment of the potential for discrimination in relation to different grounds – such as gender, age, ethnic origin, religion and sexual or political orientation;
iii. Checking the quality of data;
iv. Making sure the way the algorithm was built and operates may be meaningfully explained.

As has been said above, discrimination may also be based on the choice of data used which might not be neutral. Bias generally refers to a strong predisposition, prejudgment or a preconceived opinion about something or someone. The HLEG Assessment List for Trustworthy Artificial Intelligence defines AI (or algorithmic) bias as: "systematic and repeatable errors in a computer system that create unfair outcomes, such as favouring one arbitrary group of users over others".[532] Bias can take place because of many factors, "including but not limited to the design of the algorithm or the unintended or unanticipated use or decisions relating to the way data is coded, collected, selected or used to train the algorithm".[533] Interestingly, it may be argued that every AI system has some inherent bias as it merely mirrors a real-world situation and subjective choices of those who select, collect and prepare data.

[526] Council of Europe, Directorate General of Democracy (n 47) 13.
[527] Khaitan (n 52) 73.
[528] Race Equality Directive 2000/43/EC, Art. 2(2)(a).
[529] Hacker (n 54) 9.
[530] Hacker (n 525).
[531] Council of Europe, Directorate General of Democracy (n 47) 14.
[532] High-Level Expert Group on AI (n 9) 23.
[533] ibid.

The European Union Agency for Fundamental Rights Study 'Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights' points out that "data quality for building algorithms and AI-related technologies is one of the concerns for the fundamental rights compliant use of data".[534] Algorithms used in machine learning systems and artificial intelligence (AI) can only be as good as the data on which they learn. In statistics, this is often referred to as 'garbage in, garbage out' principle, namely low-quality data lead to low quality outcomes. That can produce algorithmic results which are biased, discriminatory and "which in turn can lead to a violation of fundamental rights".[535] Council of Europe Report sums up that "data quality checks and the appropriate documentation of data and meta-data is essential for high quality data analysis and the use of algorithms for decision making."[536]

10.3 Conclusion - Relevance for TRUSTS

In this chapter we have offered a high-level analysis of ethical issues in data sharing with the use of AI-driven tools. For further analyses of the possible implications of data sharing within the TRUSTS platform we refer to our Deliverable 9.

[534] European Union Agency for Fundamental Rights, 'Data Quality and Artificial Intelligence – Mitigating Bias and Error to Protect Fundamental Rights' (2019) 2.
[535] ibid.
[536] Council of Europe, Directorate General of Democracy (n 47) 14.

11 Conclusions and Next Actions

This deliverable provides an overview of the legal frameworks and ethical principles that may be applicable to a data market ecosystems such as TRUSTS. By doing so, the aim is mainly to provide guidance for partners in the research project to elaborate the business and technical aspects of TRUSTS.

This deliverable will be followed by continued interactions with partners for the elaboration of the TRUSTS ecosystem, as part of WP6. Where needed, more targeted legal aspects will be taken further, based on the concrete elaboration of the TRUSTS ecosystem. In order to provide both targeted guidance to partners and to be able to draw legal and regulatory conclusions from the interdisciplinary research in TRUSTS, WP6 will further the work in tasks 6.1, 6.3 and 6.4.

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