Grant Agreement Number: 825225

Safe-DEED

www.safe-deed.eu

D3.7 - Trust in Data Markets v2

Deliverable number	*D3.7*
Dissemination level	***Public***
Delivery date	*November 2021*
Status	*Final*
Author(s)	*Dieter Decraene, Alessandro Bruni, Noémie Krack, Peggy Valcke, Emre Bayamlıoğlu*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825225.

Changes Summary

Date	Author	Summary	Version
21 May 2021	Dieter Decraene	First draft	0.1
21 September 2021	Dieter Decraene	First draft (updated with survey findings)	0.2
30 September 2021	Alessandro Bruni	First review	0.3
19 October 2021	Dieter Decraene	Second draft	0.4
30 October 2021	Dieter Decraene	Second draft (updated with semi-structured interview findings)	0.5
05 November 2021	Alessandro Bruni	Second review	0.6
07 November 2021	Yiannis Markopoulos	Third review	0.7
09 November 2021	Wirawan Agahari	Fourth review	0.8
15 November 2021	Peggy Valcke	Fifth review	0.9
17 November 2021	Dieter Decraene	Final version	1.0

Abstract

Deliverable 3.7 (D3.7), complementing the analysis on the notion of trust started in D3.6 "Trust in Data Markets v1.0"[1], aims to assess the concept of organizational trust. In doing so, the deliverable focuses on the role and the economic perspective of trust in the EU Digital Single Market.

In particular, this research scrutinizes trust in data marketplaces (i.e. "digital trust"), the role of trust within the European Digital Strategy, and the trust-enhancing methods in the context of the Safe-DEED project.

Deliverable Structure

This deliverable is divided into three main parts.

The first chapter deals with the role and importance of trust in a European data-driven economy. The second chapter will focus on defining the concept of organizational trust. Here, we will pay specific attention to the notion of digital trust. The third chapter will deal with possible solutions to enhancing organizational trust in data marketplaces.

[1] This deliverable may be publicly consulted on the Safe-DEED website: https://safe-deed.eu/wp-content/uploads/2020/06/Safe-DEED_D3_6.pdf.

Table of Contents

Deliverable Structure 3
List of Abbreviations 6
List of Figures 6
Executive Summary 7
1. The role of trust in a data-sharing context 8
1.1. A European Single-Data Market 8
1.2. The issue of Trust 8
1.2.1. EU Initiatives 9
1.2.2. The European Strategy for Data 10
1.3. Safe-DEED survey on "Trust in a Data Market context" 11
1.4. Semi-structured interviews 14
2. The concept of organizational trust 14
2.1. Organizational trust *in abstracto* 15
2.1.1. Antecedents 18
2.1.1.1. Overview 18
2.1.1.2. Safe-DEED Survey & interviews: trust repair 19
2.1.1.3. Classification 20
2.1.1.3.1. Categories 20
2.1.1.3.2. Actor-related antecedents 21
Trustor characteristics 21
Trustee characteristics 22
Shared characteristics 23
2.1.1.3.3. Business-related antecedents 24
2.1.1.4. Schedule 30
2.1.2. Consequences 31
2.1.2.1. Overview 31
2.1.2.2. Classification 32
2.1.2.2.1. Groups 32
2.1.2.2.2. Nuancing observations 34
2.1.2.3. Schedule 35
2.2. Organizational trust in data marketplaces: digital trust 36

2.2.1. Actors 37
2.2.2. Antecedents 37
2.2.3. Consequences 40
3. The enhancement of organizational trust in data marketplaces 41
3.1. Two pillars 41
3.2. Privacy- and security-enhancing technologies (PETs) 42
3.2.1. Secure Multi-Party Computation and Organizational Trust 42
3.2.2. Legal Certainty and Organizational Trust 45
3.2.2.1. MPC and trust: a double-edged sword 45
3.2.2.2. Harmonization and trust 46
3.3. Codes of Conduct 48
3.3.1. Fairness 49
3.3.2. Transparency 50
3.3.2.1. Art 5(1) and Art 34 GDPR 50
3.3.2.2. Art 10 DGA 51
3.3.2.3. Art 11 DGA 51
3.3.2.4. Art 3 P2BR 53
3.3.2.5. Art 6 FFNPDR 54
3.3.3. Security 56
3.3.4. Neutrality 57
3.4. Summary: two means to enhance trust 58
Conclusion 61
Annex 62
Safe-DEED Survey 62
Semi-structured Interviews 64
Bibliography 66
Legislation 66
EU Communications 67
Doctrine 67
Books and Contributions 67
Journals 68
Online Sources 71

List of Abbreviations

Art	Article
B2B	Business-to-Business
B2C	Business-to-Consumer
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
EU	European Union
FFNPDR	Free Flow of Non-personal Data Regulation
GDPR	General Data Protection Regulation
MPC	Secure Multi-Party Computation
P2BR	Platform-to-Business Regulation
PET(s)	Privacy-enhancing Technologies
Rec	Recital
T&C(s)	Terms and Conditions

List of Figures

Figure 1. Types of trust 17
Figure 2. Antecedents of organizational trust 30
Figure 3. Consequences of organizational trust 35
Figure 4. MPC and legal uncertainty 46

Executive Summary

This deliverable describes the main characteristics linked to the notion of trust in an organizational context, such as in data marketplaces. Therefore, when mentioning trust, differently from what has been done in deliverable 3.6, we will focus our attention on organizational trust instead of its interpersonal counterpart.

KUL has preliminary assess the role of trust in a data-driven economy. In particular, the acknowledgement of trust in the European Strategy for Data shall be alluded to. Moreover, this research will expand upon the concept of organizational trust, both in general and in the data market context (i.e. "digital trust"). In both instances, this deliverable will focus on trust-enhancing antecedents and the overall consequences of a trust-based business-to-business (hereafter: "B2B") relationship.

Furthermore, we will scrutinize two concrete measures to facilitate organizational trust in data marketplaces. In a first place, the possible trust-fostering role of secure multi-party computation (hereafter: "MPC") will be assessed. Against this backdrop, some references shall be made to Safe-DEED's earlier research on MPC. In addition, it will be asserted that codes of conduct may very well be a second tool to facilitate organizational trust. In this regard, it shall be analyzed how these codes of conduct may enhance fairness, transparency, security and neutrality on marketplaces and in what ways these principles relate to the trust-antecedents covered in chapter two.

Finally, this deliverable will summarize the various challenges to organizational trust in a data marketplace while expanding on how MPC and codes of conduct may assist in resolving some current obstacles. Throughout the deliverable, the assumptions and conclusions listed in this deliverable will be substantiated by the answers collected from the survey launched in D3.6 - "Trust in a Data Market context"- and the feedback gathered during semi-structured interviews carried out by KUL with key professional stakeholders. As a result, it will be argued that both codes of conducts and the use of MPC encryption (if legally certain) may add to fostering trust in data marketplaces.

1. The role of trust in a data-sharing context

1.1. A European Single-Data Market

In view of its "European strategy for data", the EC has asserted that "*the success of Europe's digital transformation will depend on establishing effective rules to ensure trustworthy technologies, and to give businesses the confidence and means to digitize*".[2] In this regard, the European strategy for data intends to establish a single market for data that will foster Europe's data sovereignty and global competitiveness.[3] Data constitutes a fundamental resource for economic growth, innovation, competitiveness, job creation and societal development.[4]

In addition to these economic enhancements, data-driven applications are expected to foster complementary benefits, including reducing public services costs and improved sustainability and energy efficiency.[5] On an individual level, the personal profiting from data-sharing services may also foster consumers' psychological satisfaction. During an informal poll by the Safe-DEED and TRUSTS[6] research teams, it was demonstrated that most respondents valued both economic and psychological benefits when exchanging their data.[7]

In light of its European strategy for data, the EU aspires to invest two billion euros in a European High Impact Project to develop data processing infrastructures, data sharing tools, and trustworthy cloud infrastructures.[8] This investment should allow to almost triple the value of the Union's data economy, from €301 billion in 2018 (2.4% of the EU GDP) to €829 billion in 2025 (5.8% of the EU GDP).[9]

1.2. The issue of Trust

[2] European Commission, 'A European Strategy for Data' (Shaping Europe's Digital Future, 9 March 2021) <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> accessed 17 March 2021.
[3] *Ibid.*
[4] *Ibid.*
[5] *Ibid.*
[6] TRUSTS concerns the 'Trusted Secure Data-Sharing Space' research project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871481.
[7] TRUSTS and Safe-DEED, 'Legal Aspects of Data-Sharing Platforms' (online webinar) 31 March 2021.
[8] European Commission, 'A European Strategy for Data' (Shaping Europe's Digital Future, 9 March 2021) <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> accessed 17 March 2021.
[9] European Commission, 'The European Data Strategy: Fact Sheet' (Shaping Europe's Digital Future, 19 February 2020) <https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283> accessed 17 March 2021.

The European Strategy for Data foresees a Union in which: (I) data can flow freely within the EU and across sectors; (II) European rules and values are fully respected; and where (III) the rules for access to and use of data are practical, clear and fair, and (IV) where there are trustworthy data governance mechanisms in place.[10] Hence, trustworthiness takes on an integral role within the EU's data strategy.

Notwithstanding this prominent role of trust in the data strategy, the EC has stated that "*in spite of the economic potential, data sharing between companies has not taken off at sufficient scale*".[11] The EC has elaborated by stating that this burden can be partly attributed to "*the lack of trust between economic operators that the data will be used in line with contractual agreements*", and "*a lack of legal clarity on who can do what with the data*".[12]

In accordance, a lack of trust in the B2B context may impede the development of the EU Digital Single Market. In addition, one may discern an akin tendency in the business-to-consumer (hereafter: "B2C") sphere. In its "Communication on the European Strategy for Data", the EC has namely argued that *"in a society where individuals will generate ever-increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules. Citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules"*.[13] However, this deliverable's material scope is limited to sharing data between businesses (i.e. B2B transactions).

1.2.1. EU Initiatives

The enhancement of trust correlates with the safe and transparent processing of both personal and non-personal data. On individuals' personal data, the EU has already taken a series of efforts since 2014. In this view, the EC has asserted that *"with the GDPR, the EU created a solid framework for digital trust"*.[14] Moreover, several supplementary initiatives have been

[10] European Commission, 'The European Data Strategy: Fact Sheet' (Shaping Europe's Digital Future, 19 February 2020) <https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283> accessed 29 March 2021.
[11] European Commission, 'Industrial Applications of Artificial Intelligence and Big Data' (Internal Market, Industry, Entrepeneurship and SMEs, 2020) <https://ec.europa.eu/growth/industry/policy/advanced-technologies/industrial-applications-artificial-intelligence-and-big-data_en> accessed 19 March 2021.
[12] *Ibid.*
[13] European Commission, 'A European Strategy for Data' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 19 February 2020) COM /2020/66 final.
[14] *Ibid.*

taken to foster the processing of non-personal data and the consequent trust herein. Examples are the Free Flow of Non-personal Data Regulation (FFNPDR)[15] and the Open Data Directive[16]. In addition, sector-specific legislative efforts have been made in different domains to address recognized market failures.[17] These sectors include transport[18], finance[19], energy[20] and media[21].

1.2.2. The European Strategy for Data

As part of its "European Strategy for Data", the EC has announced a series of legislative initiatives. Thus far, the most notable initiative concerns the proposed Regulation on Data Governance (i.e. the Data Governance Act, or "DGA"), adopted by the EC on 25 November 2020.[22] With this instrument, the EU aims to enhance its data-driven economy, increasing trust in data intermediaries and strengthening data-sharing mechanisms in the EU.[23] [24]

[15] 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 [2018] OJ L 303.

[16] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172.

[17] European Commission, 'A European Strategy for Data' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 19 February 2020) COM /2020/66 final.

[18] Regulation (EC) No 595/2009 of the European Parliament and of the Council of 18 June 2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information and amending Regulation (EC) No 715/2007 and Directive 2007/46/EC and repealing Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC [2009] OJ L 188; Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport [2010] OJ L 207.

[19] 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 [2015] OJ L 337.

[20] Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation [2017] OJ L 220; Commission Regulation (EU) 2015/703 of 30 April 2015 establishing a network code on interoperability and data exchange rules [2015] OJ L 113; Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU [2019] OJ L 158; Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC [2009] OJ L 211.

[21] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136.

[22] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act, 25 November 2020) COM/2020/767 final.

[23] *Ibid.*

[24] *Infra.* Chapter 3.

However, despite the central role of trust as part of the European Strategy for Data[25], the concept of organizational trust remains unclear. This definitional ambiguity has been elaborated on in Safe-DEED D3.6.[26] Against this backdrop, the following chapter will scrutinize the concept of organizational trust.

1.3. Safe-DEED survey on "Trust in a Data Market context"

As part of deliverable 3.6, KUL has developed a survey to enhance knowledge and understanding on the notion of trust. To reach this goal, specific questions have been created to understand which criteria are taken into account to generate trust at an organizational level, how shareholders perceive 'trust' and how individuals can be empowered within a B2B platforms environment. The survey was addressed to consumers, civil society representatives, academics, and public servants. A overview of the methodology and questions may be found in the annex.

The survey was launched by WP3, consisted of forty-two questions, and attracted a total of sixty-three anonymous respondents. Sixty respondents were willing to share their capacity: fifty-three (88.3%) of these respondents were either consumers, academics, civil society representatives or public servants. The remaining seven (11.7%) respondents were business representatives. The survey was disseminated both internally (i.e. amongst consortium members) and externally. Dissemination channels included the European Big Data Value Forum (BDVA), Safe-DEED's social media channels and internal newsletters.

Though the responses to the survey should not be regarded as conclusive, they provide valuable insights in both businesses' and consumers' outlooks on digital trust. Throughout this deliverable, continuous reference shall be made to these survey insights. The footnotes will mention the particular question, the corresponding answers, and the number of respondents. A more elaborate overview of the survey's methodology may be consulted in the annex.[27]

With regard to the survey's scope, "B2B platforms" were defined as "*operating systems on the internet, where digital data is exchanged as products or services. It involves the generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation*

[25] *Supra* footnote 1: European Commission, 'A European Strategy for Data' (Shaping Europe's Digital Future, 9 March 2021) <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> accessed 17 March 2021.
[26] Safe-DEED Deliverable 3.6 'Trust in Data Markets v1.0', to be consulted: https://safe-deed.eu/deliverables/.
[27] *Infra* Annex.

of data enabled by digital technologies".[28] Three respondents did not agree with this working definition.[29] However, no further comments or proposals for adaptations were made.

Furthermore, "trust" was defined as *"a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action. When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him".* All respondents agreed with this working definition.[30]

Finally, "e-trust" was defined as *"the notion of trust described above in the online environment. More precisely, "e-trust occurs in an environment where direct and physical contacts do not take place, moral and social pressures can be differently perceived, and where interactions are mediated by digital devices".* Two respondents had reservations about this working definition, though no proposed adaptations were made on their behalf.[31] In this deliverable, e-trust will equally be referred to as "digital trust", as both terms are used interchangeably in doctrine.[32]

The survey aimed to understand the respondents' perception of trust-enhancing factors and their view on the importance of trust in the data market context. Despite trust often being coined as

[28] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions "Building a European Data Economy"' (COM(2017) 9 final).
[29] Safe-DEED Survey on "Trust in a Data Market context", question: *"Do you agree with the following working definition of B2B platforms: an operating system on the internet where digital data is exchanged as products or services. It involves the generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation of data enabled by digital technologies*", 10 answers were given, answer breakdown: "yes" (7 respondents, 70.0%) "no" (3 respondents, 30.0%).
[30] Safe-DEED Survey on "Trust in a Data Market context", question: *"Do you agree with the following working definition of trust: a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action. When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him*", 10 answers were given, answer breakdown: "yes" (10 respondents, 100.0%) "no" (0 respondents, 0.0%).
[31] Safe-DEED Survey on "Trust in a Data Market context", question: "Do you agree with the following working definition of e-trust: *The term encompasses the notion of trust described above in the online environment. More precisely, "e-trust occurs in an environment where direct and physical contacts do not take place, moral and social pressures can be differently perceived, and where interactions are mediated by digital devices".*" 10 answers were given, answer breakdown: "yes" (8 respondents, 80.0%) "no" (2 respondents, 20.0%).
[32] *Infra* Chapter 2.2. Organizational Trust in Data Marketplaces: Digital Trust.

a characteristic of human relations, trust can also be attributed to legal entities in a commercial setting, as was affirmed by the respondents themselves.[33]

Moreover, the value of trust in the EU Digital Single Market should not be overlooked. As the single market is built upon cooperation, trust is essential. All respondents namely agreed that the higher the level of trust in a B2B platform environment, the higher the likelihood of cooperation.[34] Furthermore, most respondents do not accept greater risk in an offline context than in a B2B platform context.[35]

In the remainder of this deliverable, the Safe-DEED survey on trust in a data market context will be referred to as "the Safe-DEED survey" or "the survey".

[33] Safe-DEED Survey on "Trust in a Data Market context", question: "Would you agree with the following statement: *Trust, even though it is a characteristic of human relations, it can be attributed to legal entities in a commercial setting."*." 10 answers were given, with an average rating of 8.7 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (0 respondents, 0.0%); "4" (0 respondents, 0.0%); "5" (1 respondent, 10.0%); "6" (0 respondents, 0.0%); "7" (0 respondents, 0.0%); "8" (3 respondents, 30.0%); "9" (2 respondents, 20.0%); "10" (4 respondents, 40.0%).

[34] Safe-DEED Survey on "Trust in a Data Market context", question: "Would you agree with the following statement: *Regarding a B2B platform environment, our organization thinks that the higher the level of trust is, the higher the likelihood of cooperation is."*, 10 answers were given, with an average rating of 8.6 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (0 respondents, 0.0%); "4" (0 respondents, 0.0%); "5" (0 respondent, 0.0%); "6" (1 respondent, 10.0%); "7" (2 respondents, 20.0%); "8" (2 respondents, 20.0%); "9" (0 respondents, 0.0%); "10" (5 respondents, 50.0%).

[35] Safe-DEED Survey on "Trust in a Data Market context", question: "Would you agree with the following statement: *Our organization accepts greater risks in an offline context, rather than in a B2B platforms environment"*, 10 answers were given, with an average rating of 4.3 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (3 respondents, 30.0%); "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (0 respondents, 0.0%); "4" (0 respondents, 0.0%); "5" (4 respondents, 40.0%); "6" (1 respondent, 10.0%); "7" (1 respondent, 10.0%); "8" (2 respondents, 20.0%); "9" (0 respondents, 0.0%); "10" (0 respondents, 0.0%).

1.4. Semi-structured interviews

After obtaining and analysing the survey results, WP3 has conducted semi-structured interviews with selected survey respondents to build further upon the survey findings and gather additional qualitative insights. The stakeholders were selected among relevant industry sectors. Members of staff as well as decision makers within companies were contacted. Conversation have for instance taken place with the manufacturing community to understand concrete barriers they may have in establishing trust in their network. Similarly to the survey, the interviews were anonymised and classified based on certain characteristics, e.g. industry sectors and type of actors.

To ensure compliance with the Covid-19 measures in Belgium at the time, interviews were conducted online, partly with the assistance of other WPs. A set of fourteen standardized questions was disseminated amongst relevant actors with the assistance of Safe-DEED partners. A total of sixteen responses was gathered.

The sixteen respondents consisted mainly of online service providers (twelve respondents), whilst four responses came from manufacturers. Though not all respondents elaborated on the industry sector their company performs its activity in, four online service providers clarified that they mainly provide consulting services. In contrast, four other respondents are active in the telecom, retail, and automotive sectors. Eight respondents stated to have less than fifty employees. Two respondents had more than one hundred employees, whilst two others have more than five hundred employees. Two respondents had more than 1000 employees on board. All respondents rely on the processing of personal and non-personal data, though one company claimed to rely only on processing of personal data.

An overview of the sample questions can be found in the annex. The ensuing qualitative insights have been integrated in chapter two of this deliverable. The Safe-DEED solutions in chapter three have subsequently implemented the forthcoming lessons from both the fundamental research, the survey and the interviews.

2. The concept of organizational trust

Tough trust in data marketplaces is vital to fostering a data-driven economy and a trust-enhancing B2B environment remains burdensome. This challenge can be partly attributed to the extensive conceptual nature of "trust". In the data market context, actors must for instance trust that the data is of high quality and dependable; the supply will be consistent and not break processes; the data will deliver value once it has started to be used; the consumer will not steal the data (or have it stolen from them); and that the consumer will not use the data for non-permitted use cases.

Against the backdrop of these various contexts, defining "trust" in a unique manner has proven to be onerous. The EC has deemed this impediment as one of the reasons why data marketplaces fail.[36] In its "Communication on Building a European Data-economy", the EC has stated that *"trust will allow the digital economy to develop across the internal market"*.[37] As a result, the EC has allowed for interdisciplinary research on the conceptualization and enhancement of trust in the data market context.[38]

The importance of a comprehensive trust enhancement vis-à-vis actors in marketplaces thus seems clear-cut. Against the backdrop of such an envisioned trust enhancement, three indispensable questions arise:

(I) how can "trust" best be defined in the data-driven context;

(II) how can trust be ensured to the most viable extent, and;

(III) what consequences may be expected to arise from more trust-driven data marketplaces?

The following subchapters intend to formulate a preliminary answer to these questions, alongside insights from the survey and semi-structured interviews. A first subchapter will deal with trust "in general". This subchapter assesses trust in abstraction from the data marketplace framework. More specifically, this part will analyze the different forms of trust, the main parties of a trust relation, and the various antecedents and consequences of a trust-enhanced B2B environment. The subsequent subchapter will then briefly apply these insights to the particular data market context.

2.1. Organizational trust *in abstracto*

In the Safe-DEED survey, trust was defined as "*a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action. When we say we trust someone*

[36] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act, 25 November 2020) COM/2020/767 final.

[37] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions "Building a European Data Economy" (COM(2017) 9 final), available at < https://eur- lex.europa.eu/legal-context/EN/TXT/?uri=COM:2017:9:FIN>, accessed 11 December 2020.

[38] In addition to the Safe- DEED research, other noteworthy projects concern the EU-funded TRUSTS project ("Trusted Secure Data Sharing Space")[38], and the KRAKEN project ("Brokerage and Market Platform for Personal Data")[38], all of which the KU Leuven Center for IT and IP Law is involved in.

or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him".[39] As stated before, all respondents agreed to this wording.[40]

In the semi-structured interviews however, respondents were asked to formulate their own definition of trust. Though most respondents did not manage to provide a coherent definition, some were able to formulate their own working definition, based on practical experiences. One respondent defined trust as "*the certitude that another party will follow up through equitable intentions*", whilst another unanimous respondent perceived trust as "*the understanding that all technical, legal and ethical requirements have been met by a business partner*". A third respondent regarded trust as "*knowing that data processing and business conduct will happen in a fair and transparent manner, despite the complexity of the business environment*". Rather than providing a coherent definition, most respondents were able to sum up a number of trust-enhancing factors, the most common answers being "transparency", "fairness" and "regulatory compliance". In this subchapter, these antecedents to trust will be further explored, while fostering a more intelligible understanding of trust in the organizational context.

In the management context, trust is generally deemed relevant on three levels. The first layer comprises the concept of interpersonal trust, which refers to trust in a specific other or others.[41] A second layer concerns "team trust", which describes trust in the context where an interdependent collectivity pursues a shared goal with inherently unique dynamics.[42] Finally, "organizational trust" refers to trust in the entity of an organization.[43]

[39] *Supra* 1.3 Safe-DEED Survey;

[40] Safe-DEED Survey on "Trust in a Data Market context", question: *"Do you agree with the following working definition of trust: a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action. When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him*", 10 answers were given, answer breakdown: "yes" (10 respondents, 100.0%) "no" (0 respondents, 0.0%).

[41] Roy Lewicki, Edward Tomlinson, Nicole Gillespie, 'Models of interpersonal trust development: Theoretical approaches, empirical evidence, and future directions' (2006) 32 Journal of Management 991; Julian Rotter, 'Interpersonal trust, trustworthiness, and gullibility' (1980) 35(1) American Psychologist 1.

[42] Richard Guzzo, Marcus Dickson, 'Teams in organizations: Recent research on performance and effectiveness' (1996) 47 Annual Review of Psychology 307; Mark Serva, Mark Fuller, Roger Maye ' The reciprocal nature of trust: A longitudinal study of interacting teams' (2005) 26 Journal of Organizational Behaviour 625.

[43] David Schoorman, Roger Mayer, James Davis, 'An integrative model of organizational trust: Past, present and future' (2007) 32 Academy of Management Review 344; Pamela Shockley-Zalabak, Kathleen Ellis, Gayelle Winograd, 'Organizational Trust: What it means, why it matters' (2000) 18(4) Organization Development Journal 35.

Each trust relationship entails at least two actors: the "trustor" and the "trustee".[44] In the organizational context -, the organization is the so-called "trustee", whilst those interacting with it (both internally and externally) are "trustors". Furthermore, organizational trust is relevant internally (i.e. vis-à-vis those active within the organization) and externally (i.e., external actors' trust in an organization). The former is often referred to as "inter-organizational trust". Moreover, some literature makes an additional distinction based on the trustor's capacity.[45] In this regard, organizational trust may encompass both "individuals' trust in organizations" and "organizations' trust in organizations".[46] This discrepancy is not of relevance in this deliverable, as data marketplaces in the Safe-DEED research exclusively allude to B2B relationships. In the remainder of this deliverable, "organizational trust" shall therefore solely refer to "organizations' trust in organizations".[47]

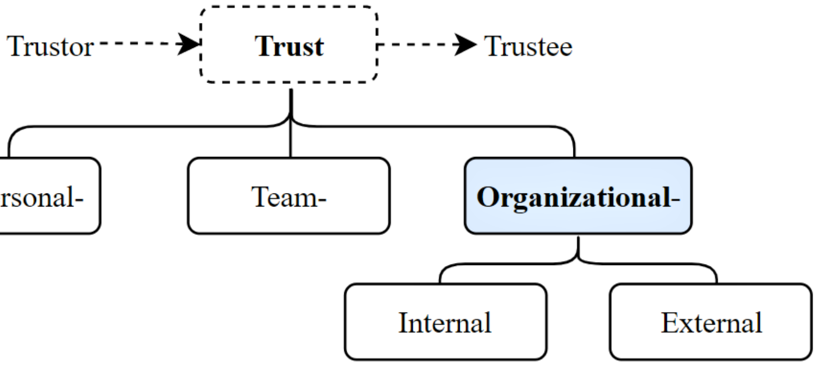

Figure 1. Types of trust [48]

Hence, in its simplest form, "organizational trust" can be defined as an organization's trust in another organization, both internally and externally, built upon variables such as (I) its mission; (II) it's leadership vision; (III) the organization's culture and values; (IV) its policy on diversity, inclusion and equality; and (V) its ethics and fairness of processes.[49]

The next subchapter will expand upon these variables. It shall be assessed what factors (i.e.

[44] See Safe-DEED D3.6, 4.1 'Key Elements that define Trust', https://safe-deed.eu/wp-content/uploads/2020/06/Safe-DEED_D3_6.pdf.
[45] Ashley Fulmer, Michele Gelfand, 'At what level (and in whom) do we trust: trust across multiple organizational levels' (2012) 38(4) Journal of Management 1167.
[46] *Ibid.*
[47] *Ibid.*
[48] Figure made by KUL (WP3), as part of the Safe-DEED research on organizational trust in D3.7.
[49] Will Otto, 'What is organizational trust (and how to build it)?' (2020) The Predictive Index Blog <https://www.predictiveindex.com/blog/what-is-organizational-trust-and-how-to-build-it/> accessed 12 December 2020.

"antecedents") enhance organizational trust.

2.1.1. Antecedents

2.1.1.1. Overview

At its core - as with trust at all levels -, social exchange theory offers a fundamental theoretical perspective to understand the underlying process of trust at the organizational level.[50]

Firstly, some trustor characteristics correlate with organizational trust.[51] In this regard, it has been shown that especially organizational identification is trust-enhancing.[52] The notion "organizational identification" refers to entities' propensity to identify themselves with an organization.[53] Moreover, trustee traits – such as a climate of integrity[54] and leadership credibility[55] - have been shown to add to trust as well. On a more inter-organizational level, it has been established that *inter alia*, a common business understanding and relationship satisfaction add to trust in an organization.[56]

Secondly, communication is another essential antecedent to establish (organizational) trust.[57] In virtual inter-organizational relations especially, trust is higher when organizations can effectively communicate their trustworthiness.[58]

Thirdly, voluntary compliance with external regulations may equally add to trust in the organizational context.[59] Furthermore, so-called "asset specificity" of the exchanged resource

[50] Ashley Fulmer, Michele Gelfand, 'At what level (and in whom) do we trust: trust across multiple organizational levels' (2012) 38(4) Journal of Management 1167.

[51] Mark Davies, Walfried Lassar, Chris Manolis, Melvin Prince, Robert Winsor, 'A model of trust and compliance in franchise relationships' (2011) 26(3) Journal of Business Venturing 321.

[52] Steve Marguire, Nelson Phillips, 'Citibankers at Citigroup: a study of the loss of institutional trusts after a merger' (2008) 45(2) Journal of Management Studies 372.

[53] *Infra* 2.2. "Organizational Trust in data marketplaces: digital trust"; Stuart Albert Blake Ashforth, Jane Dutton, 'Organizational Identity and Identification: charting new waters and building new bridges' (2000) 25(1) The Academy of Management Review 13.

[54] Michael Palanski, Francis Yammarino, 'Integrity and leadership: a multi-level conceptual framework' (2009) 20(3) The Leadership Quarterly 405.

[55] Richard Burton, Jorgen Lauridsen, Borge Obel, 'The impact of organizational climate and strategic fit on firm performance' (2004) 43(1) Human Resources Management 67.

[56] Eva Kasper-Fuehrer, Neal Ashkanasy, 'Communicating trustworthiness and building trust in interorganizational virtual organizations' (2001) 27(235) Journal of Management 1.

[57] Marcel van Marrewijk, 'The social dimension of organizations: recent experiences with "places to work" assessment practices' (2004) 55(2) Journal of Business Ethics 135; Thomas Gainey, Brian Klaas, 'The outsourcing of training and development: factors impacting client satisfaction' (2003) 29(2) Journal of Management 207.

[58] Eva Kasper-Fuehrer, Neal Ashkanasy, 'Communicating trustworthiness and building trust in interorganizational virtual organizations' (2001) 27(235) Journal of Management 1.

[59] Roy Lewicki, Edward Tomlinson, Nicole Gillespie, 'Models of interpersonal trust development: theoretical approaches, empirical evidence, and future directions' (2006) 32 Journal of Management 991.

(i.e., the extent to which the invested assets cannot be transferred, limiting the likelihood of contract breach) has also resulted to be an element positively affecting trust in an organizational set up.[60]

Fourthly, some organizational practices, such as protocols ensuring compliance with principles such as fairness, transparency and coherency, also facilitate trust in organizations.[61] With regard to this, variables external to organizations, such as unstable markets, have been asserted to impact perceptions of organizational trustworthiness.[62]

One last preliminary antecedent concerns the way in which organizations deal with trust breaches *ex post facto*, i.e. so-called "trust repair". Though one single violation does not necessarily obliterate the trust relation[63], an early violation of benevolence in the inter-organizational context hampers trust significantly.[64] In addition, if a violation stems from the conduct at a high organizational level, trust repair is significantly more challenging than when it occurs at a lower level within the organization.[65]

2.1.1.2. Safe-DEED Survey & interviews: trust repair

The Safe-DEED survey has demonstrated that the impact of trust repair should not be overvalued, as trust is seemingly fragile: once it has been broken, it is hard to restore. Respondents were asked whether they agreed with the statement, "*If one platform is not trustworthy anymore in your eyes (for example, due to a data breach, a financial scandal, or another reason), would you agree with the statement: I would stop using its services*".[66] The

---

[60] Constantine Katsikeas, Dionysis Skarmeas, 'Developing successful trust-based international exchange relationships' (2009) 40(1) Journal of International Business Studies 132; Thomas Gainey, Brian Klaas, 'The outsourcing of training and development: factors impacting client satisfaction' (2003) 29(2) Journal of Management 207.

[61] Raminta Pucetaite, Anna-Maija Lämsä, 'Developing organizational trust through advancement of employees' work ethic in a post-socialist context' (2008) 82(2) Journal of Business Ethics 325.

[62] Randy Hodson, 'Organizational Trustworthiness: findings from the population of organizational ethnographies' (2004) 15(4) Organization Science 432.

[63] Helle Neergaard, John Ulhoi, 'Government agency and trust in the formation and transformation of interorganizational entrepeneurial networks' (2006) 30(4) Entrpeneurship: Theory and Practice 519.

[64] Geoffrey Bell, Robert Oppenheimer, Andre Bastien, 'Trust deterioration in an international buyer-supplier relationship' (2002) 36 Journal of Business Ethics 65.

[65] Martyna Janowicz-Panjaitan, Rekha Krishnan, 'Measures for dealing with competence and integrity violations of interorganizational trust at the corporate and operating levels of organizational hierarchy' (2009) 46(2) Journal of Management Studies 245.

[66] Safe-DEED Survey on "Trust in a Data Market context", question: *"If one platform is not trustworthy anymore in your eyes (for example, due to a data breach, a financial scandal, or another reason), would you agree with the statement: I would stop using its services*", 53 answers were given, with an average rating of 7.1 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (1 respondents, 1.9%); "3" (2 respondents, 3.8%); "4" (3 respondents, 5.7%); "5" (6 respondents,

average answer rating was 7.1/10 (with 0 meaning "I fully disagree" and 10 meaning "I fully agree").

Moreover, about half of the respondents (26 subjects; 49%) gave a score of 8/10 or higher. It can thus be derived that at least half of the respondents would certainly no longer use a service after a trust violation. In addition, most respondents would no longer be willing to use the services of the entity's sister platforms either.[67] These insights clearly nuance the trust-enhancing impact of trust repair, though the weight of this factor unequivocally hinges on the seriousness of the trust violation, the organizational level on which it occurs and the approach to trust reparation. Following this insight, the trust-enhancement of trust repair can be expected to be more prominent in case of low-level breaches. Furthermore, 60.4% of the respondents have admitted to being more forbearing in instances where they have been using a platform for several years.[68] The impact of trust repair thus also relies upon the concrete relational duration between trustor and trustee.

Lastly, the semi-structured interviews have shown that in B2B settings, personal and non-personal data breaches similarly affect an entity's trust perception. This insight highlights the need for a trust-enhancing approach that considers both personal and non-personal data protection. This understanding has been taken into account whilst developing Safe-DEED solutions to trust enhancement in data marketplaces.[69]

2.1.1.3. Classification

2.1.1.3.1. Categories

Trust-enhancing antecedents may be inductively grouped into two overarching categories. The first group comprises characteristics linked to the nature and general conduct of the parties involved on the one hand. In contrast, the second group includes antecedents related to the

11.3%); "6" (7 respondents, 13.2%); "7" (8 respondents, 15.1%); "8" (14 respondents, 26.4%); "9" (6 respondents, 11.3%); "10" (6 respondents, 11.3%).

[67] Safe-DEED Survey on "Trust in a Data Market context", question: *"If one platform is not trustworthy anymore in your eyes (for example, due to a data breach, a financial scandal, or another reason), would you agree with the statement: I would stop using the services of its sister platforms, if any*", 53 answers were given, with an average rating of 7.1 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (5respondents, 9.4%); "3" (3 respondents, 5.7%); "4" (6 respondents, 11.3%); "5" (7 respondents, 13.2%); "6" (9 respondents, 17.0%); "7" (9 respondents, 17.0%); "8" (8 respondents, 15.1%); "9" (3 respondents, 5.7%); "10" (3 respondents, 5.7%).

[68] Safe-DEED Survey on "Trust in a Data Market context", question: *"If one platform is not trustworthy anymore in your eyes (for example, due to a data breach, a financial scandal, or another reason), would you agree with the statement: I would stop using its services. Would your answer change if you have been using the platform for several years*", 53 answers were given, answer breakdown: "yes" (32 respondents, 60.4%); "no" (21 respondents, 39.6%).

[69] *Infra* 3. 'The Enhancement of Organizational Trust in Data Marketplaces'.

business setting on the other hand.

The first group of "actor-related antecedents" includes:

(I) trustor characteristics,

(II) trustee characteristics, and

(III) their shared characteristics.

The second category of so-called "business-related antecedents" encompass characteristics such as:

(I) communication processes,

(II) structural traits,

(III) organizational characteristics, and

(IV) external characteristics to the organization.

In their turn, these subgroups entail a number of specific antecedents, all of which will be elaborated upon in the ensuing subsections.

2.1.1.3.2. Actor-related antecedents

Trustor characteristics

This first group comprises all antecedents that are linked to the nature of the respective actors (i.e. the parties to the trust relationship). The first subgroup of actor-related antecedents are so-called "trustor characteristics". This subgroup is rather limited since trust-enhancement mainly relies upon the trustee's conduct. Nevertheless, a noteworthy antecedent within this first subgroup is "organizational identification". This is "*the propensity of a member of an organization to identify with that organization*".[70] In other words, organizational identification concerns the willingness of a trustor to identify oneself with an organization. This is not a self-standing antecedent, as trustors' propensity heavily depends on the prevalence of other trust-enhancing antecedents.

Furthermore, the propensity to identify oneself with an organization partly hinges on a sense of empowerment.[71] Suppose one has a sense of control and responsibility and feels seen and heard by an organization, one may expect an increase in organizational identification and, thus, equally in organizational trust. This relationship between consumer empowerment and trust was the subject of a question in the Safe-DEED survey. Respondents were asked whether "*within a B2B platforms environment, empowering consumers is crucial for obtaining their*

[70] Stuart Albert Blake Ashforth, Jane Dutton, 'Organizational Identity and Identification: charting new waters and building new bridges' (2000) 25(1) The Academy of Management Review 13.

[71] *Ibid.*

trust".[72] Though 51 out of the 53 respondents (somewhat) agreed with this statement, more than a quarter (28.3%) gave a score of 5/10, equating a rather indifferent stance to this premise. The empowerment of consumers is thus not considered to be a fundamental trust-enhancing factor, though it can certainly be regarded as an antecedent to trust under the veil of organizational identification.

Trustee characteristics

A second subgroup concerns trustee characteristics. As trustees essentially ought to ensure trustors' organizational trust, this subgroup is more expansive than the former. In this regard, "trustee characteristics" encompass several antecedents, the most notable of which are the trustee's integrity[73], fairness[74], proficiency (i.e. "task competence")[75], equity[76] and ethical approach to business[77].

The particular antecedent of "task competence" should not be confused with "experience with a task". The trustee's technical experience, namely, does not affect the perceived trust in the organization. The Safe-DEED survey has demonstrated this insight.[78] Half of the respondents namely stated to be indifferent to the technical experience of the trustee.[79] Though proficiency with a task is a trust-enhancing antecedent, the trustee's experience in dealing with said task thus seems to be of lesser importance because of the perceived organizational trust.

[72] Safe-DEED Survey on "Trust in a Data Market context", question: *"Would you agree with the following statement: within a B2B platforms environment, empowering consumers is crucial for obtaining their trust*", 53 answers were given, with an average rating of 6.9 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (1 respondents, 1.9%); "3" (0 respondents, 0.0%); "4" (1 respondents, 1.9%); "5" (15 respondents, 28,3%); "6" (6 respondent, 11.3%); "7" (7 respondents, 13.2%); "8" (10 respondents, 18.9%); "9" (8 respondents, 15.1%); "10" (5 respondents, 9.4%).

[73] Michael Palanski, Francis Yammarino, 'Integrity and leadership: a multi-level conceptual framework' (2009) 20(3) The Leadership Quarterly 405.

[74] Lisa Scheer, Nirmalya Kumar, Jan-Benedict Steenkamp, 'Reactions to perceived inequity in US and Dutch interorganizational relationships' (2003)46 Academy of Management Journal 303.

[75] *Ibid.*

[76] Michael Palanski, Francis Yammarino, 'Integrity and leadership: a multi-level conceptual framework' (2009) 20(3) The Leadership Quarterly 405.

[77] Eva Kasper-Fuehrer, Neal Ashkanasy, 'Communicating trustworthiness and building trust in interorganizational virtual organizations' (2001) 27(235) Journal of Management 1.

[78] Safe-DEED Survey on "Trust in a Data Market context", question: "*Would you agree with the following statement: within a B2B platforms environment, our company trusts more a data savvy partner, than a partner who has less experience in B2B platforms",* 10 answers were given, with an average rating of 5.8 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (1 respondent, 10.0%); "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (0 respondents, 0.0%); "4" (0 respondents, 0.0%); "5" (5 respondents, 50.0%); "6" (0 respondents, 0.0%); "7" (2 respondents, 20.0%); "8" (0 respondents, 0.0%); "9" (1 respondent, 10.0%); "10" (1 respondent, 10.0%).

[79] *Ibid.*

Furthermore, survey findings show that "task competence" should neither be confused with "the trustee's use of sophisticated data analytics tools".[80] The Safe-DEED survey has namely shown that the sophistication level of the trustee's data analytics tools does not impact its perceived organizational trust.[81] Based on these two Safe-DEED survey insights, "task competence" should best be read as "the level of vocational aptitude demonstrated throughout the concrete collaboration between trustor and trustee". Accordingly, trust-enhancing task competence does not necessarily hinge on the trustee's past experience nor the use of particular technical tools.

Shared characteristics

A final subgroup concerns the shared characteristics between both parties. In its turn, this subgroup encompasses a series of trust-antecedents. The existence of a common business understanding[82], for example, has already been mentioned as a key characteristic. Other antecedents include the actors' expected future relationship[83] and previous relationships between the trustor and trustee[84].

One could define such a qualitative (present and future) relationship as a collaboration where both parties provide value to one another. As such, one could presume that value exchange may equally be an impactful trust-enhancing factor. To verify this premise, the Safe-DEED survey has asked respondents whether they "*consider value exchange as an important factor for increasing trust in a platform (5 meaning the most important and 1 meaning the least important)*".[85] The average response rating was 3.1/5. Moreover, an equal number of respondents (9.4%) gave a score of 1 ("not important") and 5 ("the most important"). 41.5% of

[80] Safe-DEED Survey on "Trust in a Data Market context", question: "*Within a B2B platforms environment, the more sophisticated data analytics tools our partner is using, the less control our company has over how our datasets are actually processed",* 10 answers were given, with an average rating of 3.6 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (4 respondents, 40.0%); "1" (0 respondents, 0.0%); "2" (1 respondent, 10.0%); "3" (0 respondents, 0.0%); "4" (1 respondent, 10.0%); "5" (2 respondents, 20.0%); "6" (0 respondents, 0.0%); "7" (0 respondents, 0.0%); "8" (0 respondents, 0.0%); "9" (0 respondents, 0.0%); "10" (2 respondents, 20.0%).

[81] *Ibid.*

[82] *Ibid*.

[83] Andrew Inkpen, Eric Tsang, 'Social Capital, Networks, and Knowledge Transfer' (2005) 30 Academy of Management Review 146.

[84] Henri Dekker, A.G.H.L. van den Abbeele, 'Organizational learning and interfirm control: the effects of partner search and prior exchange experiences' (2010) 21 Organization Science 1233.

[85] Safe-DEED Survey on "Trust in a Data Market context", question: *"Do you consider value exchange as an important factor for increasing your trust in a platform (5 meaning the most important and 1 meaning the least important)"*, 53 answers were given, with an average rating of 3.1, answer breakdown: "1" (5 respondents, 9.4%); "2" (17 respondents, 9%); "3" (22 respondents, 41.5%); "4" (12 respondents, 22.6%); "5" (5 respondents, 9.4%).

the respondents provided a score of 3/5, and around 20% answered with either 2/5 or 4/5.[86] These responses form a quasi-perfect Laplace-Gauss distribution. Hence, these numbers indicate that respondents acknowledge the impact of value exchange as a trust-enhancing factor, though they do not grant as much weight to this element as to some other factors[87] (e.g. quality control, transparency, security, and data management).

The semi-structured interviews have substantiated the rather limited correlation between value exchange and organizational trust. Respondents mostly argued that the exchange of value is not an important prerequisite for trust. Two respondents added that they believe value exchange might be a noteworthy antecedent to trust "*in some settings*", though they did not further elaborate on the nature of such settings.

The semi-structured interviews have also affirmed the general impact of "shared characteristics" on trust. Respondents agreed that their companies mostly trust (sub)contractors based on personal relations and prior engagement. Respondents have thus emphasized the practical weight of the antecedents "prior relationship", "joint dependence" and "relationship satisfaction".

Furthermore, interview respondents have unanimously acknowledged the importance of contractors' due diligence to generate trust. "Due diligence" should be understood in the notion's legal sense, meaning "*the care that a reasonable person exercises to avoid harm to other persons or their property*".[88] Hence, organizational trust relies on an entity taking notice of the contractors' interests whilst valuing the long-term B2B relationship. The attested impact of due diligence on trust, therefore, underlines the antecedents of "mutual adaptation", "joint dependence" and "expected future relationship". The semi-structured interviews have shown that - in practice -, these three antecedents are perceived as truly trust-enhancing by the respondents. Against this backdrop, the Safe-DEED solutions in chapter 3 will grant sufficient weight to the trust indicator of due diligence, *inter alia,* by maintaining a substantive fairness principle in the proposed codes of conduct.[89]

2.1.1.3.3. Business-related antecedents

The second group entails antecedents that are not as strictly linked to the nature of the actors,

---

[86] *Ibid.*

[87] *Infra* 2.1.1.2.3. Business-related antecedents; *Infra* 3.2. Privacy- and security-enhancing technologies.

[88] Merriam Webster, "Due Diligence" <www.merriam-webster.com/dictionary/due%20diligence> accessed 26 October 2021.

[89] *Infra* 3.3.1. Fairness.

but are more closely related to the overall collaborative business practices and (external) circumstances. This group encompasses four subgroups. A first subgroup involves "communication processes", which includes clear communication of trustworthiness[90], communication quality[91], interactional courtesy[92] and an adequate degree of two-way communication[93].

It should be noted that interactional courtesy and two-way communication may correlate with a wide margin of negotiation on the trustor's side and may equally entail an equal-levelled hierarchy in B2B communications. This insight can be derived from one of the Safe-DEED survey findings. Respondents were namely asked whether they agree that take-it-or-leave-it style agreements undermine trust.[94] Half of the respondents (50%) somewhat agreed, whilst a fifth (20%) completely disagreed. About a third (30%) of the respondents did not take in an outright stance. Though two-way communication generally enhances trust, this premise has not been conclusively affirmed in the survey findings. As the respondents' answers were rather divergent, it cannot be ascertained to what extent (if at all) a lack of contractual manoeuvre impacts one's trust in B2B collaborations.

A subsequent subgroup has been marked as "structural characteristics", including within this group reliability-enhancing antecedents, such as voluntary self-sanctioning[95], the adherence to contract provisions[96] and asset specificity[97] (which has been defined *supra*[98]).

---

[90] Eva Kasper-Fuehrer, Neal Ashkanasy, 'Communicating trustworthiness and building trust in interorganizational virtual organizations' (2001) 27(235) Journal of Management 1.

[91] Günter Stahl, Rikard Larsson, Ina Kremershof, Sim Sitkin, 'Trust dynamics in acquisitions: a case study' (2011) 50Human Resource Management 575.

[92] Josh Gullett, Loc Do, Maria Canuto-Carranco, Mark Brister, Shundricka Turner, Cam Caldwell, 'The buyer-supplier relationship: an integrative model of ethics and trust' 2009 (90) 3 Journal of Business Ethics 329.

[93] Marcel van Marrewijk, 'The social dimension of organizations: recent experiences with "places to work" assessment practices' (2004) 55(2) Journal of Business Ethics 135.

[94] Safe-DEED Survey on "Trust in a Data Market context", question: "Would you agree with the following statement: *Take-it-or-Leave-it style agreements undermine trust."*, 10 answers were given, with an average rating of 5.3 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (2 respondents, 20.0%); "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (0 respondents, 0.0%); "4" (0 respondents, 0.0%); "5" (3 respondents, 30.0%); "6" (0 respondents, 0.0%); "7" (2 respondents, 20.0%); "8" (3 respondents, 30.0%); "9" (0 respondents, 0.0%); "10" (0 respondents, 0.0%).

[95] Nicole Gillespie, Graham Dietz, 'Trust repair after an organization-level failure' (2009) 34 Academy of management review 127.

[96] Deepak Malhotra, Fabrice Lumineau, 'Trust and collaboration in the aftermath of conflict: the effects of contract structure' (2011) 54 Academy of Management Journal 981.

[97] Thomas Gainey, Brian Klaas, 'The outsourcing of training and development: factors impacting client satisfaction' (2003) 29 Journal of Management 207.

[98] *Supra* 2.1.1.1. "Overview".

Moreover, it should be underlined that such voluntary self-compliance is a form of quality control. In managerial settings, "quality control" is coined as "*a process by which entities review the quality of all factors involved in a production*".[99] The quality review may encompass three aspects of a production procedure: (I) performance, job management and integrity criteria; (II) competence, including skills, knowledge, expertise and qualifications; and (III) "soft elements", such as confidence, integrity, team spirit, motivation, relationships and organizational culture.[100] The premise that such voluntary self-compliance (as a form of quality control) enhances organizational trust has been confirmed in the Safe-DEED survey. Respondents were namely asked whether they "*consider quality control as an important factor for increasing trust in a platform*". On a scale from one ("not important") to five ("the most important"), the average respondent's rating was 4.2.[101] In addition, 90.5% of the respondents deemed that implementing quality controls and auditing procedures for the different functionalities of the B2B platform increases trust.[102] These findings thus affirm the premised weight of self-compliance and quality control as antecedents to organizational trust.

A third subgroup comprises so-called "organizational characteristics". These concerns organizational practices, and most have an impact on internal organizational trust. Therefore, this subgroup has a limited bearing on external organizations' trust in a data marketplace and mostly affect complementary service providers' trust in the data marketplace provider. Notable antecedents within this subgroup are fair and transparent policies[103], leadership credibility[104], supportive employment practices[105], and "management measures and competence"[106].

[99] International Organization for Standardization (ISO) 9000:2005, Clause 3.2.10.

[100] International Organization for Standardization (ISO) 9001:2015, Clauses 4.1-4.3.

[101] Safe-DEED Survey on "Trust in a Data Market context", question: *"Do you consider quality control as an important factor for increasing your trust in a platform (5 meaning the most important and 1 meaning the least important)"*, 53 answers were given, with an average rating of 4.2, Answer breakdown: "1" (0 respondents, 0.0%); "2" (2 respondents, 3.8%); "3" (10 respondents, 18.9%); "4" (17 respondents, 32.1%); "5" (24 respondents, 45.3%).

[102] Safe-DEED Survey on "Trust in a Data Market context", question: *"Would you agree with the following statement: within a B2B platforms environment, implementing quality controls and auditing procedures for the different functionalities of the platform increases trust*", 53 answers were given, with an average rating of 8.6 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (0 respondents, 0.0%); "4" (0 respondents, 0.0%); "5" (4 respondents, 7.5%); "6" (1 respondent, 1.9%); "7" (13 respondents, 24.5%); "8" (13 respondents, 24.5%); "9" (13 respondents, 24.5%); "10" (9 respondents, 17.0%).

[103] Nicole Gillespie, Graham Dietz, 'Trust repair after an organization-level failure' (2009) 34 Academy of management review 127.

[104] Richard Burton, Jorgen Lauridsen, Borge Obel, 'The impact of organizational climate and strategic fit on firm performance' (2004) 43(1) Human Resources Management 67.

[105] Randy Hodson, 'Organizational Trustworthiness: findings from the population of organizational ethnographies' (2004) 15(4) Organization Science 432.

[106] *Ibid*.

The importance of transparent policies has equally been upheld in the Safe-DEED survey. The question raised was: "*Do you consider transparency measures such as full pricing, visible inventory, and clear and understandable contract summaries as important factors for increasing your trust in a platform?*". The average respondent's rating was 4.6 out of 5, with 71.7% of the respondents considering transparency one of the most important trust-enhancing factors.[107] In addition, almost all respondents (94.4%) agreed that within a B2B platforms environment, measures that enhance transparency are important for generating consumers' trust.[108] Moreover, about three quarters (77.4%) of the respondents acknowledged a trust-enhancing impact of transparency in B2C platform ecosystems.[109] In the semi-structured interviews, transparency – alongside security – was unanimously affirmed to be the most important mechanism to ensure trust in respondents' experiences.

Against this backdrop, interview respondents were asked what transparency-enhancing measures they mostly rely on. The most common answers were "full pricing", "contract summaries" and "inventories of data processing steps". However, most respondents were not able to guarantee that these inventories are always easily understandable for business partners and customers. In this view, respondents have acknowledged that the complexity of inventories and contract summaries is a possible burden to bringing forth actual transparency. The Safe-DEED solutions in chapter 3 will take this insight into account.[110] Concretely, the proposed transparency principle of the codes of conduct will expand upon the importance of clear and

[107] Safe-DEED Survey on "Trust in a Data Market context", question: *"Do you consider transparency measures such as full pricing, visible inventory, clear and understandable contract summaries as important factors for increasing your trust in a platform (5 meaning the most important and 1 meaning the least important)"*, 53 answers were given, with an average rating of 4.2, Answer breakdown: "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (5 respondents, 9.4%); "4" (10 respondents, 18.9%); "5" (38 respondents, 71.1%).

[108] Safe-DEED Survey on "Trust in a Data Market context", question: *"Would you agree with the following statement: within a B2B platforms environment, measures that enhance transparency are important for generating consumers' trust*", 53 answers were given, with an average rating of 8.6 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (0 respondents, 0.0%); "4" (0 respondents, 0.0%); "5" (2 respondents, 3.8%); "6" (1 respondent, 1.9%); "7" (8 respondents, 15.1%); "8" (11 respondents, 20.8%); "9" (13 respondents, 24.5%); "10" (18 respondents, 34.0%).

[109] Safe-DEED Survey on "Trust in a Data Market context", question: *"Would you agree with the following statement: within a B2C platforms ecosystem, the enhancement of transparency measures, such as peers identity and business activities, can increase consumers' trust and consequently boost platform peers business opportunities*", 53 answers were given, with an average rating of 7.7 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (0 respondents, 0.0%); "4" (1 respondent, 1.9%); "5" (5 respondents, 9.4%); "6" (6 respondent, 11.3%); "7" (14 respondents, 26.4%); "8" (9 respondents, 17.0%); "9" (8 respondents, 15.1%); "10" (10 respondents, 18.9%).

[110] *Infra* 3. The enhancement of organizational trust in data marketplaces.

intelligible language.[111]

Moreover, most interview respondents have asserted that monitoring subcontractors' activities improves perceived trust, despite the ensuing enhanced transparency on contractors' conduct. This insight indicates that not every form of transparency evenly adds to trust. The survey and interviews have namely shown that *de priori* transparency (i.e. trustees' transparent policies) outspokenly affects businesses' trust, whilst *ex post facto* transparency (i.e. transparency as a result of monitoring or auditing by trustors) has a lesser impact on organizational trust. The Safe-DEED solutions will therefore aim to facilitate and promote transparent policies in the data market context.

Furthermore, the antecedent of "management measures and competence" can also be demonstrated by reference to the survey findings. The question "*Do you consider data management measures as an important factor for increasing your trust in a platform*" received an average rating of 4/5.[112] As can be denoted whilst consulting the answer breakdown[113], the responses to this question were quasi-perfectly divided between 3/5, 4/5 and 5/5. This relatively gradual division of responses is in stark contrast with the foregoing outspoken "5/5" votes on the importance of transparency as a factor of trust (71.7% of all votes). This comparison indicates that transparency measures are generally perceived as more trust-enhancing than data management measures, though both positively impact organizational trust.

A final subgroup of business-related qualifications includes the "external characteristics to the organization". These are overarching elements that are excluded from the organization's control and predominantly relate to a market or a sector as a whole. This subgroup entails antecedents such as the competition on the market[114], government policies[115] and market stability[116]—nevertheless, the Safe-DEED survey findings nuance the impact of some of these external

[111] *Infra* 3.3.2. Transparency.
[112] Safe-DEED Survey on "Trust in a Data Market context", question: *"Do you consider data management measures as an important factor for increasing your trust in a platform (5 meaning the most important and 1 meaning the least important)"*, 53 answers were given, with an average rating of 4.0, Answer breakdown: "1" (0 respondents, 0.0%); "2" (2 respondents, 3.8%); "3" (15 respondents, 28.3%); "4" (17 respondents, 32.1%); "5" (19 respondents, 35.8%).
[113] *Ibid.*
[114] Evelien Croonen, 'Trust and fairness during strategic change processes in franchise systems' (2010) 95 Journal of Business Ethics 191.
[115] Helle Neergaard, John Ulhoi, 'Government agency and trust in the formation and transformation of interorganizational entrepeneurial networks' (2006) 30(4) Entrpeneurship: Theory and Practice 519.
[116] Randy Hodson, 'Organizational Trustworthiness: findings from the population of organizational ethnographies' (2004) 15(4) Organization Science 432.

factors. Most respondents have namely asserted that the industry in which a partner operates is no precondition of trust.[117]

[117] Safe-DEED Survey on "Trust in a Data Market context", question: "*Would you consider the industry in which a partner operates as an important factor for trusting this partner?.",* 10 answers were given, answer breakdown: "yes" (3 respondents, 30.0%); "no" (7 respondents, 70.0%).

2.1.1.4. Schedule

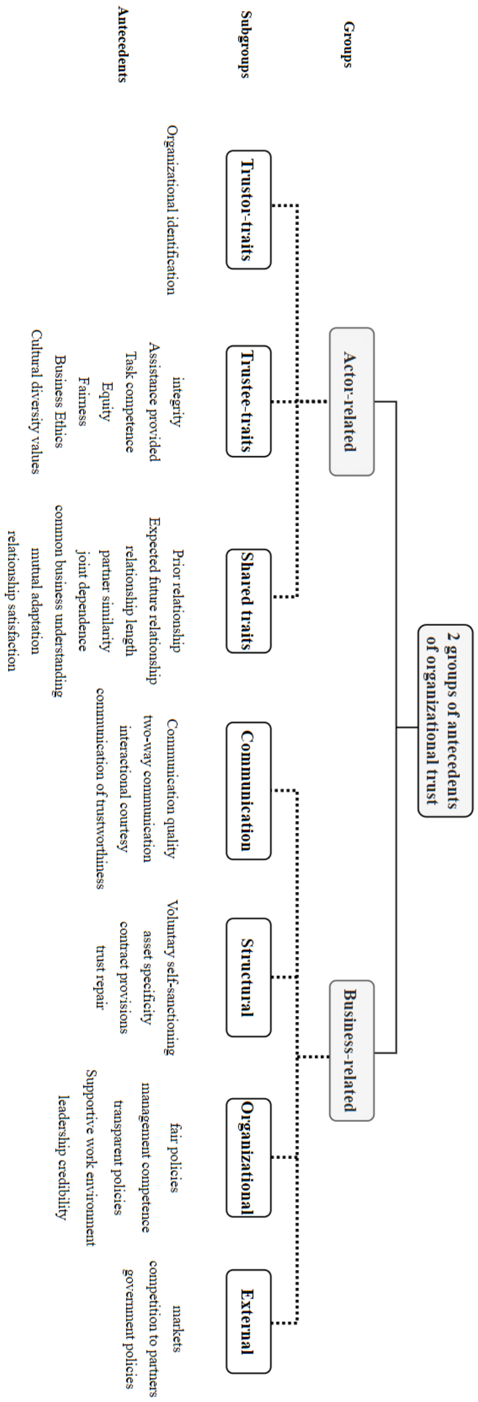

Figure 2. Antecedents of organizational trust [118]

[118] Figure made by KUL (WP3), as part of the Safe-DEED research on organizational trust in D3.7. Principally based upon the classification in: Ashley Fulmer, Michele Gelfand, 'At what level (and in whom) do we trust: trust across multiple organizational levels' (2012) 38(4) Journal of Management 1167, 1180.

2.1.2. Consequences

2.1.2.1. Overview

Once an ample degree of trust has been established, what consequences arise from this trust-enhanced B2B relation should be addressed. In the first place, this elementary overview aims to provide an insight in some predominant consequences. A subsequent part will classify these consequences, followed by visualization in a schedule. The structure of this part thus mirrors the structure of the preceding subchapter.

Firstly, a high level of organizational trust has been proven to ease the introduction of organizational change.[119] Furthermore, a trust-based relationship has been demonstrated to encourage knowledge-sharing, especially when the insight is tacit or sensitive.[120] Moreover, trust-facilitated knowledge-sharing becomes increasingly important when organizations are high on interdependence and competitive environment.[121]

Furthermore, collective perceptions that the organization is trustworthy can decrease internal conflicts. Such a downfall of conflicts enhances - among other things[122] - contract flexibility[123], decreased negotiation costs[124], contract compliance[125], willingness to cooperate[126], positive

---

[119] Karan Sonpar, Jay Handelman, Ali Dastmalchian, 'Implementing new institutional logics in pioneering organizations: the burden of justifying ethical appropriateness and trustworthiness' (2009) 90 Journal of Business Ethics 345.

[120] Heli Wang, Jinyu He, Joseph Mahoney, 'Firm-specific knowledge resources and competitive advantage: the roles of economic- and relationship-based employee governance mechanisms' (2009) 30 Strategic Management Journal 1265; Amy Pablo, Trish Reay, Ann Casebeer, Jim Dewald, 'Identifying, enabling and managing dynamic capabilities in the public sector' (2007) 44 Journal of management studies 687.

[121] Karan Sonpar, Jay Handelman, Ali Dastmalchian, 'Implementing new institutional logics in pioneering organizations: the burden of justifying ethical appropriateness and trustworthiness' (2009) 90 Journal of Business Ethics 345.

[122] Ashley Fulmer, Michele Gelfand, 'At what level (and in whom) do we trust: trust across multiple organizational levels' (2012) 38(4) Journal of Management 1167.

[123] Dries Faems, Maddy Janssens, Anoop Madhok, Bart van Looy, 'Toward an integrative perspective of alliance governance: connecting contract design, trust dynamics, and contract application' (2008) 51 (6) The Academy of Management Journal 1053.

[124] Akbar Zaheer, Bill McEvily, Vincenzo Perrone, 'Does trust matter? Exploring the effects of inter-organizational and inter-personal trust on performance' (1998) 9 (2) Organization Science 141.

[125] Mark Davies, Walfried Lassar, Chris Manolis, Melvin Prince, Robert Winsor, 'A model of trust and compliance in franchise relationships' (2011) 26 Journal of business venturing 321.

[126] Günter Stahl, Rikard Larsson, Ina Kremershof, Sim Sitkin, 'Trust dynamics in acquisitions: a case study' (2011) 50Human Resource Management 575.

interaction patterns[127], and continued cooperation.[128] In addition, the presence of trust-enhancing antecedents may result in continuous business relation despite possible failures.[129] Lastly, it has been asserted that trust increases overall performance on the trustee's side, which may materialize in improved marketing performances[130], organizational adaptability[131] and innovation[132], amongst others.

2.1.2.2. Classification

2.1.2.2.1. Groups

The consequences of organizational trust may be classified into five main groups. In their turn, these groups do not comprise any subgroups, as opposed to cataloguing the antecedents *supra*. Hence, each group directly encompasses several particular consequences. These groups are:

- (I) attitudes and preferences,
- (II) knowledge sharing and organizational learning,
- (III) communication, cooperation and conflicts,
- (IV) viability and,
- (V) performance.

"Attitudes and preferences" is the first group of consequences. A relationship of trust has been shown to add to a trustor's attitude vis-à-vis the trustee, which may materialize as an increased willingness to support the trustee[133]or an improvement in relationship satisfaction[134]. Concurrently, however, trust equally adds to preferential and attitudinal alterations on the trustee's side.[135] This may result in a more outspoken ease to introduce organizational change,

---

[127] Augustine Lado, Rajiv Dant, Amanuel Tekleab, 'Trust-opportunism paradox, relationalism and performance in interfirm relationships: evidence from the retail industry' (2008) 29(4) Strategic Management Journal 401.

[128] Deepak Malhotra, Fabrice Lumineau, 'Trust and collaboration in the aftermath of conflict: the effects of contract structure' (2011) 54 Academy of Management Journal 981.

[129] Holger Patzelt, Dean Shepherd, 'The decision to persist with underperforming alliances: the role of trust and control' (2008) 45 Journal of Management Studies 1217.

[130] Robert Audi, 'Some dimensions of trust in business practices: from financial and product representation to licensure and voting' (2008) 80 Journal of business ethics 97.

[131] Cristina Gibson, Julian Birkinshaw, 'The antecedents, consequences and mediating role of organizational ambidexterity' (2004) 17 (2) The academy of management journal 209.

[132] Xavier Molina-Morales, Teresa Martinez-Fernandez, 'Too much love in the neighborhood can hurt: how an excess of intensity and trust in relationships may produce negative effects on firms' (2009) 30 Strategic Management Journal 1013.

[133] Wei-ping Wu, 'Dimensions of social capital and firm competitiveness improvement: the mediating role of information sharing' (2007) 45 Journal of Management Studies 122.

[134] Thomas Gainey, Brian Klaas, 'The outsourcing of training and development: factors impacting client satisfaction' (2003) 29(2) Journal of Management 207.

[135] Ashley Fulmer, Michele Gelfand, 'At what level (and in whom) do we trust: trust across multiple organizational levels' (2012) 38(4) Journal of Management 1167.

as mentioned *supra*[136].[137]

A second group includes consequences in the domain of knowledge-sharing and organizational learning. A certain degree of trust has been shown to substantiate both parties' willingness to share insights.[138] This willingness may give rise to a tendency to disseminate and accumulate business-specific knowledge resources more unreservedly.[139] On an inter-organizational level, trust has also been demonstrated to enhance knowledge-sharing.[140] Nonetheless, - as stated *supra*[141] – this research scrutinizes the enhancement of external parties' trust in data marketplaces. Therefore, inter-organizational consequences will not be assessed in the remaining chapters of this deliverable.

A third group concerns the so-called "three C's" (i.e. communication, cooperation and conflicts). This group includes consequences on the relational level. On the external relational level (i.e. the relation between trustee and trustor), trust diminishes conflicts in negotiation[142], which in its turn generates overall reduced transaction costs[143], and asserts positive interaction patterns throughout the ensuing B2B relationship[144]. Other related consequences concern an augmented willingness to cooperate[145], and more chances of continuous collaboration in the longer term[146]. On the internal relational level, trust has been exhibited to reduce conflicts

[136] *Supra*. 2.1.1.1. "Overview".
[137] Karan Sonpar, Jay Handelman, Ali Dastmalchian, 'Implementing new institutional logics in pioneering organizations: the burden of justifying ethical appropriateness and trustworthiness' (2009) 90 Journal of Business Ethics 345.
[138] Ashley Fulmer, Michele Gelfand, 'At what level (and in whom) do we trust: trust across multiple organizational levels' (2012) 38(4) Journal of Management 1167.
[139] Heli Wang, Jinyu He, Joseph Mahoney, 'Firm-specific knowledge resources and competitive advantage: the roles of economic- and relationship-based employee governance mechanisms' (2009) 30 Strategic Management Journal 1265.
[140] Dirk De Clerq, H.J. Sapienza, 'When do venture capital firms learn from their portfolio companies?' (2005) 29 Entrepeneurship: theory and practice 517; Bo Bernhard Nielsen, Sabina Nielsen, 'Learning and innovation in international strategic alliances: an empirical test on the role of trust and tacitness' (2009) 46 (6) Journal of Management Studies 1031.
[141] *Supra*. 2.1. "Organizational Trust".
[142] Akbar Zaheer, Bill McEvily, Vincenzo Perrone, 'Does trust matter? Exploring the effects of inter-organizational and inter-personal trust on performance' (1998) 9 (2) Organization Science 141.
[143] Jeffrey Dyer, Wujin Chu, 'The role of trustworthiness in reducing transaction costs and improving performance: empirical evidence from the United States, Japan and Korea' (2003) 14 Organization Science 57.
[144] Steven Lui, Yue Ngo Hang, 'An action pattern model of inter-firm cooperation' (2005) 42 Journal of Management Studies 1123.
[145] Günter Stahl, Rikard Larsson, Ina Kremershof, Sim Sitkin, 'Trust dynamics in acquisitions: a case study' (2011) 50Human Resource Management 575.
[146] Michael Jensen, 'The role of network resources in market entry: commercial banks' entry into investment banking, 1991-1997' (2003) 48 Administrative Science Quarterly 466.

between employees and management.[147]

A fourth group includes viability-consequences. These aspects revolve around commitment and overall turnover on the trustee's side. As stated *supra*[148], a particular consequence within this group concerns the continuity of business relations between both parties, even in spite of possible hurdles and business failures along the way.[149]

A final group is performance-based. Hence, a degree of trust has a specific impact on organizations' overall economic performance. The concrete consequences within this group comprise *inter alia* an increased level of innovation[150], marketing success[151] and organizational adaptability.[152]

2.1.2.2.2. Nuancing observations

Two overarching observations should be stressed at this stage. Firstly, the group division of both consequences and antecedents is merely theoretical and intends to provide a degree of structure in this assessment. In practice, the various (sub-)groups of antecedents are interlinked, all the while the groups of consequences are equally correlated with one another. The consequence of organizational adaptability, for instance, strongly correlates with the "ease of introducing organizational change". By the same token, the antecedent of "voluntary self-compliance" naturally goes along a proficient degree of leadership credibility and integrity.

A second general remark concerns the limits of trust. Whilst the consequences mentioned above are generally positive elements, an overabundance of trust may in fact be detrimental on the organizational level. Too much trust may result in a reluctance to adequately realize the opposing party's failures or managerial flaws.[153] In this sense, it has been discerned that an outspoken degree of organizational trust may result in unfavourable consequences, such as

---

[147] Randy Hodson, 'Organizational Trustworthiness: findings from the population of organizational ethnographies' (2004) 15(4) Organization Science 432.
[148] *Supra*. 2.1.1.1. "Overview".
[149] Holger Patzelt, Dean Shepherd, 'The decision to persist with underperforming alliances: the role of trust and control' (2008) 45 Journal of Management Studies 1217.
[150] Xavier Molina-Morales, Teresa Martinez-Fernandez, 'Too much love in the neighborhood can hurt: how an excess of intensity and trust in relationships may produce negative effects on firms' (2009) 30 Strategic Management Journal 1013.
[151] Robert Audi, 'Some dimensions of trust in business practices: from financial and product representation to licensure and voting' (2008) 80 Journal of business ethics 97.
[152] Cristina Gibson, Julian Birkinshaw, 'The antecedents, consequences and mediating role of organizational ambidexterity' (2004) 17 (2) The academy of management journal 209.
[153] Keith Blois, 'Is it commercially irresponsible to trust?' (2003) 45 Journal of Business Ethics 183.

stunting economic growth.[154] Though an overabundance of trust mainly thwarts economic growth on the inter-organizational level, these disapproving effects equally hamper trust between external organizations.[155] Therefore, research has shown that an inverted U-shape can best visualize the relationship between organizational trust and organizational innovation.[156]

2.1.2.3. Schedule

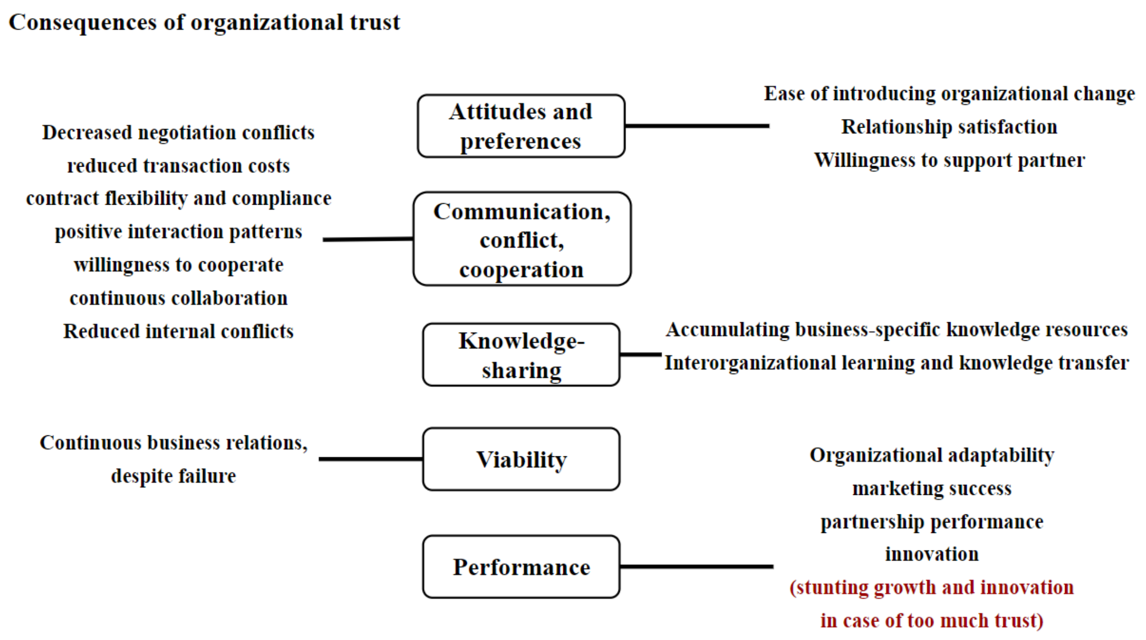

Figure 3. Consequences of organizational trust[157]

[154] Randall Morck, Bernard Yeung, 'Family control and the rent-seeking society' (2004) 28 Entrepreneurship: theory and practice 391.
[155] Ashley Fulmer, Michele Gelfand, 'At what level (and in whom) do we trust: trust across multiple organizational levels' (2012) 38(4) Journal of Management 1167.
[156] Xavier Molina-Morales, Teresa Martinez-Fernandez, 'Too much love in the neighborhood can hurt: how an excess of intensity and trust in relationships may produce negative effects on firms' (2009) 30 Strategic Management Journal 1013.
[157] Figure made by KUL (WP3), as part of the Safe-DEED research on organizational trust in D3.8. Principally based upon the classification in Ashley Fulmer, Michele Gelfand, 'At what level (and in whom) do we trust: trust across multiple organizational levels' (2012) 38(4) Journal of Management 1167, 1180.

2.2. Organizational trust in data marketplaces: digital trust

In the Safe-DEED survey, e-trust was defined as *"the notion of trust described above in the online environment. More precisely, "e-trust occurs in an environment where direct and physical contacts do not take place, moral and social pressures can be differently perceived, and where interactions are mediated by digital devices".* Two respondents had reservations about this working definition, though no proposed adaptations were made on their behalf.[158]

Though the reasoning behind these two reservations is not known, the semi-structured interviews have further elucidated the respondents' definitional apprehensions. All respondents agreed that the working definition of "trust in an online environment" has changed. Specifically, respondents argued that the data economy has become more complex, ubiquitous and competitive. As a result, respondents acknowledged that digital trust relies on a growing number of elements. One respondent elaborated that many data processing activities have gotten much more complicated over the past years, making it harder for companies to be transparent and compliant with data protection laws. According to all respondents, the benchmark to foster trust in the data economy has therefore considerably risen.

One respondent added that preventing security issues has become a much more prevalent antecedent to trust, especially in the smart manufacturing sector. In this context, all respondents agreed that security – alongside transparency – is the most vital mechanism to ensure trust in their experience. Two respondents also stated that preventing security- and privacy issues have come to the forefront in safeguarding trust. Against this backdrop, the Safe-DEED solutions in chapter 3 will – *inter alia* - propose PETs (i.e. MPC encryption) as a means to enhance organizational trust in data marketplaces.[159] Moreover, given the growing importance of security measures to ensure digital trust, the proposed codes of conduct in chapter 3 will equally implement security-enhancing best practices.[160]

Following the rapidly changing nature of the concept of digital trust, this subchapter will not attempt to present a static definition of trust in data marketplaces. Instead, this analysis will scrutinize the most predominant antecedents to organizational trust in data marketplaces. Before doing so, the main actors in the trust relationship will be discussed.

[158] Safe-DEED Survey on "Trust in a Data Market context", question: "Do you agree with the following working definition of e-trust: *The term encompasses the notion of trust described above in the online environment. More precisely, "e-trust occurs in an environment where direct and physical contacts do not take place, moral and social pressures can be differently perceived, and where interactions are mediated by digital devices"*." 10 answers were given, answer breakdown: "yes" (8 respondents, 80.0%) "no" (2 respondents, 20.0%).
[159] *Infra* 3.2 Privacy-and Security-enhancing Technologies.
[160] *Infra* 3.3.3. Security.

2.2.1. Actors

As touched upon *supra*, the European Union has acknowledged the growing need to foster trust amongst the actors involved in data marketplaces.[161] The main actors in this context are (I) data providers and (II) data users (i.e. "data consumers"; these terms are used interchangeably). Both data providers and data users can be regarded as external "trustors", whilst the platform controller (i.e. the data marketplace provider) is the "trustee". Other actors, such as complementary service providers[162], can be classified as "trustors" on the inter-organizational level. As stated before, however, the scope of this research is limited to the fostering of external organizational trust.

Nonetheless, the role of complementary service providers may not be overlooked in this context either, since these providers play a role in ensuring trust amongst data providers and data users. Hence, complementary service providers have a twofold role in the trust context: they are an external trustee vis-à-vis the data provider and data user, though internally serve as a trustor of the data marketplace provider. However, given those data providers and data users are the central actors in the data exchange, the remainder of this research will focus on these actors and organizational trust in the external sense.

At this point, however, this latter divergence between external and internal organizational trust should be nuanced. As stated, data providers and data users are essentially external actors to the marketplace. Nevertheless, these parties are also internal actors on the platform. In the data marketplace setting, the distinction between internal and external organizational trust is thus not as outspoken - nor as pivotal - as in other frameworks.

2.2.2. Antecedents

Several antecedents of trust have been outlined in the previous part of this chapter.[163] The following assessment will apply these antecedents to the particular data marketplace context whilst expanding upon their relevance for fostering data users' providers' organizational trust in data marketplaces.

First is the antecedent of organizational identification, which has been defined as "*the propensity of a member of an organization to identify with that organization*".[164] Hence, the more a data user or data provider is inclined to identify with a data marketplace, the more

[161] *Supra* 1.1. "A European Single Data-market".
[162] *i.e.* providers of services such as data aggregation, data analysis or data visualization.
[163] *Supra*. 2.1.1. "Antecedents".
[164] Stuart Albert Blake Ashforth, Jane Dutton, 'Organizational Identity and Identification: charting new waters and building new bridges' (2000) 25(1) The Academy of Management Review 13.

likely they will trust the platform. Common factors of such identificatory inclination include: (I) organizational support, (II) communication, and (III) organizational prestige.[165] In the data marketplace context, these factors may respectively take the form of (I) clear organizational support for both data user and provider, (II) coherent communication on the data sharing processes, and (III) the overall reputation of the platform.

Integrity has been described as another noteworthy antecedent. Hence, there may be a need for a standardized code of conduct applicable in the data market context, which could be rooted in integrity-inducing ethical guidelines, as covered in Safe-DEED deliverable D3.1-D3.5, which may be consulted here.

Such a code of conduct may also enhance leadership credibility (i.e. credibility ofdata market platform controllers). Furthermore, a code of conduct may undeniably bring forth an equal level playing field between the trustees and the trustor, adding to their common business understanding. Concretely, a code of conduct may enhance the conviction amongst data providers and data users that they are at an equal stance vis-à-vis the data market provider while sharing and buying data in an integer setting. In addition, the principle of integrity has been laid down in Art 5(1) (f) of the GDPR.[166] In this article, integrity, security, and confidentiality are closely interlinked and bestow upon the controller and processor the general obligation to "*ensure appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures*".[167] The scope of this general principle has been further expanded upon in Art 24 GDPR and Art 32 GDPR.[168] The latter article clarifies that "*appropriate technical or organizational measures*" may include the pseudonymization and encryption of personal data.[169] To safeguard trust-enhancing integrity in the data marketplace context, it is, therefore, necessary to ascertain in each case whether the GDPR applies. Concretely, providers should thus assess whether the data exchange on the marketplace can be classified as the processing of personal data, according to Art 2(1) GDPR.

Furthermore, Art 24 GDPR once again reaffirms the potential value of privacy- and security-preserving techniques because of the enhancement of organizational trust. Therefore, this preliminary assessment underlines the importance of legal certainty and encryption in

[165] Daniel Cable, Jeffrey Edwards, 'Complementary and supplementary fit: a theoretical and empirical integration' (2004) 89 Journal of Applied Psychology 822.
[166] Regulation (EU) 2016/679 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) [2016] OJ L 119 4.5.2016, Art 5.
[167] *Ibid*.
[168] *Ibid*. Art 24, Art 32.
[169] *Ibid*.

safeguarding integrity, amongst other trust-fostering antecedents. The following chapter will deal with these elements in more depth.[170]

Another antecedent group concerned "communication". In this view, a clear and visual outline of the data sharing process and precise communication on complementary service providers' role and involvement are fundamental. This need for a clear outline goes along with the understanding that organizational characteristics (e.g. fair, coherent, and transparent policies) add to trust. The impact of this antecedent on digital trust-building in data marketplaces cannot be overlooked. The digital economy is namely increasingly marked by a deepening information asymmetry between data controllers on the one hand, and data subjects on the other hand. This asymmetry can be most noticeably discerned in the informational divergence between data subjects and gatekeepers.[171]

The EU has asserted to lift some of these asymmetries in occasions where gatekeepers provide "core platform services", including online intermediation services.[172] According to the latter, the EU's Digital Markets Act (hereafter: "DMA")[173] thus equally seems to apply vis-à-vis large data market providers that fall within the scope of Art 3 of the DMA.[174] Hence, the inclusion of 'online intermediation services" in Art 2(2)(a) of the DMA seems to indicate the EU's acknowledgement of the existing informational discrepancies and power asymmetries between the data market provider on the one hand, and data providers and data users on the other hand. Moreover, this informational divergence has been shown to impact subjects' trust in all organizations, regardless of whether the latter can be classified as a gatekeeper.[175] This level of distrust can be expected to be higher when the data user or providers suspects that the data marketplace provider intentionally attempts to uphold this informational asymmetry.[176] Hence, clear communication on the precise data sharing processes, in conjunction with a code of conduct marked by fairness and transparency, seems vital to foster external parties' trust in the data marketplace.

170 *Infra*. Chapter 3.
171 Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) [2020] COM/2020/842 final, Art 2(1), Art 3.
172 *Ibid*. Art 2(2).
173 *Ibid*.
174 *Ibid*. Art 3.
175 Melissa Graebner, 'Caveat venditor: trust asymmetries in acquisitions of entrepreneurial firms' (2009) 52 Academy of Management Journal 435; Roberto Hernan Gonzalez, Praveen Kujal, 'Trust and trustworthiness under information asymmetry and ambiguity' (2017) 147 Economics Letters 1.
176 *Ibid*.; Frank Pasquale, *The Black Box Society: the secret algorithms that control money and information* (1st edn, Harvard University Press 2016); Rana Foroohar, *Don't be evil: the case against big tech* (1st edn, Allen Lane Penguin Random House UK 2019).

Another antecedent concerned "asset specificity".[177] This element entails that data marketplaces should limit how data can be transferred to restrict unwarranted data sharing scenarios.[178] Against this backdrop, such limitation seems to necessitate the use of security- and privacy-enhancing technologies (PETs). Moreover, applying the GDPR to a concrete data sharing scenario could argue that purpose-limitation Art 5(1)(b) GDPR governs such scenarios.[179] This principle asserts that personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".[180] Suppose the exchange of data on the marketplace can be categorized as the processing of personal data under Art 2(1) GDPR. In that case, it could be argued that the trust-enhancing antecedent of "asset specificity" can be legally enforced under Art 5(1)(b) GDPR.

It has equally been asserted that economically unstable sectors or failing markets negatively impact organizational trust. Still, instability does not seem to be of utmost relevance in the data market context, given that the business of data sharing is unequivocally expected to gain economic weight ona global scale. Nonetheless, the assurance of other external antecedents may be less self-evident. Besides general market conditions, factors such as government policies namely equally impact the enhancement of trust. Against this backdrop, the enhancement of organizational trust thus seems to necessitate clear and coherent regulatory action.

2.2.3. Consequences

The antecedents summed up in the previous subsection may irrefutably foster organizational trust in data marketplaces, both amongst data providers and data users. It has – amongst others - been shown that an interdependent and competitive business environment enhances trust. In the data market context, strong business competition and interdependence are usually clearly present. Moreover, it has been mentioned that a high level of trust eases the introduction of organizational change. This is an important insight, given that in a rapidly evolving data market, swift organizational adaptations are crucial.

In addition, the consequence of "knowledge-sharing and organizational learning" cannot be overlooked in the rapidly evolving data-driven market. Hence, the more a data provider trust

[177] *Supra*. 2.1.1.1. "Overview".

[178] Constantine Katsikeas, Dionysis Skarmeas, 'Developing successful trust-based international exchange relationships' (2009) 40(1) Journal of International Business Studies 132; Thomas Gainey, Brian Klaas, 'The outsourcing of training and development: factors impacting client satisfaction' (2003) 29(2) Journal of Management 207.

[179] Regulation (EU) 2016/679 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) [2016] OJ L 119 4.5.2016, Art 5.

[180] *Ibid*.

the data market platform, the more inclined this actor will be to share higher volumes and varieties of datasets on the marketplace. The "knowledge transfer" implies clear-cut economic benefits for the data marketplace provider, which could serve as an incentive to guarantee an environment of trust. Furthermore, the relevance of the three C's (i.e. communication, conflict & cooperation) cannot be understated either. As asserted, an adequate degree of trust correlates with reduced transaction costs and an increased willingness to cooperate. Given the former, a trusted data marketplace may thus be expected to bring forth economic benefits for both data providers and data users.

Both the consequences of "willingness to contribute" and "continuous collaboration" suggest a higher relational retention rate, which in its turn is predominantly positive for the data marketplace provider. Moreover, trust has been shown to augment contract flexibility and decreased conflicts both prior to the B2B relation (i.e. during the negotiation phase) as well as during the subsequent stages (i.e. "positive interaction patterns" and "contract flexibility and compliance").[181] Against this backdrop, trust thus seems to enhance relational flexibility.

Nonetheless, this consequence – as with all other consequences - should be assessed in conjunction with all other trust-related elements. A lack of a coherent legal framework or of a code of conduct may deter any relational flexibility.

It should be reiterated that neither antecedents nor consequences should be assessed in an abstraction of other trust-impacting elements. Henceforth, enhancing organizational trust calls for a comprehensive approach, taking into account all antecedents of trust, while outweighing the various group-transcending consequences. Such an overarching resolution shall be presented in the next chapter of this deliverable.

3. The enhancement of organizational trust in data marketplaces

3.1. Two pillars

The previous chapter has outlined the main antecedents and consequences of organizational trust. In addition, these elements have been applied to the particular data market context. This final chapter will analyze how the antecedents of organizational trust may be fostered in the data markets framework.

Moreover, the various antecedents were grouped into two chief categories: actor- and business-

[181] *Supra*. 2.1.1.1. "Overview".

related characteristics. In its turn, the first group comprised several subgroups. Irrespective of this theoretical classification, it has been asserted that these trust-enhancing antecedents are heavily interlinked and should be assessed in an all-embracing manner. Following this insight, it was concluded that enhancing trust starkly relies upon a comprehensive approach that transcends each particular (sub)group.

Furthermore, the Safe-DEED survey and interviews have shown that digital trust is a dynamic concept, though fundamentally relies on security and transparency. Furthermore, the attested value of due diligence and personal engagement have showcased the importance of fairness and neutrality in generating trust.

The following analysis shall make a distinction between two particular methods to enhance trust in the data market context: (I) the implementation of privacy- and security-enhancing technologies, (II) and the use of codes of conduct. The ensuing subchapters shall respectively elaborate upon each pillar whilst building further upon the insights gathered from the fundamental research, the survey and the semi-structured interviews, as outlined in the previous chapter.[182]

Concurrently, these trust-enhancing methods will be mirrored against the EU's most recent regulatory actions in ascertaining trust in data marketplaces. In this light, the EU's Digital Strategy (and in particular the EU's novel Data Governance Act (hereafter: "DGA")) will be scrutinized.[183] This particular analysis should allow for a better understanding of the practical viability of each trust-enhancing method against the backdrop of the EU's envisioned approach to data governance.

3.2. Privacy- and security-enhancing technologies (PETs)

3.2.1. Secure Multi-Party Computation and Organizational Trust

Secure multi-party computation (hereafter "MPC") is a subfield of cryptography, the utility of which has been comprehensively assessed throughout the Safe-DEED research. In particular, WP2 and WP5 have extensively analyzed the development of new multi-party computational methods that require creating a multi-party platform.[184]

In essence, the use of MPC intends to safeguard both privacy- and security concerns, both amongst data users and data providers. Lifting these concerns has proven to ease the

[182] *Supra* 2. The concept of organizational trust.
[183] Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act) [2020] COM(2020) 767 final.
[184] For more information, please consult Safe-DEED deliverables D2.1-D2.7 and D5.1-5.12 here.

development of organizational trust among both trustors[185], like privacy- and security-preservation correlate with various antecedents of trust.[186] Firstly, the use of MPC facilitates asset specificity.[187] As stated before, the latter implies that invested assets cannot be easily transferred.[188] In the data market context, these assets are data in the form of datasets that are exchanged on the platform. The use of MPC prevents these data from being acquired by adversaries, which enhances asset specificity. The GDPR also includes asset specificity under the veil of "purpose limitation" in Art 5(1)(b).[189] Nevertheless, there are multiple instances in which the GDPR does not apply to share a particular dataset on the data market platform. These instances include occasions where the dataset falls outside the scope of Art 2 GDPR or in other cases of legal uncertainty, where the applicable legal framework remains ambiguous in a concrete case. [190] Despite these nuances, the use of MPC ensures a certain degree of asset specificity, which in its turn implies purpose limitation, even in instances where the eponymous legal principle in Art 5(1) (b) GDPR may not apply.[191] In this sense, one should not overlook the use of MPC encryptionprotocol because of ensuring trust-enhancing structural characteristics.

In addition, the use of MPC encryption adds to the overall perceived fairness of the data exchange, as no adversaries can be expected to acquire datasets.[192] Such perceived fairness may, in its turn, positively impact certain trustee characteristics, amongst which business ethics, equity and integrity[193], the latter of which also has a legal basis in the GDPR.[194]

Furthermore, Rec 83 of the GDPR calls for implementing security measures (including encryption) by controllers and processors.[195] This principle has also been adopted as an explicit

[185] Giovanni Sartor, 'Privacy, Reputation and Trust: Some Implications for Data Protection' in Ketil Stolen, William Winsborough, Fabio Martinelli, Fabio Massacci (eds), *Trust Management. iTrust 2006. Lecture Notes in Computer Science* (vol 3986 Springer Publishing 2006).
[186] *Supra*. 2.1.1.1. "Overview".
[187] Thomas Gainey, Brian Klaas, 'The outsourcing of training and development: factors impacting client satisfaction' (2003) 29(2) Journal of Management 207.
[188] *Supra*. 2.1.1.1. "Overview".
[189] GDPR Art 5.
[190] *Ibid*. Art 2.
[191] *Ibid*. Art 5(1) (b).
[192] Nicole Gillespie, Graham Dietz, 'Trust repair after an organization-level failure' (2009) 34 Academy of management review 127.
[193] Eva Kasper-Fuehrer, Neal Ashkanasy, 'Communicating trustworthiness and building trust in interorganizational virtual organizations' (2001) 27(235) Journal of Management 1; Lisa Scheer, Nirmalya Kumar, Jan-Benedict Steenkamp, 'Reactions to perceived inequity in US and Dutch interorganizational relationships' (2003) 46 Academy of Management Journal 303; Michael Palanski, Francis Yammarino, 'Integrity and leadership: a multi-level conceptual framework' (2009) 20 (3) The Leadership Quarterly 405.
[194] *Supra*. 2.1.1.2.2. "Actor-related Antecedents".
[195] GDPR Rec 83.

duty in Art 32(1)(a) of the GDPR.[196] The same encryption-implementing responsibility has been enshrined in the European Data Governance Act as well, though this recital merely applies to the prevention of unlawful access to non-personal data.[197]

Hence, in both personal and non-personal data exchange instances, the implementation of security-enhancing technologies has been embedded in the EU legal framework. By stressing the value of *inter alia* encryption of non-personal data in the recent DGA, the Union has clearly opted to reaffirm that preventing unlawful access is a duty inherent to all data exchanges, irrespective of the (non-)personal nature of the data. In previous 'European Digital Strategy' initiatives on the processing of non-personal data, such as the Free Flow of Non-Personal Data Regulation (hereafter: "FFNPDR"), neither the duty to prevent unlawful access, nor the necessity to adopt encryption were namely mentioned.[198] By affirming the importance of encryption in ensuring the lawful processing of both personal and non-personal data, the EU has now given a substantially broad scope to asset specificity in its legal framework. Hence, asset specificity is a crucial trust-enhancing antecedent, fostering equity, fairness and integrity.[199] A comprehensive approach to the principle of lawful access may therefore positively impact advancing trust in data marketplaces, irrespective of the nature of the data (i.e. personal or non-personal) that is being exchanged.

This value of security measures in fostering organizational trust has been affirmed in the Safe-DEED survey. The question raised was: "*Do you consider security measures such as the adoption of specific security standards as an important factor for increasing your trust in a platform? (5 meaning the most and 1 meaning the least important)*". Out of 53 respondents, the average score was 4.3/5, rating security measures as very important trust factors.[200] Furthermore, the vast majority of respondents (84.9%) acknowledged that in the B2B platforms' context, technical and organizational security measures are necessary to increase peers' trust and boost business opportunities.[201]

[196] GDPR Art 32.

[197] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) [2020] COM(2020) 767 final, Rec 18.

[198] Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (Free Flow of Non-personal Data Regulation) [2018] OJ L303/59.

[199] *Supra* 2.1.1.1. "Overview".

[200] Safe-DEED Survey on "Trust in a Data Market context", question: *"Do you consider security measures such as the adoption of specific security standards as an important factor for increasing your trust in a platform (5 meaning the most important and 1 meaning the least important)"*, 53 answers were given, with an average rating of 4.3/5, Answer breakdown: "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (11 respondents, 20.8%); "4" (13 respondents, 24.5%); "5" (29 respondents, 54.7%).

[201] Safe-DEED Survey on "Trust in a Data Market context", question: *"In the B2B platforms' context, technical and organizational security measures are a necessary precondition to increase peers' trust and consequently boost business opportunities*", 53 answers were given, with an average rating of 7.8 (0 meaning "I fully disagree" and

In sum, the use of MPC encryption marks a clear-cut antecedent to enhancing external parties' trust in a data market. Security- and privacy- measures such as encryption have namely been asserted to benefit asset specificity on the one hand and the principles of equity, fairness, business ethics and integrity on the other hand. Moreover, it has been discerned that all these antecedents have been given a legal basis in various European instruments focused on the development of a data-agile economy. In this regard, the introduction of the European Cybersecurity Act also clearly demonstrates the Union's acknowledgement of security-enhancing technologies' central role in furthering data-driven markets.[202]

3.2.2. Legal Certainty and Organizational Trust

3.2.2.1. MPC and trust: a double-edged sword

The EU legislator has also stressed encryption's role within the fostering of central principles such as the lawful processing of personal data, purpose limitation, and integrity. In their turn, all of these GDPR-principles have been recognized as trust-enhancing antecedents in the previous chapter of this deliverable.[203]

With regard to the lawfulness of the non-personal data processing, the EU has recently explicitly emphasized the role of encryption in Rec 18 DGA. Hence, the correlation between security-enhancing technologies and trust is now a legal basis for personal and non-personal data.

Notwithstanding this acknowledgement of trust-enhancing encryption measures in various legal instruments, it frequently remains ambiguous to what extent these frameworks apply to a specific scenario. The exchange of personal data on a marketplace may illustrate this sporadic ambiguity. If a data provider sells personal data on a marketplace, the GDPR principally applies.[204] During the transaction, the personal datasets will be encrypted pursuant to secure multi-party computation. Complementary service providers conduct this encryption, constituting the "processing" of personal data.

10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (1 respondents, 1.9%); "3" (1 respondents, 1.9%); "4" (1 respondents, 1.9%); "5" (3 respondents, 5.7%); "6" (2 respondents, 3.8%); "7" (13 respondents, 24.5%); "8" (11 respondents, 20.8%); "9" (12 respondents, 22.6%); "10" (9 respondents, 17.0%).

[202] Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15; For more information on the EU encryption framework and its role within the data economy, Safe-DEED deliverable D3.1 may be consulted here.

[203] *Supra* Chapter 2.

[204] GDPR Art 2.

Nevertheless, once the personal data gets encrypted with a random mask, the data ceases to be "personal" pursuant to Art 4(1) GDPR, as the identifiability-requirement is no longer fulfilled.[205] Hence, the subsequent aggregation of the masked datasets no longer falls within the material scope of Art 2 GDPR, as the dataset now concerns non-personal data. *A fortiori*, the GDPR's general principles of purpose limitation and lawfulness of processing can no longer be enforced.[206] With regard to this non-personal data, it has been stated that the antecedent of asset specificity has been acknowledged in the new DGA, though merely in a recital (i.e. Rec 18)[207], which does not have a similar legal standing compared to the enforceable general principles of the GDPR.

Following this, it may be argued that the use of MPC impedes the legal enforceability of asset specificity, which has been recognized as a vital trust-enhancing antecedent in the data market context. To a certain extent, the relationship between MPC encryption and organizational trust thus seems to be a double-edged sword. On the one hand, MPC (and privacy- and security-enhancing technologies in general) incontrovertibly enhance numerous trust-enhancing antecedents, thereby distinctly adding to external parties' trust in data marketplaces. On the other hand, the use of MPC creates ambiguity because of the applicable legal framework throughout the data exchange, which irrefutably impedes legal certainty, thus hampering organizational trust.

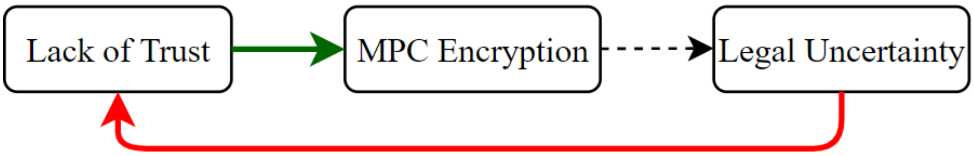

Figure 4. MPC and legal uncertainty[208]

3.2.2.2. Harmonization and trust

In the previous chapter, it has been denoted that external forces (i.e. the lack of clear policies and regulation) may hinder organizational trust. Therefore, this legal uncertainty may render the use of trust-enhancing security measures partially obsolete. In addition, it has been shown that even if it is known what legal framework applies, there are still discrepancies in the legal standing of some trust-enhancing antecedents, depending on whether the data exchange entails personal or non-personal data.[209]

[205] *Ibid*.
[206] *Ibid*. Art 5-6.
[207] DGA Rec 18.
[208] Figure made by KUL (WP3), as part of the Safe-DEED research on organizational trust in D3.7.
[209] *Supra* 2.2.2. "Antecedents": it has for instance been shown that "asset specificity" has been implemented in Art 5 and 6 of the GDPR, whereas the same antecedent has merely been acknowledged in a recital of the DGA with regard to non-personal data.

In the semi-structured interviews, the issue of legal uncertainty has been touched upon. Respondents were asked whether they believe legislation such as the GDPR offers them crucial support in their business practices. About half of the respondents (i.e. 7 out of 16 respondents) argued the contrary. According to them, the GDPR has rather overburdened their activities without adding value in terms of security. This apprehension has been voiced mostly by online service providers. To them, the GDPR's added value was mostly indirect, as GDPR compliance may raise customers' perception of the entity's trustworthiness. Smaller entities (i.e. less than fifty employees) have claimed that ensuring GDPR compliance often is complicated. This insight accentuates that clarity on the applicable legal rules is an essential prerequisite for any Safe-DEED solution proposed in this chapter. In addition, the double-edged relationship between MPC and organizational trust illustrates that the use of security-enhancing technologies *as such* does not suffice to safeguard external parties' trust in data marketplaces. There is an additional need for elucidation regarding the applicable legal framework in cases of MPC encryption.[210]

In the semi-structured interviews, some respondents (especially smaller service providers) claimed that distinguishing between personal and non-personal data is sometimes burdensome, as this discrepancy does not always coincide with data processing practices. One respondent substantiated that it is hard to make this distinction when data has been encrypted or pseudonymized. At what stage of the encryption/pseudonymization process does the data cease to be personal? And what legal rules apply to "mixed" datasets, entailing both personal and non-personal data? Against this backdrop, fostering trust in data marketplaces seems to rely on sufficiently harmonized rules and obligations vis-à-vis the data market provider, irrespective of the personal or non-personal nature of the dataset.

The European Union seems to acknowledge this present lack of legal certainty. In the DGA, the EU has affirmed that "*in order to increase trust in data sharing services, in particular related to the use of data and the compliance with the conditions imposed by data holders*[211]*, it is necessary to create a Union-level regulatory framework, which would set out highly harmonized requirements related to the trustworthy provision of such data sharing services. This will contribute to ensuring that data holders and data users have better control over the access to and use of their data, in accordance with Union law. Both in situations where data sharing occurs in a business-to-business context and where it occurs in a business-to-consumer context, data sharing providers should offer a novel, 'European' way of data governance(…)*".[212]

[210] In this view, the Safe-DEED consortium has already drawn up preliminary answers to several compelling legal questions on MPC use, which may be consulted here.
[211] The DGA uses the term "data holders" for "data providers". Both terms can be used interchangeably.
[212] DGA Rec 25.

The following subchapter will among other things, further assess the DGA, which may bring forth more clarity on what this so-called "European way of data governance" may entail and how this European approach may foster organizational trust.

3.3. Codes of Conduct

In the previous subchapter, it has been argued that the harmonization of trust-enhancing rules is of pivotal importance to effectuate more legal certainty in the data market context. In Rec 25 of the DGA, the EU has already hinted at the need for more harmonized rules on the trustworthy provision of data sharing services.[213] This necessity may materialize in a comprehensive code of conduct for data market providers and all other intermediaries. The EU has implicitly acknowledged the potential need for such a code of conduct in Rec 30 DGA, where it is accentuated that "*the benefits of a trustworthy data exchange environment would be best achieved by imposing a number of requirements for the provision of data sharing services, but without requiring any explicit decision or administrative act by the competent authority for the provision of such services*".[214]

Furthermore, the Safe-DEED survey included the question, "*What are the mechanisms that your organization uses within B2B platforms environments to agree upon the stakeholders' relations (obligation, rights, etc.) and to establish and/or increase trust between partners?*". The respondents unanimously acknowledged the value of both contracts or any type of formal agreement between the trustor and trustee that recognizes the terms governing their cooperation.[215] As codes of conduct constitute such formal agreements, the survey findings thus underline their possible value in fostering organizational trust. In addition, the Safe-DEED survey findings have demonstrated that standardizing such codes of conduct does not hamper their perceived trustworthiness.[216] This insight is highly relevant for advancing a trust-based

---

[213] DGA Rec 26.

[214] DGA Rec 30.

[215] Safe-DEED Survey on "Trust in a Data Market context", question: "What are the mechanisms that your organization uses within B2B platforms environments to agree upon the stakeholders' relations (obligations, rights, etc.) and to establish and/or increase trust between partners", 5 answers were given, answer breakdown: "a contract" (5 respondents, 100%); "any types of formal agreements between two or more parties that recognize the terms governing their cooperation" (5 respondents, 100%); "technical solutions" (3 respondents, 60%); "other" (0 respondents, 0.0%).

[216] Safe-DEED Survey on "Trust in a Data Market context", question: "Regarding a B2B platforms environment, if a developer/owner of a platform offered to your organization a standard form agreement for a certain service, would your organization consider this practice as untrustworthy?", 10 answers were given, answer breakdown: "no" (5 respondents, 50.0%); "not relevant, the existence of a standard form agreement is not related to the

European digital single market, as such standardization considerably increases the likelihood of the large-scale adoption of codes of conduct.

In the data market context, such a code may comprise four overarching elements: (I) fairness, (II) transparency, (III) security and (IV) neutrality. The remainder of this subchapter will briefly expand on these elements and their perceived impact on organizational trust in data marketplaces.

3.3.1. Fairness

Firstly, the principle of fairness entails that intermediaries ought to substantially balance the interests of all parties involved whilst processing the data exchange. In this sense, the code of conduct's fairness principle would *mutatis mutandis* mirror the substantive scope of the eponymous concept in Art 5(1)(a) GDPR.[217] Furthermore, the precise scope of the fairness principle may also be based upon the semantic notions of correctness, equitability and loyalty, which are all trust-enhancing antecedents[218] and have their roots in the Roman law notion of good faith (i.e. *bona fide*).[219] In both understandings of fairness in the GDPR and domestic traditions, fairness is effect-based.[220] In this view, fairness essentially does not depend on the formal respect for procedures but rather relies on mitigating other entities' vulnerabilities through specific safeguards and measures.[221]

This understanding of fairness safeguards the concept mentioned above of due diligence, which was defined as *"the care that a reasonable person exercises to avoid harm to other persons or their property"*.[222] As interview respondents deemed due diligence an essential trust-enhancing factor in the data market context, including a substantive fairness principle in the codes of conduct aims to safeguard due diligence.[223] Moreover, doctrine tends to put forward that substantive - rather than procedural - fairness is the most trust-generating in the B2B context.[224] The interview respondents' experiences of due diligence being a trust-enhancing

generation of trust between the parties" (3 respondents, 30.0%); "do not know" (2 respondents, 20.0%); "yes" (0 respondents, 0.0%); "other" (0 respondents, 0.0%).

217 GDPR Art 5.

218 *Supra* 2.1.1.1. "Overview".

219 Gianclaudio Malgieri, 'The concept of fairness in the GDPR: a linguistic and contextual interpretation' (2020) FACCT: Fairness, Accountability, and Transparency 154.

220 *Ibid*.

221 *Ibid*.; Damian Clifford and Jef Ausloos, 'Data Protection and the role of fairness' (2018) 37 Yearbook of European Law 130;

222 *Supra* 2.1.1.3.2. Actor-related antecedents; Merriam Webster, "Due Diligence" <www.merriam-webster.com/dictionary/due%20diligence> accessed 26 October 2021.

223 *Infra* 2.1.1.3.2. Actor-related antecedents.

224 *Ibid*.; Lee Bygrave, *Data Protection Law: Approaching its rationale, logic and limits* (The Hague Kluwer International 2002) 58: Tom Douglas, 'Biased Algorithms: here's a more radical approach to creating fairness',

factor has confirmed this premise.

The focal point of the fairness assessment should therefore be the consideration of all parties' interests and trust-impeding apprehensions. A code of conduct may comprise a series of procedural steps to ensure fairness during the data exchange, though the final appraisal should always be made on a substantive case-to-case basis. Such a substantive fairness assessment would require the intermediary to conduct an overall impact assessment while implementing appropriate technical and organizational measures to ensure that – by default and in good faith – the data exchange safeguards the rights and vulnerabilities of all parties involved. This substantive fairness principle may thus call for a trust assessment "by design and by default", similar to the existing obligations concerning the protection of personal data in Art 25 GDPR.[225] Hence, in addition to a risk-based approach and the implementation of appropriate measures, the intermediary may also be expected to ensure and demonstrate compliance with the substantive fairness requirements in the code of conduct.[226]

3.3.2. Transparency

3.3.2.1. Art 5(1) and Art 34 GDPR

A second principle in the code of conduct is transparency. Firstly, this principle has already been enshrined in Art 5(1) GDPR.[227] Moreover, Art 34 GDPR imposes a risk-based communication duty upon data subjects in the scenario of serious personal data breaches.[228]

The impact on trust of such a communication duty is straightforward. In the first place, it has been denoted that communication processes (e.g. two-way communication and communication quality) are a primary group of trust-enhancing antecedents.[229] The obligation to communicate in "*clear and plain*" language in Art 34(2) GDPR thus adds to the communication quality and interactional courtesy and benefits external parties' trust in the intermediary.

In addition, the insights gathered from the Safe-DEED survey affirm the trust-enhancing impact of clear and plain language. All respondents, namely, agreed that the trust is enhanced if there

The Conversation, accessed 3 May 2021 <https://theconversation.com/biased-algorithms-heres-a-more-radical-approach-to-creating-fairness-109748>.

[225] GDPR Art 25.

[226] *Ibid*.

[227] GDPR Art 5

[228] GDPR Art 34.

[229] *Supra*. 2.1.1.3. "Schedule".

are rules that clarify and demystify data processing and data protection procedures.[230] Trustees should therefore not only inform trustors about how their data is being processed (as is *de lege lata* enshrined in Art 5(1) and 34 GDPR). In addition, they should also make efforts to inform trustors about the applicable legal framework, clearly and understandably.

3.3.2.2. Art 10 DGA

Though the obligation in Art 5(1) and 34 GDPR only materially applies to the processing of personal data[231], a similar duty seems to have been enshrined in the DGA. Art 10 DGA namely imposes a so-called "notification duty" upon data sharing service providers.[232] Nonetheless, this notification duty is more comprehensive than the communication duty in Art 34 GDPR. The duty in Art 10 DGA is namely not merely risk-based. It also includes a more extensive list of information that should be notified by the intermediation service (*i.e.* the data market provider) to the competent public authorities.[233]

Art 10(6) DGA specifically enlists that authorities should be notified about *inter alia* the name of the data market provider[234], their legal status[235], their address[236], their website[237], and the provider's contact information[238]. Hence, this duty does not directly affect data providers' and data users' trust in the service, as they are no party to the notification process. Instead, Art 10 DGA aims to provide the European Union with a register of all data intermediaries.

Nevertheless, this envisioned transparency enhancement might indirectly add to businesses' trust in a data marketplace, as the inclusion in the register would irrefutably add to the marketplace's perceived integrity.

3.3.2.3. Art 11 DGA

Furthermore, the notified information according to Art 10 DGA may be used by public

[230] Safe-DEED Survey on "Trust in a Data Market context", question: *"Within a B2B platforms environment, trust between the partners is enhanced if there are rules clarifying and demystifying data processing and data protection procedures"*, 10 answers were given, with an average rating of 9.3 (0 meaning "I fully disagree" and 10 meaning "I fully agree"), answer breakdown: "0" (0 respondents, 0.0%); "1" (0 respondents, 0.0%); "2" (0 respondents, 0.0%); "3" (0 respondents, 0.0%); "4" (0 respondents, 0.0%); "5" (0 respondents, 0.0%); "6" (0 respondents, 0.0%); "7" (2 respondents, 20.0%); "8" (0 respondents, 0.0%); "9" (1 respondents, 10%); "10" (7 respondents, 70%).
[231] GDPR Art 2.
[232] DGA Art 10, 11.
[233] *Ibid*.
[234] *Ibid*. Art 10(6) (a).
[235] *Ibid*. Art 10(6) (b)
[236] *Ibid*. Art 10(6) (c)
[237] *Ibid*. Art 10(6) (d)
[238] *Ibid*. Art 10(6) (e).

authorities to monitor the marketplace's compliance with the comprehensive series of conditions in Art 11 DGA.[239] These conditions are aimed at enhancing both transparency and fairness vis-à-vis data providers and data users.[240] A number of these conditions correlate with principles and antecedents that have been previously mentioned in this deliverable.[241] Art 11(1) for instance stipulates that "*the provider may not use the data for which it provides services for other purposes than to put them at the disposal of data users and data sharing services shall be placed in a separate legal entity*".[242] This article thus represents a principle similar to that of purpose limitation in Art 5(1)(b) GDPR and is equally rooted in the antecedent of asset specificity.

Furthermore, Art 11(3) embeds the principles of fairness and transparency.[243] Nonetheless, this article merely mentions procedural fairness regarding access to the data market (i.e. "*the provider shall ensure that the procedure for access to its service is fair*").[244] Hence, this procedural notion of fairness is notably narrower than the broad substantive conception of fairness that was derived from Art 5(1)(a) GDPR and the *bona fide* principle (i.e. rooted in equitability, correctness and loyalty) in domestic legal traditions.[245]

In addition, Art 11(7) provides that "*the provider shall put in place adequate technical, legal and organizational measures in order to prevent transfer or access to non-personal data that is unlawful under Union law*".[246] This preventative obligation seems to align with the duty to "*implement appropriate technical and organizational measures*" as part of data protection by design and by default in Art 25 GDPR.[247] Nonetheless, the scope of Art 11(7) is rather limited, as it only comprises the prevention of unlawful access or transfers to non-personal data. Therefore, this obligation falls short of adding up to so-called "trust-enhancement by design and by default", as touched upon *supra*.[248] The latter would namely imply an all-encompassing assessment of all trust-antecedents and the vulnerabilities of all parties involved, based on the comprehensive substantive fairness principle that was put forward.[249]

Nevertheless, with its Art 11(7) DGA, the EU has acknowledged the importance of preventative organizational measures to enhance trust. The inclusion of this provision in the DGA may thus

[239] *Ibid*. Art 10, 11.
[240] *Ibid*. Art 11.
[241] *Supra*. 2.2.2. "Antecedents".
[242] DGA Art 11(1).
[243] *Ibid*. Art 11(3).
[244] *Ibid*.
[245] *Supra*. 3.3.1. "Fairness".
[246] DGA Art 11(7).
[247] GDPR Art 25.
[248] *Supra*. 3.3.1. "Fairness".
[249] *Supra*. 3.3.1. "Fairness".

constitute a wary first step towards a more wide-ranging principle of "trust-enhancement by design and by default". The obligation to act "*in the data subjects' best interest*" in Art 11(10) further substantiates this claim.[250] Nevertheless, - as with Art 11(7) DGA - the obligation in Art 11(10) is mainly limited to an advisory and procedural obligation (i.e. "*in particular by advising data subjects*"[251]) and equally falls short of entailing a broad risk-assessment based on a substantive fairness principle.

3.3.2.4. Art 3 P2BR

Both principles of fairness and transparency are also promoted in the EU's Platform-to-Business Regulation (hereafter: "P2BR").[252] In this regulation, "transparency" is defined as the intermediary's obligation to provide unambiguous terms and conditions.[253] This principle is, therefore, more limited than the abovementioned risk-based communication duty in Art 34 GDPR.[254] Furthermore, it has been often asserted that terms and conditions (hereafter: "T&Cs") are barely read by any users, which may profoundly impede the practical relevance of Art 3 P2BR.[255] A report by the European EC on "Consumers' attitudes towards terms and agreements"[256] further substantiated this insight, affirming that "*the vast majority of consumers accept Terms and Conditions (T&Cs) without even reading them*".[257] This reluctance to read T&Cs is argued to be rooted in their long and complicated wording. At present, - five years after the report's publishing - little seems to have changed. Nonetheless, both the EC's report and the P2BR propose the same resolution to enhance users' engagement: terms and conditions should be shorter and ought to be drafted in plain and intelligible language.

Moreover, the EC's report states that the visual presentations of T&Cs may need improvement. Hence, these insights may indicate that in the data market context, a plain and visually pleasing code of conduct may foster transparency beyond the currently limited practicality of Art 3

[250] DGA Art 11(10).
[251] *Ibid*.
[252] Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57.
[253] *Ibid* Art 3.
[254] *Supra*. 3.3.2.1. "Art 5(1) and 34 GDPR".
[255] Tim Sandle, 'Report finds only one percent reads terms and conditions' (*Digital Journal*, 29 January 2020) <https://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article> accessed 1 May 2021; Thomas Chivers, 'Privacy complacency: the hidden dangers lurking beneath today's surface-level data protection' (*ProPrivacy*, 28 January 2020) <https://proprivacy.com/privacy-news/privacy-complacency-ebook > accessed 1 May 2020;
[256] Commission, 'Study on consumers' attitudes towards Terms and Conditions (T&Cs)' (final report, 1 March 2016) <https://ec.europa.eu/info/sites/default/files/terms_and_conditions_final_report_en.pdf> accessed 1 May 2020.
[257] *Ibid*.

P2BR. This premise has been affirmed by the aforementioned survey finding on the trust-enhancing demystification of data processing and data protection procedures.[258]

Furthermore, the P2BR also promotes the principle of fairness. Nevertheless, the regulation restricts this principle to its procedural component by providing effective out-of-court redress mechanisms, comprising an internal complaint-handling system[259], and specialized mediation[260]. As with the DGA[261], the P2BR thus also seems to opt for a non-substantive conception of fairness.

3.3.2.5. Art 6 FFNPDR

Art 6 FFNPDR comprises the facilitation of codes to "*contribute to a competitive data economy, based on the principles of transparency and interoperability*".[262] Though this provision specifically alludes to the facilitation of data porting, it does include insightful clarifications on what a general code of conduct for marketplace providers may entail. The codes of conduct in Art 6 namely consist of four elements: (I) best practices[263], (II) minimum information requirements[264], (III) approaches to certification schemes[265], and (IV) communication roadmaps[266].

These four elements each correlate with one or multiple trust-enhancing antecedents. The use of best practices may namely foster both organizational characteristics[267], as well as positively impact trustee characteristics (e.g. task competence[268] and the provision of assistance to trustors[269]).

Furthermore, the information requirements in Art 6(1) (b) FFNPDR relate to the processes, timeframes, charges and technical requirements of data porting[270], align with the fostering a

[258] *Supra* 3.3.2.1. "Art 5(1) and Art 34 GDPR".
[259] *Ibid*. Art 11.
[260] *Ibid*. Art 12, 13.
[261] *Supra*. 3.3.2.2. "Art 10 DGA".
[262] FFNPDR Art 6.
[263] *Ibid*. Art 6(1)(a).
[264] *Ibid*. Art 6(1)(b).
[265] *Ibid*. Art 6(1)(c).
[266] *Ibid*. Art 6(1)(d).
[267] Randy Hodson, 'Organizational Trustworthiness: findings from the population of organizational ethnographies' (2004) 15(4) Organization Science 432.
[268] Josh Gullett, Loc Do, Maria Canuto-Carranco, Mark Brister, Shundricka Turner, Cam Caldwell, 'The buyer-supplier relationship: an integrative model of ethics and trust' 2009 (90) 3 Journal of Business Ethics 329.
[269] Jeffrey Dyer, Wujin Chu, 'The role of trustworthiness in reducing transaction costs and improving performance: empirical evidence from the United States, Japan and Korea' (2003) 14 Organization Science 57.
[270] FFNPDR Art 6(1)(b).

common business understanding[271] and communication quality[272]. Thirdly, the use of certification schemes aims to facilitate the comparison of data processing products and services.[273] These schemes thus serve as a means to communicate the trustworthiness of each service provider[274] and allow for a high degree of integrity[275] and interactional courtesy[276] vis-à-vis trustors. Lastly, Art 6(1)(d) FFNPDR provides for communicative roadmaps; intended to raise awareness of the codes of conducts amongst all stakeholders.[277] By providing overarching roadmaps, the legislator aims to acquaint all actors involved, enhancing trust amongst all parties.[278] As opposed to Art 6(1)(a) to (c), this last element thus touches on an entire subgroup[279] of trust-enhancing antecedents (i.e. "communication processes[280]), rather than upon a number of particular ones.

Furthermore, Art 6(2) FFNPDR stipulates that these codes should be closely developed with all relevant stakeholders, "*including associations of SMEs and start-ups, users and cloud service providers*".[281] Similar to Art 6(1) (d), this paragraph equally aligns with an entire subgroup of trust-enhancing antecedents, being the "shared characteristics between trustor and trustee".[282] The users' involvement of (i.e. the trustor) creates a prior relationship between trustor and trustee,[283] sets out a clear vision on their expected future relationship[284], creates joint

[271] Eva Kasper-Fuehrer, Neal Ashkanasy, 'Communicating trustworthiness and building trust in interorganizational virtual organizations' (2001) 27(235) Journal of Management 1.
[272] Günter Stahl, Rikard Larsson, Ina Kremershof, Sim Sitkin, 'Trust dynamics in acquisitions: a case study' (2011) 50Human Resource Management 575.
[273] FFNPDR Art 6(1)(c).
[274] Eva Kasper-Fuehrer, Neal Ashkanasy, 'Communicating trustworthiness and building trust in interorganizational virtual organizations' (2001) 27(235) Journal of Management 1;
[275] Michael Palanski, Francis Yammarino, 'Integrity and leadership: a multi-level conceptual framework' (2009) 20(3) The Leadership Quarterly 405.
[276] Josh Gullett, Loc Do, Maria Canuto-Carranco, Mark Brister, Shundricka Turner, Cam Caldwell, 'The buyer-supplier relationship: an integrative model of ethics and trust' 2009 (90) 3 Journal of Business Ethics 329.
[277] Art 6 (1)(d) FFNPDR.
[278] Randy Hodson, 'Organizational Trustworthiness: findings from the population of organizational ethnographies' (2004) 15(4) Organization Science 432.
[279] *Supra*. 2.1.1.3. "Schedule".
[280] *Ibid*.
[281] Art 6(2) FFNPDR.
[282] *Supra*.
[283] Henri Dekker, A.G.H.L. van den Abbeele, 'Organizational learning and interfirm control: the effects of partner search and prior exchange experiences' (2010) 21 Organization Science 1233.
[284] Andrew Inkpen, Eric Tsang, 'Social Capital, Networks, and Knowledge Transfer' (2005) 30 Academy of Management Review 146.

dependence[285], fosters a common business understanding[286] and allows for mutual adaptation between trustor and trustee[287].

The codes of conduct in Art 6 FFNPDR have a limited scope *ratione materiae,* as they merely apply to the enhancement of the porting of non-personal data. Nevertheless, it has been demonstrated that the practices within these codes clearly correlate with various antecedents of organizational trust. Hence, the structure and content of Art 6 (1) FFNPDR may serve as a possible example *mutatis mutandis* for the codes of conduct for data market providers. Furthermore, Art 6(2) FFNPDR sets an example for the involvement of all actors in the establishment of codes of conduct. Especially the inclusion of trustors seems indispensable to foster organizational trust, even in the stage prior to the formation of the code of conduct. Lastly, it has been demonstrated that Art 6(1) (a) to (c) enhance a number of particular trust-antecedents, whilst Art 6(1) (d) and Art 6(2) FFNPDR facilitate an entire trust-enhancing subgroup. Against this backdrop, the procedural elements of Art 6 FFNPDR (i.e. the use of communicative roadmaps and the *a priori* involvement of trustors) should be especially considered in moving toward trust-enhancing codes of conducts for data market providers.

3.3.3. Security

Thirdly, a code of conduct may equally impose certain security-enhancing obligations on the data market provider. The assessment in the previous subchapter has demonstrated that the EU legal framework is governed by a certain lack of legal certainty and coherence in security measures.[288] Hence, inclusion of security measures in a harmonized code of conduct may alleviate several present inconsistencies in the legal framework.

With regard to security, Art 11(8) DGA mentions that measures should be taken to "*ensure a high level of security for the storage and transmission of non-personal data*".[289] As expanded upon *supra*, security-enhancing measures starkly affect organizational trust.[290] Within the realm of the Safe-DEED research, it was emphasized that encryption techniques such as MPC indispensably impact external parties' trust in a data marketplace.[291] Art 11(8) seems to affirm

[285] Thomas Gainey, Brian Klaas, 'The outsourcing of training and development: factors impacting client satisfaction' (2003) 29(2) Journal of Management 207.

[286] Eva Kasper-Fuehrer, Neal Ashkanasy, 'Communicating trustworthiness and building trust in interorganizational virtual organizations' (2001) 27(235) Journal of Management 1.

[287] Stephen Carson, Anoop Madhok, Rohit Varman, George John, 'Information Processing Moderators of the Effectiveness of Trust-Based Governance in Interfirm R&D Collaboration' (2003) 14 (1) Organization Science 45.

[288] *Supra*. 3.2.2. "Legal Certainty and Organizational Trust".

[289] DGA Art 11(8).

[290] *Supra* 3.2. "Privacy- and security-enhancing technologies".

[291] *Supra* 3.2.1. "Secure multi-party computation and organizational trust".

this claim, though it remains to be seen to what extent (MPC) encryption falls within the ambit of this article. The DGA's only report on encryption concerns the Rec 18 mentioned above, which outlines that "*data sharing providers (…) should take all reasonable measures to prevent access to the systems where non-personal data is stored, including encryption of data or corporate policies*".[292]

The DGA thus merely acknowledges the role of encryption in preventing unlawful access to the marketplace, though disregards any mention of the use of encryption to safeguard the transmission of non-personal data. This discrepancy between the scopes of Rec 18 and Art 11(8) may turn out to be an inconsistency in the wording of the DGA. Therefore, it may be possible that the EU legislator intended to equally stress the role of encryption during the transmission of non-personal data. However, as it stands now, it seems that the obligation of Art 11(8) only includes the use of encryption to prevent unlawful access to non-personal data during the storage phase on the platform's system. Nonetheless, a literal reading of Rec 18 suggests that – *de lege lata* - the obligation to use encryption does not apply to data transmission and is merely restricted to the prevention of unlawful access to stored data on the system.

Though this discrepancy between Rec 18 and Art 11(8) may be an unintentional inconsistency, it once again stresses the lack of legal certainty regarding the legal standing of encryption obligations under EU law. Based on a literal reading of the DGA, it thus remains to be seen whether this Act will succeed in setting out "*highly harmonized requirements related to the trustworthy provision of data sharing services*".[293] This brief assessment thus strengthens the need for harmonized rules on the use of (MPC) encryption in a code of conduct, alongside a clear explanation of the functioning of encryption techniques and the applicable legal frameworks.

3.3.4. Neutrality

In Rec 26 DGA, it is mentioned that data-sharing service providers' neutrality is a key element to bring trust and more control to data providers and data users.[294] Following this, data market providers may only act as intermediaries in the transactions and cannot use the data for any other purposes.[295] Furthermore, Rec 26 proceeds by stating that structural separations will be needed between the data-sharing service and other services to avoid conflicts of interest.[296]

[292] DGA Rec 18.
[293] *Ibid*. Rec 25.
[294] DGA Rec 26.
[295] *Ibid*.
[296] *Ibid*.

Neutrality can be expected to foster a number of trustee characteristics, such as integrity, business ethics, and equity, and enhance organizational trust.

The precise scope of the neutrality requirement in Rec 26 DGA is still rather unclear.[297] The explanatory memorandum adds that neutrality may enhance trust and incentivizes the development of common European data spaces.[298] However, little is currently known about these data spaces, as is the case with other novelties in the DGA, such as data cooperatives and data altruism organizations. Though further legislative actions will thus undeniably clarify these new conceptions, it is currently not yet possible to conduct a thorough assessment of their trust impact.

Nevertheless, it seems that the neutrality requirement will call upon all data market providers to take all necessary measures to avoid any conflicts of interest. Therefore, it seems that certain underlying good practices may be incorporated in the code of conduct. Upcoming legislative actions within the European Strategy for Data shall undeniably shed more light on this conception and its place within the trust-enhancing code of conduct.

3.4. Summary: two means to enhance trust

This deliverable proposes two concrete means to facilitate organizational trust in data marketplaces, based on insights from fundamental research, the Safe-DEED survey and the semi-structured interviews.

In the first place, the enhancement of trust relies on the use of security- and privacy-enhancing technologies. In the data market context, the use of MPC is therefore invaluable in fostering organizational trust. In particular, secure multi-party computation enhances the antecedents of asset specificity and perceived fairness. Nevertheless, the use of MPC equally gives rise to a degree of legal uncertainty, in its turn diminishing organizational trust. The EU seems to be aware of this peril by stressing the increased need for clear and harmonized provisions related to trust-building in the data market context. The precise nature of these efforts will depend on the further legislative actions to foster the "European approach to data governance". Though the harmonization emphasis in the DGA is a vital first step, further regulatory initiatives within

[297] DGA Rec 26.
[298] DGA Explanatory Memorandum.

the European Digital Strategy shall need to expand on the legal uncertainty arising from the use of privacy-and security-enhancing technologies.[299]

In addition, a code of conduct may equally enhance organizational trust. Concerning its content, this deliverable has put forward four principles. First is the principle of fairness. In order to safeguard a wide range of trust antecedents, it has been stated that an effect-based principle of fairness should be maintained. This principle has been based on the fairness principle in both the GDPR, on interview respondents' attestation of the importance of due diligence, and on domestic *bona fide* interpretations. In essence, this principle would oblige data market providers to continuously and *a priori* mitigate trustors' vulnerabilities and relational asymmetries. Therefore, this conception of fairness would come rather close to an obligation of "trust-enhancement by design and default".

A second principle in the code of conduct is transparency. This deliverable has drawn upon a number of transparency requirements within the European Digital Strategy. Firstly, Art 10 and 11 DGA have been assessed. Though the corresponding notification duty does not manage to outline a comprehensive transparency requirement, these articles (especially Art 11(7) and Art 11(10) DGA) showcase the EU's acknowledgement of the need for a broader substantive fairness principle. Though both Art 11(3) DGA and Art 3 P2BR uphold a procedural reading of "fairness", the transparency-enhancing notification duty in Art 11(7) DGA may constitute a wary move toward a more substantive notion of fairness in the EU's approach to data governance.

Furthermore, the transparency-inducing methods of Art 6 FFNPDR may serve as a structural example *mutatis mutandis* for the codes of conduct for data market providers. It has namely been shown that the inclusion of best practices, minimum information requirements and the approach to certification schemes (i.e. Art 6(1) (a) to (c) FFNPDR) positively impact a number of trust-enhancing antecedents.

Art 6(1) (d) and Art 6(2) FFNPDR have confirmed that communicative roadmaps and the *a priori* involvement of trustees enhance entire subgroups of trust-antecedents are necessary steps for the establishment of codes of conduct. Concerning these communicative steps, an assessment of both Art 3 P2BR and the EC's Report on T&Cs has stressed the importance of clear, short, intelligible and visually pleasing communication as a means to foster trust vis-à-vis external parties.

[299] In this regard, the aforementioned "legal Q&A" by the Safe-DEED consortium may serve as a preliminary guidance.

Thirdly, the precise implementation of security measures should be included in codes of conduct as well. This incorporation may serve as a tool to preventively clarify potential legal disputes arising from the use of encryption techniques, especially since trustors ought to be involved in establishing these codes. Such an *a priori* dialogue on possible legal issues may very well alleviate some of the aforementioned concerns of MPC-induced legal uncertainty. Nonetheless, more regulatory clarity on the legal issues arising from MPC remains desirable, which ultimately hinges on the future legal initiatives within the European Digital Strategy.

Lastly, a code of conduct should equally include provisions to prevent conflicts of interest. In this regard, the EU has affirmed the principle of neutrality in Rec 26 DGA. As with the security element, the precise scope of this neutrality obligation still largely depends on the upcoming legislative initiatives as part of the European Digital Strategy. It seems evident that codes of conduct may include practical guidance to avoid any (perception) of non-neutrality on the trustee's side.

Conclusion

This deliverable started with an elaboration upon the role of trust in a data-driven European economy. In particular, the first chapter has touched on the EU's acknowledgement of trust-building within its broader European Strategy for Data.

A second chapter aimed to clarify the concept of trust as such. A first subchapter has enlisted a series of trust-enhancing antecedents and consequences, all the while elaborating upon the concrete concept of organizational trust. A second subchapter has then applied these insights to the data market context (i.e. "digital trust").

A third chapter assessed two methods to enhance digital trust. The use of secure multi-party computation was a first proposed method. Regardless of the legal uncertainty arising from encryption, it was shown that the use of MPC clearly facilitates a series of trust-enhancing antecedents. A second method concerned the use of codes of conduct vis-à-vis data marketplace providers. Based on - *inter alia* - the semi-structured interview insights, this research has put forward four guiding principles for such codes. In the first place, the importance of a substantive fairness principle has been stressed despite the EU's common inclination toward a procedural conception of fairness. Secondly, codes of conduct should uphold an adequate degree of transparency, the content of which has been drawn upon provisions within the GDPR, the P2BR, the FFNPDR and the DGA. Significantly, Art 6 FFNPDR has been asserted to constitute an illustration of the various transparency elements the code of conducts may entail. In addition, Art 6 FFNPDR has stressed the use of communicative roadmaps, which ought to be clear, concise and visually pleasing, as can be derived from the EC's Report on T&Cs and Art 3 P2BR. Furthermore, it has been proclaimed that codes of conduct should also include practical security- and neutrality- enhancing provisions, the scope of which still widely depends on the EU's upcoming actions as part of its Digital Strategy.

Annex

Safe-DEED Survey

As part of this deliverable, the Safe-DEED consortium has created a survey to understand better how organizations generate trust, how shareholders perceive 'trust', and how individuals can be empowered within a B2B platforms environment. The survey was addressed to consumers, civil society representatives, academics, and public servants.

The survey was launched by WP3, consisted of forty-two questions, and attracted a total of sixty-three anonymous respondents, sixty of which were willing to share their capacity: fifty-three (88.3%) of these respondents were either consumers, academics, civil society representatives or public servants. The remaining seven (11.7%) respondents were business representatives. It should be noted that none of the questions were obligatory. As a result, the number of respondents per question may vary slightly. These differences in response rate were taken into account whilst analysing the survey outcomes.

The survey was disseminated both internally (i.e. amongst consortium members) and externally. Dissemination channels included Safe-DEED's social media channels, internal newsletters and the European Big Data Value Forum (BDVA), as this association incorporates experts and stakeholders in the field of Safe-DEED business activities. A detailed description of the methodology used may be consulted in Safe-DEED D3.6.[300]

From a privacy and data protection perspective, it should stressed that information gathered during survey and semi-structured interviews does not include personal data as defined by Art. 4(1) GDPR.[301]

The derived results were aggregated to complement the research activities within this deliverable. The platform used was Typeform. A link to Typeform's terms and conditions was provided to the respondents in the survey's introductory description. The data assembled was consequently analysed and coded via NVivo software.

[300] Safe-DEED deliverable 3.6, https://safe-deed.eu/wp-content/uploads/2020/06/Safe-DEED_D3_6.pdf.
[301] Respondents were notified *that "KU Leuven Centre for IT and IP law (CiTiP) is organising this survey. CiTiP does not collect via your participation in this survey any type of identifiers that could directly or indirectly identify you, such as a name, identification numbers, location data, online identifiers or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of yours. CiTiP aims to use aggregated results of this survey in order to complement its research activities within the Safe-Deed project. Comments you provide via your input may be shared in Safe-DEED deliverables as anonymous quotes only.".*

The survey’s questions can be divided into several groups. The first range of questions dealt with the weight respondents gives to various trust-enhancing factors. The respondents could answer any number between zero (i.e. the factor is not trust-enhancing) and five (i.e. the factor is very trust-enhancing). The second group of questions provided a series of hypotheses. The respondents were asked for their stance on these statements by giving a score from 0 (“I completely disagree”) to 10 (“I fully agree”)—the third set of questions laid down definitions. Respondents were asked whether they agreed with the formulation and scope of definitions by clicking either “yes” or “no”. A fourth-round included questions on the respondent’s activities' general nature and the respondent's concrete trust issues. A final range of queries aimed to ascertain what industries and sectors the respondents generally regard as (un)trustworthy.

The results of this survey were incorporated into this deliverable. An explicit reference to the precise wording of the corresponding question has been added to the footnotes. These footnotes also mention the answer ratio and the number of respondents. As some questions did not receive as many responses as others, one should assess the statistical relevance of the answers in a nuanced manner. However, even those answers with fewer responses are considered of value to understand consumers’ and businesses’ perceptions of trust. Moreover, these responses will be further substantiated by the semi-structured interviews.

Semi-structured Interviews

The semi-structured interviews aimed at gaining qualitative insights, building further upon the Safe-DEED survey responses. Safe-DEED's approach to these interviews has been explained in "1.4. Semi-structured interviews".

The interviews consisted of fourteen questions, answering to which was both voluntary and anonymous. The first pair of questions (Q1-2) aimed at better understanding the setting (sector, industry and entities' size) in which the respondent operates. A subsequent series of questions (Q3-10) concerned the respondents' data (sub)processing activities, followed by questions on the perceived impact of legislation on generating security and trust. The final four questions (Q10-14) delved into the notion of trust and the experienced impact of particular trust antecedents. The questions were the following:

1. In which industry or sector does your company perform its activities?
2. Can you provide us numbers to help us understand how big the entity is where you work?
3. Does your company rely on (personal) data processing?
4. How much do you rely on subcontractors to perform activities involving data processing?
    a. On which basis does your company "trust" these subcontractors?
        i. Personal relations/engagement
        ii. Due diligence
        iii. Monitoring activity
        iv. No market alternatives
    b. What monitoring activities is your trust relationship with them based on?
5. Does your company rely on data other than personal data?
6. Do you think there is a clear distinction between personal and non-personal data?
7. From a business perspective, do you think more serious damage might come from a loss of personal or non-personal data?
8. Do you think IP protected data, crucial to protect algorithms and data-valorisation tools, are protected as much as personal data? Do you think the legislator should do more?
9. Do you think legislation such as the GDPR offers you crucial support? Or has it been overburdening your activity without a clear added value?
10. Do you think the GDPR helps in supporting users' trust toward companies and organisations?
11. How would you define "trust" in a business-oriented online environment?
12. Do you think the notion of trust in an online environment has changed?
13. Do you rely on transparency-enhancing measures? Which ones?
    a. Full pricing

   b. Inventory of data processing steps
   c. Contract summaries

14. Which particular mechanisms have proven most vital to ensure trust in your experience?
    a. Security
    b. Transparency
    c. Data management software and protocols
    d. Personal engagement and client/provider fidelisation
    e. Value exchange

Bibliography

Legislation

- EC Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation [2017] OJ L 220; EC Regulation (EU) 2015/703 of 30 April 2015 establishing a network code on interoperability and data exchange rules [2015] OJ L 113.
- 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 [2015] OJ L 337.
- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172.
- Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136.
- Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU [2019] OJ L 158
- Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC [2009] OJ L 211.
- Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport [2010] OJ L 207.
- Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) [2020] COM/2020/842 final.
- Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act) [2020] COM/2020/767 final.
- Regulation (EC) No 595/2009 of the European Parliament and of the Council of 18 June 2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information and amending Regulation (EC) No 715/2007 and Directive 2007/46/EC and repealing Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC [2009] OJ L 188/1.

– Regulation (EU) 2016/679 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) [2016] OJ L 119/1.
– Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (Free Flow of Non-personal Data Regulation) [2018] OJ L303/59.
– Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57.
– Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15.

EU Communications

– European EC, 'A European Strategy for Data' (Shaping Europe's Digital Future, 9 March 2021) <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>.
– European EC, 'The European Data Strategy: Fact Sheet' (Shaping Europe's Digital Future, 19 February 2020).
– European EC, 'Industrial Applications of Artificial Intelligence and Big Data' (Internal Market, Industry, Entrepreneurship and SMEs, 2020).
– European EC, 'A European Strategy for Data' (Communication from the EC to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 19 February 2020) COM /2020/66 final.
– European EC, 'Communication from the EC to the European Parliament, the Council, the European Economic and Social Committee of the Regions "Building a European Data Economy"' (COM(2017) 9 final).
– EC, 'Study on consumers' attitudes towards Terms and Conditions (T&Cs)' (final report, 1 March 2016).

Doctrine

Books and Contributions

- Pasquale F., *The Black Box Society: the secret algorithms that control money and information* (1st edn, Harvard University Press 2016).
- Foroohar R., *Don't be evil: the case against big tech* (1st edn, Allen Lane Penguin Random House UK 2019).
- Sartor G., 'Privacy, Reputation and Trust: Some Implications for Data Protection' in Ketil Stolen, William Winsborough, Fabio Martinelli, Fabio Massacci (eds), *Trust Management. iTrust 2006. Lecture Notes in Computer Science* (vol 3986 Springer Publishing 2006).
- Bygrave L., *Data Protection Law: Approaching its rationale, logic and limits* (The Hague Kluwer International 2002) 58.

Journals

- Ashforth S., Dutton J., 'Organizational Identity and Identification: charting new waters and building new bridges' (2000) 25(1) The Academy of Management Review 13.
- Audi R., 'Some dimensions of trust in business practices: from financial and product representation to licensure and voting' (2008) 80 Journal of business ethics 97.
- Bell G., Oppenheimer R., Bastien A., 'Trust deterioration in an international buyer-supplier relationship' (2002) 36 Journal of Business Ethics 65.
- Bernhard Nielsen B., Nielsen S., 'Learning and innovation in international strategic alliances: an empirical test on the role of trust and tacitness' (2009) 46 (6) Journal of Management Studies 1031.
- Blois K., 'Is it commercially irresponsible to trust?' (2003) 45 Journal of Business Ethics 183.
- Burton R., Lauridsen J., Obel B., 'The impact of organizational climate and strategic fit on firm performance' (2004) 43(1) Human Resources Management 67.
- Cable D., Edwards J., 'Complementary and supplementary fit: a theoretical and empirical integration' (2004) 89 Journal of Applied Psychology 822.
- Carson S., Madhok A., Varman R., John G., 'Information Processing Moderators of the Effectiveness of Trust-Based Governance in Interfirm R&D Collaboration' (2003) 14 (1) Organization Science 45.
- Clifford D. and Ausloos J., 'Data Protection and the role of fairness' (2018) 37 Yearbook of European Law 130.
- Croonen E., 'Trust and fairness during strategic change processes in franchise systems' (2010) 95 Journal of Business Ethics 191.

- Davies M., Lassar W., Manolis C., Prince M., Winsor R., 'A model of trust and compliance in franchise relationships' (2011) 26(3) Journal of Business Venturing 321.
- De Clerq D., Sapienza H.J., 'When do venture capital firms learn from their portfolio companies?' (2005) 29 Entrepeneurship: theory and practice 517.
- Dekker H., van den Abbeele A., 'Organizational learning and interfirm control: the effects of partner search and prior exchange experiences' (2010) 21 Organization Science 1233.
- Dyer J., Chu W., 'The role of trustworthiness in reducing transaction costs and improving performance: empirical evidence from the United States, Japan and Korea' (2003) 14 Organization Science 57.
- Faems D., Janssens M., Madhok A., van Looy B., 'Toward an integrative perspective of alliance governance: connecting contract design, trust dynamics, and contract application' (2008) 51 (6) The Academy of Management Journal 1053.
- Fulmer A., Gelfand M., 'At what level (and in whom) do we trust: trust across multiple organizational levels' (2012) 38(4) Journal of Management 1167.
- Gainey T., Klaas B., 'The outsourcing of training and development: factors impacting client satisfaction' (2003) 29(2) Journal of Management 207.
- Gibson C., Birkinshaw J., 'The antecedents, consequences and mediating role of organizational ambidexterity' (2004) 17 (2) The academy of management journal 209.
- Gillespie N., Dietz G., 'Trust repair after an organization-level failure' (2009) 34 Academy of management review 127.
- Graebner M., 'Caveat venditor: trust asymmetries in acquisitions of entrepreneurial firms' (2009) 52 Academy of Management Journal 435.
- Gullett J., Do L., Canuto-Carranco M., Brister M., Turner S., Caldwell C., 'The buyer-supplier relationship: an integrative model of ethics and trust' 2009 (90) 3 Journal of Business Ethics 329.
- Guzzo R., Dickson M., 'Teams in organizations: Recent research on performance and effectiveness' (1996) 47 Annual Review of Psychology 307.
- Hernan Gonzalez R., Kujal P., 'Trust and trustworthiness under information asymmetry and ambiguity' (2017) 147 Economics Letters 1.
- Hodson R., 'Organizational Trustworthiness: findings from the population of organizational ethnographies' (2004) 15(4) Organization Science 432.
- Inkpen A., Tsang E., 'Social Capital, Networks, and Knowledge Transfer' (2005) 30 Academy of Management Review 146.

– Janowicz-Panjaitan M., Krishnan R., 'Measures for dealing with competence and integrity violations of interorganizational trust at the corporate and operating levels of organizational hierarchy' (2009) 46(2) Journal of Management Studies 245.
– Jensen M., 'The role of network resources in market entry: commercial banks' entry into investment banking, 1991-1997' (2003) 48 Administrative Science Quarterly 466.
– Kasper-Fuehrer E., Ashkanasy N., 'Communicating trustworthiness and building trust in interorganizational virtual organizations' (2001) 27(235) Journal of Management 1.
– Katsikeas, C. Skarmeas D., 'Developing successful trust-based international exchange relationships' (2009) 40(1) Journal of International Business Studies 132.
– Lado A., Dant R., Tekleab A., 'Trust-opportunism paradox, relationalism and performance in interfirm relationships: evidence from the retail industry' (2008) 29(4) Strategic Management Journal 401.
– Lewicki R., Tomlinson E., Gillespie N., 'Models of interpersonal trust development: Theoretical approaches, empirical evidence, and future directions' (2006) 32 Journal of Management 991.
– Lui S., Ngo Hang Y., 'An action pattern model of inter-firm cooperation' (2005) 42 Journal of Management Studies 1123.
– Malgieri G., 'The concept of fairness in the GDPR: a linguistic and contextual interpretation' (2020) FACCT: Fairness, Accountability, and Transparency 154.
– Malhotra D., Lumineau F., 'Trust and collaboration in the aftermath of conflict: the effects of contract structure' (2011) 54 Academy of Management Journal 981.
– Marguire S., Phillips N., 'Citibankers at Citigroup: a study of the loss of institutional trusts after a merger' (2008) 45(2) Journal of Management Studies 372.
– Molina-Morales X., Martinez-Fernandez T., 'Too much love in the neighborhood can hurt: how an excess of intensity and trust in relationships may produce negative effects on firms' (2009) 30 Strategic Management Journal 1013.
– Morck R., Yeung B., 'Family control and the rent-seeking society' (2004) 28 Entrepreneurship: theory and practice 391.
– Neergaard H., Ulhoi J., 'Government agency and trust in the formation and transformation of interorganizational entrepeneurial networks' (2006) 30(4) Entrpeneurship: Theory and Practice 519.
– Pablo A., Reay T., Casebeer A., Dewald J., 'Identifying, enabling and managing dynamic capabilities in the public sector' (2007) 44 Journal of management studies 687.
– Palanski M., Yammarino F., 'Integrity and leadership: a multi-level conceptual framework' (2009) 20(3) The Leadership Quarterly 405.

- Patzelt H., Shepherd D., 'The decision to persist with underperforming alliances: the role of trust and control' (2008) 45 Journal of Management Studies 1217.
- Pucetaite R., Lämsä A., 'Developing organizational trust through advancement of employees' work ethic in a post-socialist context' (2008) 82(2) Journal of Business Ethics 325.
- Rotter J., 'Interpersonal trust, trustworthiness, and gullibility' (1980) 35(1) American Psychologist 1.
- Scheer ML., Kumar N., Steenkamp J., 'Reactions to perceived inequity in US and Dutch interorganizational relationships' (2003) 46 Academy of Management Journal 303.
- Schoorman D., Mayer R., Davis J., 'An integrative model of organizational trust: past, present and future' (2007) 32 Academy of Management Review 344.
- Serva M., Fuller M., Maye R. ' The reciprocal nature of trust: A longitudinal study of interacting teams' (2005) 26 Journal of Organizational Behaviour 625.
- Shockley-Zalabak P., Ellis K., Winograd G., 'Organizational Trust: What it means, why it matters' (2000) 18(4) Organization Development Journal 35.
- Sonpar K., Handelman J., Dastmalchian A., 'Implementing new institutional logics in pioneering organizations: the burden of justifying ethical appropriateness and trustworthiness' (2009) 90 Journal of Business Ethics 345.
- Stahl G., Larsson R., Kremershof I., Sitkin S., 'Trust dynamics in acquisitions: a case study' (2011) 50Human Resource Management 575.
- van Marrewijk M., 'The social dimension of organizations: recent experiences with "places to work" assessment practices' (2004) 55(2) Journal of Business Ethics 135.
- Wang H., He J., Mahoney J., 'Firm-specific knowledge resources and competitive advantage: the roles of economic- and relationship-based employee governance mechanisms' (2009) 30 Strategic Management Journal 1265.
- Wu W., 'Dimensions of social capital and firm competitiveness improvement: the mediating role of information sharing' (2007) 45 Journal of Management Studies 122.
- Zaheer A., McEvily B., Perrone V., 'Does trust matter? Exploring the effects of inter-organizational and inter-personal trust on performance' (1998) 9 (2) Organization Science 141.

Online Sources

- Chivers T., ‘Privacy complacency: the hidden dangers lurking beneath today’s surface-level data protection’ (*ProPrivacy*, 28 January 2020) <https://proprivacy.com/privacy-news/privacy-complacency-ebook > accessed 1 May 2020.
- Douglas T., ‘Biased Algorithms: here’s a more radical approach to creating fairness’, The Conversation, accessed 3 May 2021 <https://theconversation.com/biased-algorithms-heres-a-more-radical-approach-to-creating-fairness-109748>.
- International Organization for Standardization (ISO) 9000:2005.
- International Organization for Standardization (ISO) 9001:2015.
- Otto W., ‘What is organizational trust (and how to build it)?’ (2020) The Predictive Index Blog <https://www.predictiveindex.com/blog/what-is-organizational-trust-and-how-to-build-it/> accessed 12 December 2020.
- Sandle T., ‘Report finds only one percent reads terms and conditions’ (*Digital Journal*, 29 January 2020) <https://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article> accessed 1 May 2021.
