

Grant Agreement Number: 825225

Safe-DEED

www.safe-deed.eu

D3.5 Syllabus for Teaching Module

Deliverable number	<i>D3.5</i>
Dissemination level	<i>Public</i>
Delivery date	<i>20 January 2021</i>
Status	<i>Final</i>
Author(s)	<i>Alessandro Bruni, Dieter Decraene, Noémie Krack</i>



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
20.01.2021	Dieter Decraene	First draft	0.1
22.01.2021	Alessandro Bruni	Internal review	0.2
28.01.2021	Dieter Decraene	First complete draft	1.0
01/02/2021	Alessandro Bruni	Internal review	1.1
05/02/2021	Dieter Decraene	Second complete draft	2.0
15/02/2021	Hosea Ofe	Consortium review	2.1
15/02/2021	Abdel Aziz Taha	Consortium review	2.2
17/02/2021	Dieter Decraene	Final version	3.0
17/02/2021	Alessandro Bruni	Final version review	3.1

Executive Summary

Deliverable 3.5 (D3.5) provides a teaching module for law students and researchers to familiarise themselves with the Safe-DEED project's research objectives. This syllabus is aimed at two target audiences: (I) researchers within and external to the consortium; and (II) students from all relevant disciplines. Given these two groups' different levels of expertise, it has been opted to write an accessible syllabus, ideally understandable for those with no prior knowledge of various subject matters. This syllabus shall be accompanied by a series of nine video lectures, all of which shall correspond with a chapter in this syllabus. In essence, this syllabus aims at educating the reader on the various challenges hampering the advancement of a data-driven European economy. Besides, it intends to make the reader acquainted with the Safe-DEED consortium's research and its approach in overcoming some of these burdens. Furthermore, this teaching module would ideally also encourage the reader's critical stance on the topics presented, including several issues arising from the various legal, ethical, and societal forces that momentarily dominate the data-driven debate.

The nine chapters have been divided into three main parts: (I) the first two chapters present an introduction to the Safe-DEED consortium and research; (II) the following three chapters deal with the various legal and ethical considerations relevant to the project; (III) the final four chapters then acquaint students with the main challenges that the Safe-DEED research aims to overcome.

Henceforth, the first two chapters of this syllabus will focus on familiarizing the reader with the value of data and the overall functioning of data marketplaces. These two introductory sessions should enhance the reader's understanding of some of the core concepts, which shall be important throughout the remaining seven sessions.

Chapters three to five will consequently assess the various ethical and legal provisions that should be considered whilst developing a European digital economy. Thus, these three chapters should foster insights into the multiple societal considerations that revolve around the current debate. In addition, these chapters aim at acquainting the reader with their own rights as “data subjects” and some elemental legal provisions innate to the protection of data and privacy. Hence, these chapters equally intend to raise a modest degree of awareness regarding the worth of (personal) data and the fundamental values at stake.

The final four chapters will subsequently expand upon several particular challenges hindering the development of a European digital economy. It will concurrently present some possible resolutions to that, following the Safe-DEED research. It has been opted to structurally present the final chapter in a “question and answer” style so that the reader acquires a better grasp of the sorts of issues researchers get confronted with daily. At the end of the syllabus, a general overview of the most predominant insights and takeaways shall be provided.

This teaching module aims at offering the reader a visual and engaging teaching experience. It aims at making the reader more aware of the immense interdisciplinary challenges innate to the development of a European data-driven economy, whilst raising a better understanding of the value of data, and the various interdisciplinary implications it brings forth. We hope this syllabus may trigger the reader's curiosity in this intriguing subject matter.

Table of Contents

Executive Summary	3
List of Abbreviations.....	8
List of Figures.....	9
Introduction	10
1 Syllabus Structure Overview.....	12
1.1 Structure	12
1.1.1 Schematic Overview.....	12
1.1.2 Video sessions	14
1.2 Lecture Series' Dissemination Plan	14
2 PART I. THE ADVANCEMENT TOWARD A EUROPEAN DATA-DRIVEN ECONOMY: INTRODUCTION	16
2.1 CHAPTER 1. The value of data.....	16
2.1.1 Value?.....	16
2.1.2 Data?.....	18
2.1.3 Data Value?	19
2.1.4 Data-enabled Economic Development	21
2.1.4.1 Current Barriers	21
2.1.4.2 Safe-DEED Project.....	22
2.2. CHAPTER 2. Data marketplaces: an introduction.....	24
2.2.1. What?.....	24
2.2.2. Who?	25
2.2.3. Relevance	26
2.2.4. Significance	28
3. PART II. THE ADVANCEMENT TOWARD A EUROPEAN DATA-DRIVEN ECONOMY: INTERDISCIPLINARY CONSIDERATIONS.....	30
3.1. CHAPTER 3. Ethical guidelines	30
3.1.1. Fundamental Moral Principles	31
3.1.2. Digital Ethics	33
3.1.2.1. Socio-Cultural Shifts in the Digital Age.....	34
3.1.2.2. A Look into the Future	35
3.2. CHAPTER 4. The protection of personal data.....	37
3.2.1. Personal vs. Non-Personal Data	37
3.2.2. The Right to Data Protection.....	38
3.2.3. The General Data Protection Regulation.....	38
3.2.3.1. Material Scope: the Processing of Personal Data.....	39
3.2.3.1.1. Processing	39

3.2.3.1.2. Personal Data	40
3.2.3.2. Subjective Scope (of application): (Joint-) Controllers and Processors	42
3.2.3.3. General Principles	44
3.2.3.4. Obligations	49
3.2.3.5. Rights.....	50
3.2.3.6. Relevance	52
3.3. CHAPTER 5. The protection of non-personal data	54
3.3.1. “Building a European Data-Economy”	55
3.3.2. Free Flow of Non-Personal Data Regulation	57
3.3.2.1. Scope	58
3.3.2.2. Aims	59
3.3.2.2.1. The Prohibition of Mandatory Data Localization Requirements	60
3.3.2.2.2. The Guarantee of Data Availability for Competent Authorities	61
3.3.2.2.3. Porting of Data.....	62
3.3.3. Platform-to-Business Regulation.....	63
3.3.3.1. Scope	63
3.3.3.2. Purposes.....	64
3.3.4. Legal Considerations: Concluding Note.....	65
4. PART III. THE ADVANCEMENT TOWARD A EUROPEAN DATA-DRIVEN ECONOMY: CHALLENGES & OPPORTUNITIES	66
4.3. CHAPTER 6. The valuation of data	66
4.3.1. The Classification of “Data”: an economic approach	67
4.3.1.1. Data as a Commodity	67
4.3.2. Data Ownership	68
4.3.2.1. Data as Property	69
4.3.2.2. Intellectual Property Law: Copyright	70
4.3.2.2.1. Legal Regimes related to Intellectual Property.....	70
4.3.2.2.2. GDPR.....	71
4.3.2.2.3. The economic approach: key insights.....	71
4.3.3. Moving forward from the economic approach	72
4.3.4. Remaining Open Questions.....	73
4.4. CHAPTER 7. Organizational trust.....	75
4.4.1. What is Organizational Trust?.....	76
4.4.1.1. The Concept of Organizational Trust	76
4.4.1.2. Antecedents of Organizational Trust.....	78
4.4.1.3. Consequences of Organizational Trust.....	80
4.4.2. Organizational Trust in Data Marketplaces.....	81
4.4.2.1. Trustee and Trustor	81

4.4.2.2. Antecedents of Organizational Trust in Data Marketplaces.....	82
4.4.2.3. Consequences of Organizational Trust in Data Marketplaces.....	83
4.4.3. Fostering Organizational Trust in Data Marketplaces.....	84
4.4.3.1. Three Pillars	84
4.4.3.2. MPC Encryption and Trust.....	84
4.4.4. Moving Forward.....	85
4.5. CHAPTER 8. Secure Multi-party Computation (MPC)	87
4.5.1. EU Encryption Framework.....	87
4.5.1.1. ENISA Opinion Paper on Encryption	88
4.5.1.2. Eleventh Progress Report: Towards an Effective and Genuine Security Union	89
4.5.1.3. European Electronic Communications Code.....	90
4.5.2. MPC explained.....	91
4.5.2.1. Concept.....	91
4.5.2.2. MPC in the data marketplace context.....	93
4.5.2.3. Relevance	94
4.6. CHAPTER 9. Secure Multi-party Computation: Legal Questions & Answers.....	95
4.6.1. Liability for Wrongful Data-sharing	95
4.6.2. Liability in Decentral MPC Protocol.....	98
4.6.3. The Trustworthiness of MPC Protocol.....	99
4.6.4. Reliability of MPC Protocol.....	100
4.6.5. Assurances of Non-Identification.....	100
4.6.6. Legal Safety of MPC Protocol	101
4.6.6.1. Certification of MPC Processes.....	102
4.6.6.2. Evaluation of Encrypted and Personal Data	103
Concluding Note	104
References	104
Doctrine.....	104
Case law.....	108
Legislations	108
Others	110
Annex.....	112
Chapter 1. The Value of Data.....	112
Chapter 2. Data Marketplaces	120
Chapter 3. Ethical Guidelines.....	124
Chapter 4. The Protection of Personal Data	127
Chapter 5. The Protection of Non-Personal Data.....	131
Chapter 6. The Valuation of Data.....	136

Chapter 7. Organizational Trust	142
Chapter 8. Secure Multi-Party Computation	147
Chapter 9. Secure Multi-Party Computation: Legal Q&A	152

List of Abbreviations

Art	Article
CJEU	Court of Justice of the European Union
DRM	Digital Rights' management
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Cybersecurity
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	Privacy-enhancing technologies
TEU	Treaty on European Union
TFEU	Treaty on the functioning of the European Union

List of Figures

Figure 1. Safe-DEED Research Goals	23
Figure 2. Roles in data marketplaces ecosystems, adapted from Spiekermann (2019).....	25
Figure 3. Organizational trust versus interpersonal trust	78
Figure 4. Organization trust and MPC encryption	85
Figure 5. Organizational trust: summary.....	86
Figure 6. MPC explained.....	92
Figure 7. Roles in data marketplaces ecosystems, adapted from Spiekermann (2019).....	93

Introduction

Is data really “the new oil”? How do companies make money off of your internet usage? What may the future of the European digital economy look like?... These questions are just a handful of issues that shall be at the forefront of this syllabus.

This teaching module predominantly aims to educate the reader on the multiple challenges hampering a data-driven European economy's advancement and possible resolutions to advance thereto.

Just to name of few considerations: what role can you as an individual play in the digital advancement of the EU? What rights do you have concerning your data? What exactly is that “GDPR”-buzzword you continuously see mentioned in your mailbox? And can you possibly make any profit off of your personal data? These are just a number of the sub-questions which will be addressed in this syllabus.

Of course, this syllabus will merely provide an elemental insight into these issues. In essence, it aims at outlining the fundamental burdens and potentialities in advancing toward a more secure and well-functioning European data-driven economy. Whilst doing so, fields such as privacy law, cryptography and data science will be assessed.

The main insights in this document result from the research of the Safe-DEED consortium, an interdisciplinary research team of cryptographers, data scientists, engineers and jurists. The members of the Safe-DEED consortium are: the Know-Center, The Research Studios Austria Forschungsgesellschaft mbH, Eurecat, KU Leuven, TU Delft, Infineon Technologies AG and LSTech Espana SL.

The following slide summarize Safe-DEED's general and specific research goals. The subsequent slide provides general information concerning the lecture series.



Project & Goals

- **Interdisciplinary consortium**
Data scientists, jurists, encryption experts and engineers
- **Overall Goals**
Overcoming current impediments to acceptance and growth of data marketplaces in the European Union, thus moving toward a more data-enabled European economy
- **Specific research goals:**
 1. Data valuation protocol: empowering *all* data owners
 2. Fostering trust in data markets
(encompassing a sound legal & ethical framework)
 3. Enabling large-scale secure multi-party computation



Lecture series: general information

- **What?** Teaching module
- **How?** Syllabus & 9 video lectures (10min. each)
- **Why?** (I) Raising awareness about value of data & data marketplaces, from an interdisciplinary angle
(II) Creating a more direct and engaging format for syllabus and teaching material
- **For Whom?** Students & Consortium
- **By Whom?** KUL CiTiP Researchers



Syllabus Structure Overview

1.1 Structure

1.1.1 Schematic Overview

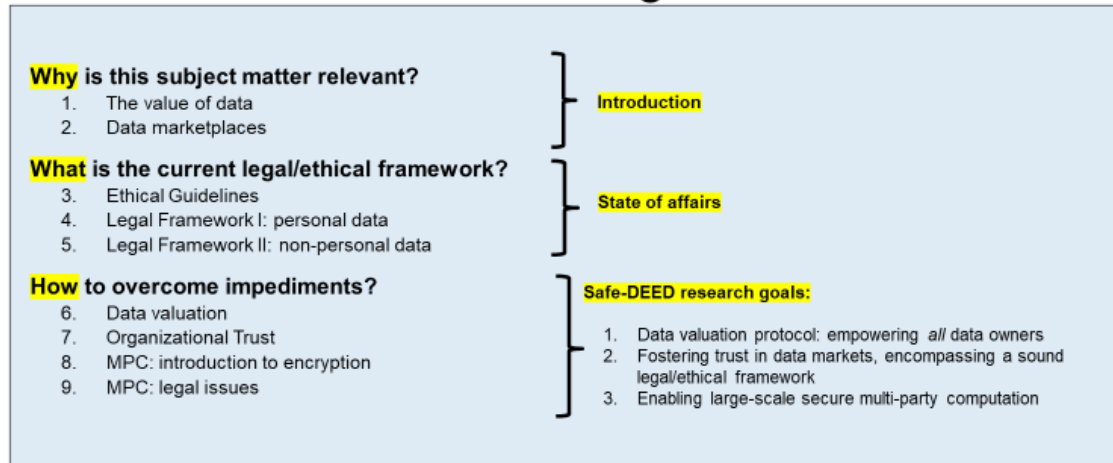
As mentioned before, this syllabus's overall theme is “the advancement toward a data-driven European economy”. This syllabus consists of nine chapters, each focusing on a different topic. Subject-wise, these nine topics can be divided into three overarching parts.

Part I The advancement toward a European data-driven economy: Introduction	
Chapter 1	The Value of Data
Chapter 2	Data Marketplaces
Part II The advancement toward a European data-driven economy: Interdisciplinary Considerations	
Chapter 3	Ethical Guidelines
Chapter 4	The Protection of Personal Data
Chapter 5	The Protection of Non-Personal Data
Part III The advancement toward a European data-driven economy: Challenges & Opportunities	
Chapter 6	The Valuation of Data
Chapter 7	Organizational Trust
Chapter 8	Secure Multi-Party Computation Encryption (MPC)
Chapter 9	MPC: Legal Questions and Answers
Conclusion	

The following slide provides an alternative formulation of the lecture series' structure and goals.



Lectures series: overview & goals



1.1.2 Video sessions

In addition to this syllabus, nine accompanying video lectures have been provided. Each video session has been presented by a researcher from the KU Leuven Centre for IT & IP Law (CiTiP) and covers one chapter of this syllabus. These video sessions will entail visual presentations (i.e., PowerPoint slides) with keywords and the syllabus's main takeaways. It is hoped that this combination of the syllabus and the video series makes the lecture series more engaging and accessible to all. The PowerPoint slides used per lecture have been added in the annex at the end of this syllabus.¹ It is encouraged to consult these slides whilst studying this syllabus, as these provide a concise overview of each chapter's key points.

1.2 Lecture Series' Dissemination Plan

This lecture series (i.e., syllabus and video recordings) will be disseminated across two main channels: a “formal” and an “informal” route.

The **formal route** encompasses the distribution of the lecture series through the official channels of the KU Leuven. The student platform of the KU Leuven is called “Toledo”. Hereon, students have access to their course materials, emails, and all documentation relevant to their course of study. In particular, this lecture series seems to suitably fit into the content of the course “Technology and Law” (B-KUL-C01M6A). This concerns a new course – introduced three years ago – which is mandatory for law students in the first year of their master's. In essence, this course aims to teach students to reflect upon the interconnection between law and technology critically. Doing so addresses topics such as privacy-enhancing technologies, security issues, data ownership, and data protection. These broad issues have also been dealt with by this lecture series. Therefore, this series may serve as an interesting practical added value on top of the technical introduction offered to law students in the course curriculum. In discussion with faculty members, it has been decided that the relevant chapters of this syllabus should be added to the “additional information” folder of each lecture. In addition, this “Technology and Law” course also entails a “resource page for students” and an event page. The entire lecture series is expected to be distributed hereon as well. Lastly, biweekly faculty newsletters are sent to all students on Toledo. Promoting the lecture series this way may reach a vast number of additional students. With regard to the latter, a request shall be sent to all relevant faculties at the KU Leuven.

A second distributive route is more **informal**, i.e., shall make use of channels affiliated with the KU Leuven. The first way concerns the dissemination via student organizations. There are 101 recognized student organizations at the KU Leuven, 36 of which represent faculties, courses of study, and 65 unaffiliated organizations. A number of these organizations' activities deal with the issues inherent to the Safe-DEED research. A first example concerns UNYA (The United Nations Youth Association),

¹ See *infra* ‘Annex: PowerPoint Slides’

which is organizing a so-called “tech trilogy”, i.e. a three-part course on technology and society. Another relevant student association with similar activities is KULMUN (KU Leuven Model United Nations). A third notable organization is VRG (the Flemish Law Society), which is continuously aiming to foster its members’ tech-savviness by organizing sporadic lecture series on law and technology. Other relevant organizations are ELSA Leuven (the European Law Student Association), EKONOMIKA (the Economics Students’ Association), EMERGENT (an unaffiliated association focused on “data driven and analytical decision-making”), CAPITANT (an unaffiliated association focused on finance and economy) and AFT (Academics for Technology). The representatives of each organization's contact details have been assembled, all of whom shall be contacted once the video sessions have been recorded. Ideally, the Safe-DEED lecture series might be implemented in (one of) these organizations’ activities.

On top of these student organizations, there are several additional alternative routes via which the lecture series may be distributed. One concerns the “Leuven AI Forum”, an event where law students and AI students come together to discuss new technologies' legal implications. In this sense, this series' second part (chapters three to five) may be useful. Another informal channel concerns “KU Leuven Kick”, an entrepreneurship organization in Leuven that may be especially interested in the functioning of data marketplaces (chapter two). Moreover, there are currently plans to potentially organize optional extracurricular workshops for law students on data science. Furthermore, the lecture series shall be promoted during any informal gatherings in the subsequent months, one of which concerns an upcoming research lunch on “law, data and technology”.

2 PART I. THE ADVANCEMENT TOWARD A EUROPEAN DATA-DRIVEN ECONOMY: INTRODUCTION

2.1 CHAPTER 1. The value of data

Within the Safe-DEED research, WP4 has extensively researched the subject matter of data valuation. Hence, this chapter summarizes several key findings of this earlier research and transposes some writings of previous deliverables. These concern D4.1, D4.2, D4.3, and D4.4, and may be consulted at <https://safe-deed.eu/deliverables/>.

2.1.1 Value?



Up until 2009, energy and oil companies dominated the top-10 of the world's most valuable firms. A decade later, in 2020, data-centric companies, such as Microsoft, Amazon.com, the Alibaba Group, Apple Inc., and Alphabet Inc. (Google's parent company), are exclusively sharing the top-5, with Facebook Inc. and Tencent trailing not too far behind in the top-10.² The global economy increasingly relies on data, with businesses adopting data-enabled decision-making practices in analytics or machine learning. So much so that this has reshaped the paradigm for data production and consumption – including the perception of data as an asset, subject to transactions, the subsequent appearance of new stakeholders whose activity is based on the acquisition, re-packaging and selling of

² The rankings we refer to are retrieved from Wikipedia's compilation of Financial Times Global 500 lists from 1996-2020. URL: https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization#2020

data sets, and finally the steady emergence of data markets. In this context, a question is becoming increasingly pervasive: “*what is the value of my data?*”³



To answer this question, we first need to understand what is “data value”. While the ranking just presented makes it clear that data generates value, the mechanisms in which this happens are still very much unclear. Organisations are only starting to think about the necessity to formalise these concepts. Until now, preoccupations around the value of data were only triggered by large impact events – mergers and acquisitions, bankruptcy, data transactions, data breaches – which is perhaps why comparisons between data and other commodities (oil, gold,...) or intangible assets have become so common.

Chapter six of this syllabus will deal with the valuation of data in depth.⁴ However, the remnant of this first chapter will primordially serve as an introduction to the concept of data and its value. It will offer an initial insight into the various types of data, some core concepts in data science, and why it is more important than ever to comprehend the vast importance of data value.

³ This evolution, as well as the subsequent issue of ‘data valuation’ has been described in length in another deliverable within the Safe-DEED Research. See Safe-DEED Deliverable 4.3, p. 7.

URL: https://drive.google.com/file/d/1ig5TJetnCTjvA6_6C091cD1MBOVVUkJ/view

⁴ *Infra* Chapter 6 ‘The Valuation of Data’.

2.1.2 Data?

An astounding ninety percent of all the world's data has been created in the past two years alone, and its value is rapidly rising.⁵ It thus seems essential to first dwell on some key concepts and definitions inherent to the data jargon.

Let's start with the very basics: what is data? Data can best be defined as “*characteristics or information - usually numerical - that are collected through observation*”.⁶ Hence, in a more technical sense, data concern a set of values of quantitative or qualitative variables regarding one or more persons or objects, whilst the singular “*datum*” refers to a single value of a single variable.⁷



Following this, numerous (sub)types of data can be discerned, depending on the metrics and criteria used. One common classification concerns the differentiation between personal data and non-personal data. Personal data can be defined as “*any information relating to an identified or identifiable natural person*”.⁸ On the other hand, all data falling outside this scope is automatically qualified as non-personal data. Chapters four and five will further expand on (the relevance of) this discrepancy.⁹

Another commonly used term concerns “big data”. This notion suffers from being too broad to be useful.¹⁰ It is more helpful to read it as “*sets of data whose size goes beyond the reach of commonly used software tools to capture, manage, and process the information within a reasonable period of*

⁵ Bello-Orgaz et al (2016). Social Big Data: Recent achievements and new challenges. Information Fusion, 28: 45–59; see also: <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=1ef989d60ba9>.

⁶ OECD Glossary of Statistical Terms. OECD. 2008. p. 119. ISBN 978-92-64-025561.

⁷ ‘Statistical Language - What are Data?’. Australian Bureau of Statistics. 13-07-2013. URL: <https://www.abs.gov.au/websitedbs/D3310114.nsf/Home/Statistical+Language+-+what+are+data>

⁸ European Parliament and Council of European Union (2016) Regulation (EU) 2016/679, Art 4.

⁹ *Infra* Chapter 4 ‘The Protection of Personal Data’ and Chapter 5. ‘The Protection of Non-Personal Data’.

¹⁰ Cumbley and Church (2013). Is “Big Data” creepy? Computer Law & Security Review, 29: 601–609.

time”.¹¹ The possible creation of value from big data fundamentally relies on its key characteristics. These characteristics of big data are commonly described as the so-called “four V’s”: velocity, volume, variety, and veracity.¹² A brief description of each “V” has been provided in the following table:

The four V’s of big data

Characteristic	Description
Data Volume	The amount of data collected and available.
Data Velocity	This entails either: <ol style="list-style-type: none"> 1. The rate at which data is accumulated; 2. The speed at which data arrives; 3. The rate at which data gets purged; 4. The frequency at which data changes; and/or 5. The rate at which data becomes outdated.
Data Variety	The types of data required for analysis; either: <ol style="list-style-type: none"> 1. Structured data: databases, Excel Tables,... 2. Unstructured data: video, audio, text,...
Data Veracity	The accuracy, precision and reliability of the data, based on the collection methods and tools.

2.1.3 Data Value?

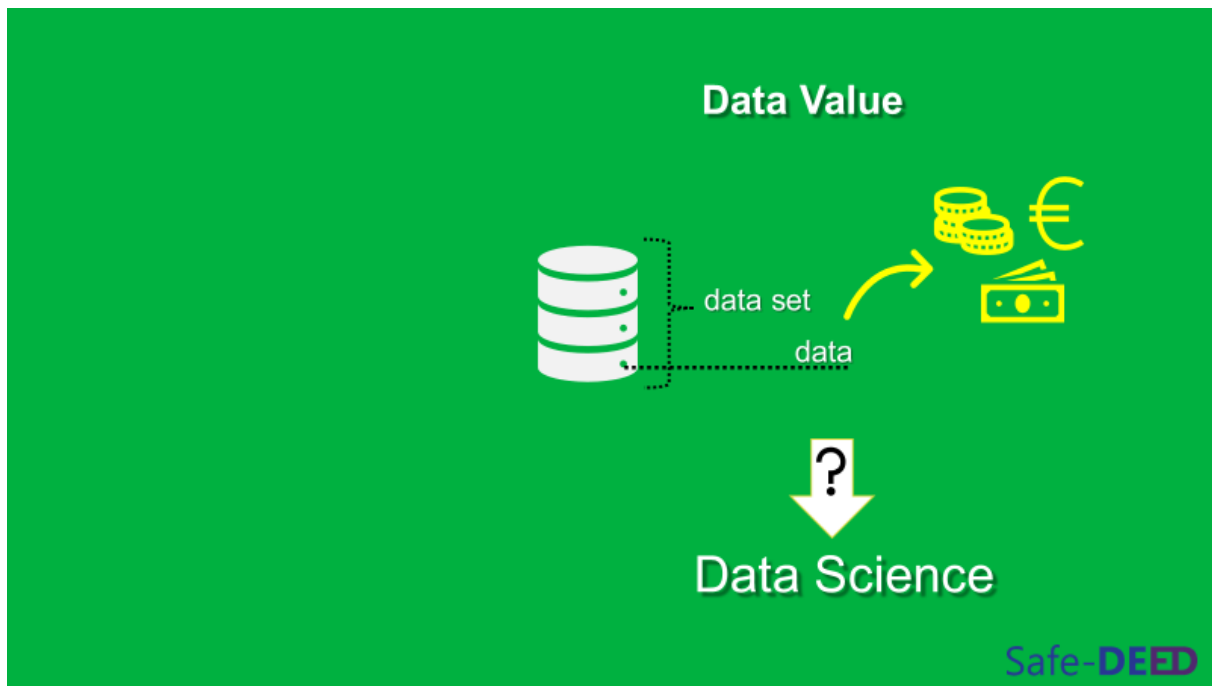
There is currently increased attention to a fifth “V”: the “value” of data. The data value can best be defined as “*the value derived from the processing of data, which in its turn contributes to decision making and problem-solving*”.¹³

Hence, the question arises of how we can process data – despite its volume, velocity, variety, or veracity- to create value out of the data assembled effectively. This situation is where data science comes into play.

¹¹ Definition retrieved from ‘2.3. Definition of Big Data’ in Evodevo srl and the European Economic and Social Committee, ‘Study on the Ethics of Big Data: Balancing Economic Benefits and Ethical Questions of Big Data in the EU Policy Context’, p. 15-20, 36. URL: <https://www.eesc.europa.eu/sites/default/files/resources/docs/qe-04-17-306-en-n.pdf>

¹² *Ibid.*, p. 15-16.

¹³ Definition retrieved from IGI Global Publisher of timely Knowledge. URL: <https://www.igi-global.com/dictionary/big-data-issues-and-challenges/41415>



Data science is an interdisciplinary field that uses scientific methods, processes, algorithms, and systems to extract knowledge and insights from data.¹⁴ There is a multitude of techniques and methods which data scientists are using to extract insights (and subsequently, value) from data.

Generally speaking, we can divide a data science project into six consecutive steps:

1. **Data Collection:** this first step in the process concerns the mere assembly of unstructured data utilizing social media monitoring, transactional data tracking, online marketing analytics,... The purpose of this first step is simple yet fundamental: the collection of relevant data into relevant datasets (i.e. “packages of data”).
 2. **Data Storage:** the collected data is stored in a storage medium. In the technical context, a storage medium concerns the server of a general-purpose computer. If one wants to store data for doing data science, the initial task is to have a clear-cut idea of what goals you ultimately wish to achieve with the data stored. This primordial question is often referred to as “OKR”: objectives and key results in the software industry.¹⁵ OKR provides a thorough strategy to only store and ultimately measure the data which matters most to the final objective and perceived results of the data science project.
 3. **Data Cleansing:** The stored data will then be cleansed; i.e. the detection and correction (or removal) of incorrect, incomplete or inaccurate parts of the data from the database
- **Data Aggregation:** The data collection, storage, and cleaning stages altogether come down to the so-called “aggregation” of data, which concerns the process of gathering data and presenting it in a summarized format. The data may be gathered from multiple data sources to

¹⁴ Dhar, V. (2013). "Data science and prediction". *Communications of the ACM*. **56**(12), 64–73.

¹⁵ <https://towardsdatascience.com/the-power-of-goal-setting-for-your-data-science-project-9338bf475abd>.

combine these data sources into a summary for data analysis. Effective data aggregation thus helps to minimize performance problems during the subsequent data analysis stage.

4. **Data Analysis:** The aggregated data will then be analyzed. Data analysis concerns the process of inspecting, cleansing, transforming, and modeling data to discover useful information, informing conclusions, and supporting decision-making.¹⁶

Small and medium-sized enterprises often use third-party tools to collect and analyze data relevant to them. A well-known example of such a third-party tracking service is Google Analytics, which provides website owners with a visual overview of the number of website visitors, the amount of clicks on each website page, etc. Hence, this service collects all relevant data. It assembles it in datasets that may be of use for the company at issue.

5. **Data visualization:** The analyzed data will then be visualized, which concerns the graphical representation of information and data.¹⁷ Using visual elements like charts, graphs, and maps, data visualization tools provide an accessible way to see and understand trends, outliers, and patterns in data.
6. **Data-driven Decision:** lastly, the action is taken based on the insights gathered from previous steps.

It should be emphasized that this concerns a rather rudimentary overview of the data science process. Nevertheless, these six steps provide an elemental insight into the big data life cycle used to extract value from data. This cycle is at the basis of the core business models of companies such as Google and Facebook. It has largely allowed these companies to grow exponentially throughout the previous decades.

2.1.4 Data-enabled Economic Development

2.1.4.1 Current Barriers

The foregoing overview has briefly demonstrated the data science process, which intends to extract value from large quantities of data or big data. Moreover, it has been shown that the value of data is increasingly fueling the global economy. Following this, one may wonder how digital data is exchanged. In other words: how does data reach the relevant actors who may be interested in using it to optimize their business? The resolution to these questions can be found in data marketplaces, which concern marketplaces where data are exchanged. They also allow for the “*generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation of data enabled by digital technologies*”.¹⁸ The next chapter of this syllabus will expand on this subject matter.

¹⁶ Definition retrieved from Wikipedia: https://en.wikipedia.org/wiki/Data_analysis#cite_note-1.

¹⁷ Sadiku, M. *et al.* (2016). ‘Data Visualization’. *International Journal of Engineering Research and Advanced Technology* (IJERAT). 12. 2454-6135.

¹⁸ European Data Market study, SMART 2013/0063, IDC, 2016.

Building a European Data Driven Economy

Challenges:

1. Lack of coordination
2. Lack of infrastructure/funding
3. Shortage of expertise/skills
4. Legal Complexity

Safe-DEED

Against this backdrop, there are plenty of interdisciplinary barriers that still hamper the acceptance and development of data markets in the European Union (EU). Consequently, these barriers equally impede the overall growth of a data-driven European economy. Nonetheless, a robust data-driven economy would undeniably enhance citizen well-being, create numerous new business opportunities and enable more innovative public services. For this reason, the EU Commission has laid down a Communication on “Building a European data economy”.¹⁹ Herein, the Commission mentions four specific burdens to the growth of a data-driven EU economy: (I) the lack of cross-border coordination; (II) insufficient infrastructure and funding opportunities; (III) a shortage of data experts and related skills; and (IV) a complex legal environment.

2.1.4.2 Safe-DEED Project

As a response, the Commission has equally proposed several potential resolutions to these issues. These include *inter alia* the need for transparent rules on data ownership and liability in the digital context, creating a climate of open data exchange (in this context, one may think of data marketplaces), and establishing a network of data processing facilities in the EU.

Against this backdrop, Safe-DEED brings together partners from cryptography, data science, business innovation, and the legal domain to overcome some of these core challenges. More concretely, the Safe-DEED project intends to achieve five interdisciplinary research objectives: (I) the empowerment of all data owners; (II) the contribution to a more sound legal and ethical framework; (III) the fostering of economic growth; (IV) the fostering of trust in data marketplaces; and (V) the possibility of large-scale multi-party computation. Ultimately, these research goals should enhance a safe data-enabled

¹⁹ 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-content/EN/TXT/?uri=COM:2017:9:FIN>>, accessed 22 November 2020.

economic development in the European Union, allowing for a more successful data-driven EU economy.

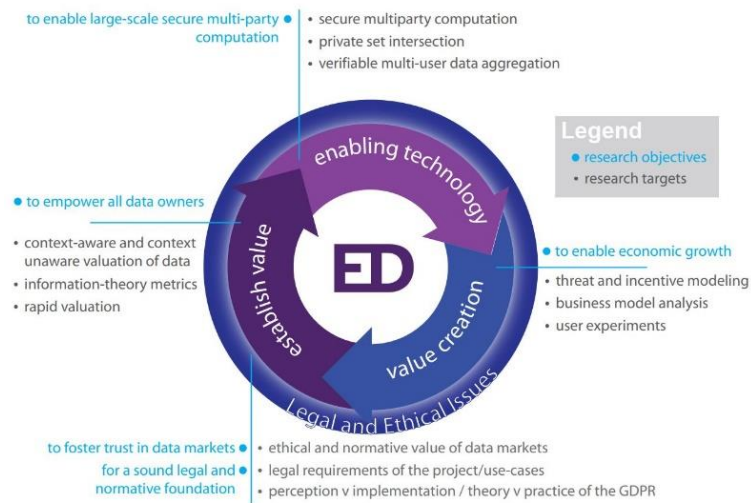


Figure 1. Safe-DEED Research Goals²⁰

The next chapters will provide a better understanding of the various research objectives. It should be stated that these objectives are heavily interlinked and build further upon one another. In the main, however, each respective chapter shall primordially focus on the following research goals:

Syllabus Chapter Number	Safe-DEED Research Objective
Two	The empowerment of all data owners
Three, Four, Five	The contribution to a more sound legal and ethical framework
Six	The fostering of economic growth
Seven	The fostering of trust in data marketplaces
Eight, Nine	The possibility of large-scale multi-party computation

²⁰ Official representation of Safe-DEED's research goals, as visualized on: <https://safe-deed.eu/>.

2.2. CHAPTER 2. Data marketplaces: an introduction

The previous chapter has highlighted the economic importance of extracting value from data and the general process at its core. This second chapter will assess the concept of data marketplaces and the advancement of an EU data-driven economy. A first subchapter shall provide a concise yet essential understanding of data marketplaces. Subsequently, a brief overview of the main actors on marketplaces. A final subchapter will deal with the relevance and significance of data marketplaces regarding the advancement toward a data-driven economy.

Within the Safe-DEED research, WP2 has extensively researched the subject matter of data marketplaces. Hence, this chapter summarizes several key findings of this earlier research and transposes some writings of previous deliverables. These concern D2.1 and D2.2, and may be consulted at <https://safe-deed.eu/deliverables/>.

2.2.1. What?

A data marketplace can best be understood as a virtual platform where users buy or sell different data sets from several sources, the data providers. Think of a stock exchange, but for data, where buyers and sellers can determine the price of data based on the supply and demand. A true comprehensive data marketplace like this, where individuals and all private actors can sell their data in this open model, does not yet exist today. However, currently, many fragmented data marketplaces allow both individuals and companies to sell and buy particular data sets. Notable examples of personal data marketplaces concern Datum, Fysical, and DataWallet. Prominent illustrations of B2B (“business-to-business”) data marketplaces are AudiencePrime, Salesforce, Dawex, Snowflake, and Adobe Audience Manager Marketplace. Nevertheless, all these marketplaces are still widely fragmented, not as systematically regulated as they should perhaps be, and their existence is vastly unknown to the broad public. The lack of coherent regulation of data marketplaces is a shame since they offer important economic incentives for both individuals and companies, as discussed in this chapter.

At the moment, data marketplaces are thus mostly cloud services where predominantly businesses can upload data to the cloud. Those platforms enable self-service data access while ensuring security, consistency, and high data quality for both parties.

KUL in Safe-DEED: Identification of the Context

EU Data Market Place

European Commission
Communication "Building a
European Data Economy"

Where digital data is exchanged as products or services derived from raw data – on the economy as a whole. It involves the generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation of data enabled by digital technologies



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



Data marketplaces can thus be considered digital platforms that enable organizations to share and sell datasets.²¹ The data marketplace commonly governs access to the data, manipulation, and the use of the data by other entities, employing a range of standardized or negotiated licensing models. On top of that, data marketplaces also offer complementary applications and services such as data visualizations, data valuation, and data analytics. Hence, such platforms would create value to its participants by lowering transaction costs, stimulating innovation by third-party developers, and generating network effects.

2.2.2. Who?

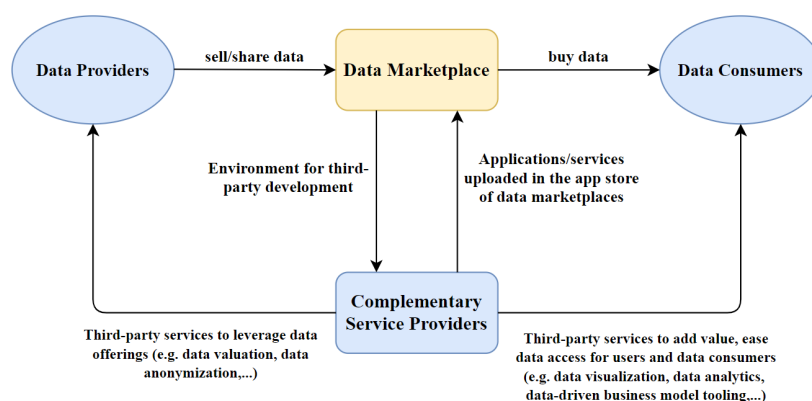


Figure 2. Roles in data marketplaces ecosystems, adapted from Spiekermann (2019)²²

²¹ Spiekermann, M. (2019). Data Marketplaces: Trends and Monetization of Data Goods. *Intereconomics*, 54(4), 208-216.

²² Figure made by WP3 in light of Safe-DEED D3.5; inspired on: Spiekermann, M. (2019). Data Marketplaces: Trends and Monetization of Data Goods. *Intereconomics*, 54(4), 208-216.

The visualization above has been inspired on the research work of Spiekermann.²³ It visualizes the main actors involved in the data marketplace ecosystem. The core function of data marketplaces is to match between two sides of the market. On the one side, data providers want to monetize their data by sharing/selling it via data marketplaces. Then, data consumers, on the other side want to buy the data products offered by data providers and therefore, access data marketplaces and look for available data. A simple illustration could be the following: one may think of a food blog which writes blog posts on all sorts of granola. A granola manufacturer may be interested in knowing which blog posts attract most visitors, and what granola types are the most popular. Hence, the blog owner could sell its website traffic data on a data marketplace, where the granola manufacturer can purchase these particular data sets and use the information extracted to further develop its business strategy, distribute personalized advertisements, and so on. The blog owner is the data provider, whilst the manufacturer is the data user (also often referred to as “the data consumer”). In its simplest form, data marketplaces thus serve as data-exchange platforms between the provider and user.

Other than that, data marketplaces also provide an environment for complementary service providers, which join the platform to develop data-driven applications and services. Examples include data anonymization, data valuation, data visualizations, and data analytics. These applications and services are uploaded in the application store provided by data marketplaces, which data providers can use to leverage data offerings or by data consumers to add value to the data they bought. Hence, data marketplaces equally serve as platforms that enable the aggregation and analysis of data, thus lowering potential burdens in the data value creation process.

2.2.3. Relevance

What are the benefits of data marketplaces? Why should companies make use of them? Well, data marketplaces benefit both data providers and data users. Let’s look into some key advantages on both sides.

Firstly, data markets provide benefits to data users (businesses that aim to buy data for value creation). Marketplaces, namely, provide them with access to data from external sources. This data is aggregated and optimized for use by external organizations (i.e., the complementary service providers), so it tends to be clean, well-presented and easily accessible for data users. A second benefit concerns the speed at which data users can derive insights from data marketplaces, as the gathering of data on the marketplace makes data collection less burdensome. Hence, businesses can focus more on data analytics (if not yet done by complementary service providers or third-party sources, as touched on in the previous chapter) and other essential business processes. Data marketplaces also frequently allow providers to transfer their data to analytics tools and software systems easily. A well-known example concerns the Microsoft Azure DataMarket, allowing developers to access data via Excel and PowerPivot.

²³ *Ibid.*

A third benefit concerns the safe data sharing on data marketplaces. Ideally, marketplaces should serve as a trustworthy and secure data exchange environment. In practice, however, there currently seems to be some degree of lack of organizational trust in data markets. This issue shall be dealt with in chapter seven. Furthermore, encryption techniques, such as secure multi-party computation, maybe of essential value in lifting these trust and security concerns. In the final two chapters of this syllabus, the encryption's usefulness to ensure security on data marketplaces will be expanded on.

Benefits for Data Users

1. Access to outside data
2. Speed
3. Safety, however:
 1. Trust problems
 2. Security issues

Safe-DEED

On the data providers' side, we can equally distinguish various benefits. An obvious first advantage concerns the ability for companies to generate revenue from data. Data marketplaces allow them to monetize data that they would otherwise not use or normally not have the facilities to process. Secondly, by selling data to businesses, providers can expect to get more personalized services in the future. Let's illustrate this with the granola example we've used before. Suppose a granola blog sells its website traffic data to a granola manufacturer. In that case this will allow the manufacturer to tailor their granola assortment to the consumer market's interests. As a result, more consumers will know about this particular granola assortment, which will drive more readers to the corresponding granola blog posts.

Consequently, this increased website traffic will provide the blog owner with even more detailed traffic data, which increases the quality of this data, making it even more lucrative for the data owner.²⁴ Hence the provision of data by data providers may equally entail economic benefits in the longer run. Thirdly, the sharing of data on marketplaces allows data providers to contribute to the overall entrepreneurial landscape. Many young companies and startups can emerge solely thanks to the data

²⁴ For more on data quality (metrics), see chapter 6. 'The valuation of data'.

collected and sold on marketplaces. Hence, this general economic advantage should not be overlooked against the backdrop of the EU data-driven economy's development.²⁵



2.2.4. Significance

Data marketplaces are taking off. As stated hereabove, their impact on the European data-driven economy ought not to be understated.²⁶ This tendency is fundamentally rooted in the steadily growing value of big data, as described in the first chapter.

Some numbers to illustrate the growing economic relevance of big data, alluding to the ever-increasing importance of data marketplaces on a global scale: 90% of companies say analytics is key to digital transformation. Moreover, the number of companies investing more than 500 million dollars annually in big data has grown from 12.7% in 2018 to 21.1% in 2019. In addition, companies spent about 187 billion (!) US dollars on data analytics in 2019 alone. Lastly, the global data market reached 26 billion US dollars in 2019.²⁷

Hence, the significance of big data and data marketplaces cannot be understated. Data marketplaces offer a promising enhancement of how data is traded between companies, and – potentially – even directly between the data subject (the individual) and the data user (though this aspect falls outside this teaching module). Data marketplaces offer data providers an incentive to share data that they might otherwise disregard and equally ease providing complementary services such as the aggregation and analysis of data. Multiple steps of the data sharing value chain are thus eased by using a data market

²⁵ Spiekermann, M. (2019). Data Marketplaces: Trends and Monetization of Data Goods. *Intereconomics*, 54(4), 208-216.

²⁶ *Supra* Chapter 1, 'The value of data'.

²⁷ Blake Morgan, '100 Stats on Digital Transformation and Customer Experience', URL: <https://www.forbes.com/sites/blakemorgan/2019/12/16/100-stats-on-digital-transformation-and-customer-experience/?sh=357f12d73bf3>

platform. Though these marketplaces generally benefit from developing a data-driven EU economy, there are still certain impediments to their acceptance and growth. As stated before, the lack of trust and security concerns are two common barriers. Chapters seven to nine will, therefore more thoroughly assess Safe-DEED's role in alleviating these concerns.²⁸

Before doing so, we will assess the data-driven EU economy from a broader and external perspective. In the next three chapters, we will consider the various ethical and legal considerations that should be taken into account whilst creating value from (personal) data. Firstly, various ethical guidelines shall be discussed.

²⁸ *Infra.* Chapter 7 'Organizational Trust', Chapter 8 'Secure Multi-Party Computation' and Chapter 9. 'Secure Multi-Party Computation: Legal Questions and Answers'.

3. PART II. THE ADVANCEMENT TOWARD A EUROPEAN DATA-DRIVEN ECONOMY: INTERDISCIPLINARY CONSIDERATIONS

3.1. CHAPTER 3. Ethical guidelines

In the previous two chapters, we have discussed the significant relevance of data (value) and how data marketplaces can contribute to data-value creation. In this third chapter, we take a brief step back and assess what general ethical guidelines should be considered in light of the progression toward a data-driven EU economy.²⁹

Within the Safe-DEED research, WP3 has extensively researched the subject matter of ethical guidelines. Hence, this chapter summarizes several key findings of this earlier research and transposes some writings of previous deliverables. These concern D3.1, D3.2, and D3.3 and may be consulted at <https://safe-deed.eu/deliverables/>.



Lecture 3: Ethical guidelines

Overview	Particular Ethical Challenges
<ul style="list-style-type: none"> Fundamental moral principles (autonomy, justice, beneficence,...) EDPS' ethics advisory group 2018 report, towards a digital ethics <ul style="list-style-type: none"> Socio-cultural shifts in the digital age (toward a scored society, digital subjects, convergence of human & machine,...) Ethical reflection for the digital age From foundational values to digital values (dignity, freedom, autonomy,... and trust) Digital ethics of the innovation ecosystem (innovation as ethics, data markets, digital property rights,...) Ethics guidelines for trustworthy AI 	<ul style="list-style-type: none"> Thinking ethically in the digital age <ul style="list-style-type: none"> Dignity of the person remains inviolable Personhood and personal data are inseparable Data commodification risks shifting value from persons to personal data Specific ethical challenges in dealing with personal data From an Impact assessment to a value assessment

Safe-DEED

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

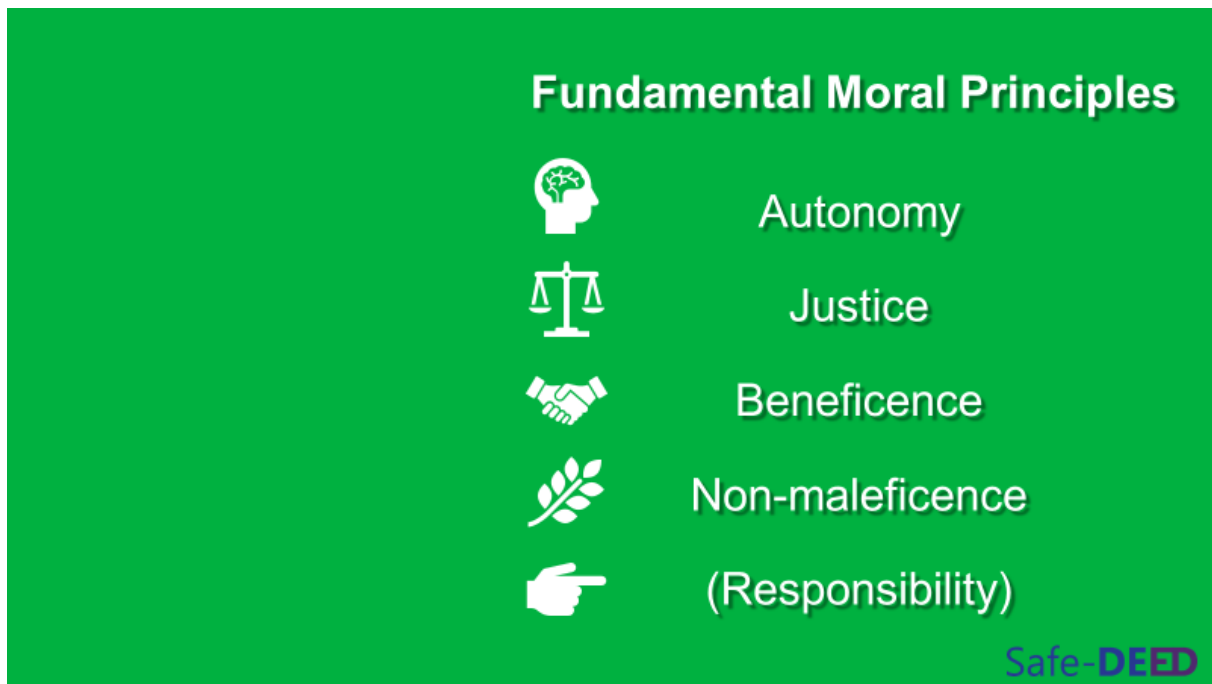


²⁹ Within the Safe-DEED research, WP3 has already extensively researched the subject matter of “ethical guidelines”. Therefore, this chapter merely summarizes the key findings of earlier research. D3.1, D3.2, D3.3 and D3.4 provide a more elaborate analysis of the ethical guidelines at issue. These deliverables can be consulted at: <https://safe-deed.eu/deliverables/>.

3.1.1. Fundamental Moral Principles

Legal and ethical principles have been influencing each other for many years. Generally, while the law offers the legislative setting that allows individuals, society, and authorities to carry out their activities, ethics provides the basis to build the normative architecture, supporting its interpretation and offering guidance. When it comes to the ethical guidelines, the overall aim is to ensure individuals and society's well-being.

In the first place, there are four generally accepted ethical-moral principles developed in the legislative context: autonomy, justice, beneficence and nonmaleficence. Additionally, the secondary principle of responsibility will be briefly presented.



The principle of autonomy - According to this principle, every individual has the fundamental right to self-determination. This principle comes with positive and negative obligations. As a negative obligation, the principle of autonomy implies that individual actions should not result in a constraint for others. As a positive obligation, the principle requires respectful treatment when revealing information and making independent decisions. The respect to privacy and confidentiality of information, together with the request for consent for processing personal information, are considered moral rules or obligations strictly linked to this ethical principle.

The principle of justice - The principle of justice requires that all individuals “*are entitled to have the same degree of attention and moral concern.*”³⁰ This implies that all persons must be treated with fairness according to their different needs, contributions, and vulnerabilities. In the privacy and data protection framework, the principle of justice and fairness is well represented in the GDPR. The subsequent chapter will elaborate upon this principle in the context of personal data protection.

³⁰ Verhenneman G, Vedder A, WITDOM, D6.1 – Legal and Ethical framework and privacy and security principles, p. 39, 2015, available at: <http://www.witdom.eu/deliverables>, accessed 01/12/2020.

The principle of beneficence - According to this principle, all individuals must contribute to personal and societal well-being. In the data market context, this implies that those in charge of processing activities (data aggregation, data analytics,...) have to ensure the security of the individuals that are affected by their activities.

The principle of non-maleficence - This principle originated from Hippocrates' oath ("*primum non nocere*" – first do no harm) and has been developed from biomedical ethics. The principle implies that individuals have a duty not to cause harm to others insofar as it lies within their power to do so without undue harm to themselves, their vital health, and security interests.³¹



The (secondary) principle of responsibility - This principle requires that each partner involved in a given project should behave and fulfill its moral obligations, which stem from its role in a project, at the best of its abilities. Such a principle gives each member of the data value chain responsibilities for the work they are carrying out and the consequences that might come from it. The principle of responsibility also implies that the duties have to be equally and fairly divided among the members in an interoperable environment.

³¹ Verhenneman G, Vedder A, WITDOM, D6.1 – Legal and Ethical framework and privacy and security principles, p. 6, 2015, available at: <http://www.witdom.eu/deliverables>., accessed 01/12/2020.



Applying Ethical Principle to Safe-DEED Consortium



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



3.1.2. Digital Ethics

In 2018, the European Data Protection Supervisor (EDPS) has issued a report on digital ethics.³² The European Data Protection Supervisor (EDPS) authority is the EU body in charge of monitoring and ensuring the protection of privacy and personal data in processing activities by EU institutions. Besides this function, the EDPS provides opinions and advice to EU institutions and agencies regarding their legislative initiatives that might impact privacy and data protection.

During the last years, ethics has been a hot topic on the EDPS' agenda. Against this backdrop, the EDPS has published a Report on Ethics in the digital age. In this Report, the EDPS describes how the new technological trends are reshaping the relationship between technology and human values.

³² Ethics Advisory Group 2018 Report, Towards a digital ethics, available at < https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>, accessed 01/12/2020.

3.1.2.1. Socio-Cultural Shifts in the Digital Age

Seven shifts that urge the need to redefine digital ethics



Concretely, the EDPS Ethics Advisory Group has described the effects of digital innovation on society and identifies different “moves” that require policymakers' intervention. According to the Report, it is possible to observe seven shifts where there is a need to redefine digital ethics:

From individuals to digital subjects - The growing trend of profiling through algorithms resulted in a situation where individual identity is defined through digital patterns and constructs rather than through psychological, cultural, and moral qualities.

From analogue to digital life - Human life has always been interpreted by reference to specific socio, cultural and political activities. Enhanced reliance on digitalization and data leads to the conclusion that the social, cultural and political values contributing to developing personal identity may not necessarily be taken into account anymore.

From institutional governance to governability through data, a shift in governance has occurred in the last decade. From a society governed by institutional governments, democratically elected and accountable for their decisions, the governance shifted to algorithms and automated decision-making affecting citizens' life more than institutional governments ever could.

From a risk society to scored society - To address potential societal risks, institutions have always relied on data aggregation, even if with different gathering and collecting techniques. Nonetheless, government institutions' political decisions that have been taken so far about certain risks have also taken into account moral principles such as justice and fairness. Nowadays, algorithms can customize the risks and needs of every individual. The role of solidarity is consequently questioned by opaque social and credit scoring that undermines our society's social texture.

From human autonomy to the convergence of human and machine - The new frontier of technology is characterized by “autonomous machines” that can perform activities without human

interactions. Consequently, there is a shift from a period where technological tools were supporting human activities (e.g. GPS) to one where machines decide without human interaction.

From Individual responsibility to distributed responsibility - The availability of large amounts of data is affecting the concept of responsibility. The network and interconnected eco-system that characterize our daily life require to reconsider the idea of responsibility. Moreover, the discussion on algorithmic transparency and accountability is among the most vividly debated themes of our times. Simultaneously, the discussion on algorithms responsibility should never decrease or alleviate the responsibility of human agents.

From Criminal Justice to pre-emptive justice - One of the main purposes of criminal justice is to ensure security, safeguarding at the same time the human rights of anyone. Nowadays, the criminal justice sector's latest actions are focusing on techniques to predict criminal behaviour, using the output of big data-driven analysis and smart algorithms. This investigative trend generates concerns in relation to potential drawbacks that it may have on those subjected to investigative and coercive measures.

3.1.2.2.A Look into the Future



The ethical analysis made by the EDPS Ethics Advisory Group concludes by providing five political (non-binding) recommendations to support and develop the European values based on the ones embedded in the data protection framework:

1. Regardless of the changes that occur in society, the essential and inviolable **human dignity** has to be preserved;
2. **Personhood**, with his or her moral values and social and cultural characteristics, cannot be taken apart from his or her personal data;
3. **Freedom of choice** has to remain a pillar of society, and autonomous decision making cannot undermine such a principle;

4. **Accountability**, especially in the context of profiling should be fostered to avoid any form of discrimination; and
5. Data commoditization can lead to potential tensions if **human moral values** are not taken into account.



These five policy recommendations aim to fit the seven shifts mentioned above into a framework that strengthens the digital context's main ethical principles. These guidelines should be strongly taken into account while assessing the future advancement of a data-driven EU economy. As outlined in the introduction to this syllabus, chapters six to nine will highlight several ways in which the Safe-DEED project aims to overcome various impediments to developing a data-driven economy. It should thus be considered that each of these resolutions ought to both respect and proactively uphold these ethical considerations.

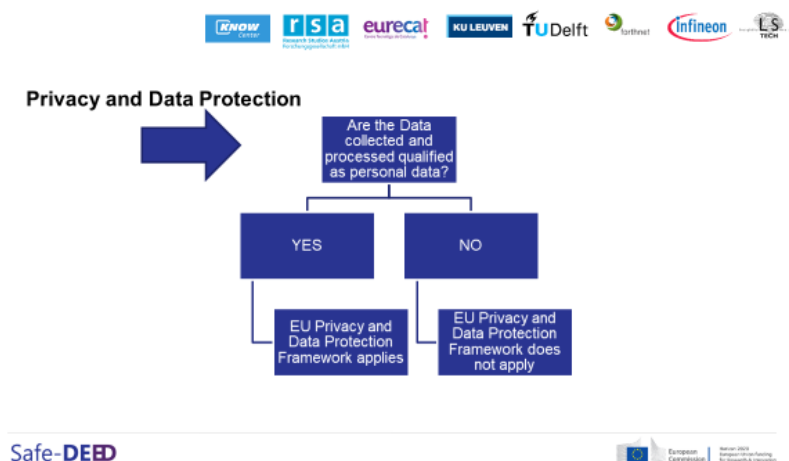
3.2. CHAPTER 4. The protection of personal data

Within the Safe-DEED research, WP4 has extensively researched the protection of personal data. Hence, this chapter summarizes several key findings of this earlier research and transposes some writings of previous deliverables. These concern D3.1 and D3.2 and may be consulted at <https://safe-deed.eu/deliverables/>.

3.2.1. Personal vs. Non-Personal Data

In moving toward a data-driven economy, the existing (European) legal framework must be well-respected. This chapter will describe the main legal principles related to the protection of personal data. The subsequent chapter will then deal with the legal requirements concerning non-personal data.³³

At first sight, the difference between personal data and non-personal data seems rather straightforward. In essence, personal data concerns any information relating to an identified or identifiable natural person.³⁴ Nevertheless, the precise determination of what can be deemed “personal data” is not always fully unambiguous. This shall be expanded upon further down in this chapter.



³³ Within the Safe-DEED research, WP3 has already extensively researched the subject matter of “Protection of personal data”. Therefore, this chapter merely summarizes the key findings of earlier research. D3.1, D3.2, D3.3 and D3.4 provide a more elaborate analysis of the ethical guidelines at issue. These deliverables can be consulted at: <https://safe-deed.eu/deliverables/>.

³⁴ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 4(1).

3.2.2. The Right to Data Protection

The right to data protection is mentioned in Art 8 of the European Convention on Human Rights (ECHR)³⁵ and Convention 108 on the Protection of Individuals concerning the automatic processing of personal data.³⁶

Art 8 ECHR states that: “1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”.³⁷

Nonetheless, this right is not absolute, meaning that restrictions may potentially be justified if strict conditions are met. This aspect falls outside the scope of this introduction.

3.2.3. The General Data Protection Regulation



The General Data Protection Regulation

- 25 May 2018
- Aims:
 - The regulation of the processing of personal data
 - The regulation of the free movement of personal data

Safe-DEED

³⁵ Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5.

³⁶ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

³⁷ Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, Art 8.

The EU has recently developed a new data protection framework to foster a stronger data protection regime, bringing forth the General Data Protection Regulation (GDPR).³⁸ This chapter shall assess what main provisions the GDPR entails and what objectives it aims to achieve.

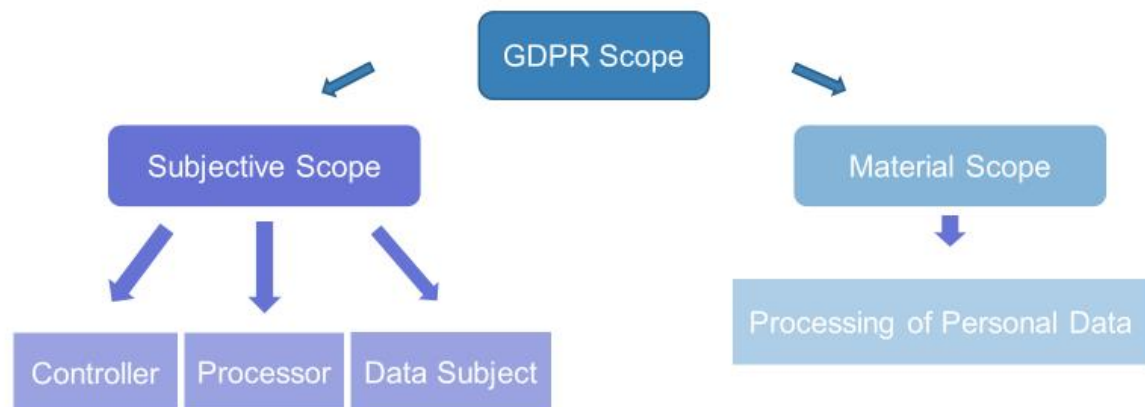
First, the GDPR is a regulation, and thus concerns a legal act of the EU that becomes immediately enforceable as law in all member states simultaneously instead of so-called “EU directives”. Regulations, thus, ensure the uniform application of its provisions amongst all 27 EU member states. The GDPR entered into force on 25 May 2018 and to regulate the protection of personal data and the free movement of such data.

The GDPR represents the cornerstone of the new Data Protection Framework, as it sets a higher standard for what concerns the protection of individuals. The new regime will enhance EU entities' business opportunities and, consequently, boost the EU Digital Single Market.

What and who does the GDPR apply to? In other words, what is its scope? The answer to this question can be found in Art 2(1) of the GDPR, which states that the regulation applies to *“the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system”*.³⁹ Materially, the GDPR thus applies to the processing of personal data.



KUL in Safe-DEED: GDPR Alphabetization



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



3.2.3.1. Material Scope: the Processing of Personal Data

3.2.3.1.1. Processing

First off, the notion of processing has been laid down in Art 4(2) GDPR and defines the activity of processing as *“any operation or set of operation which is performed on personal data or on sets of*

³⁸ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 4(1).

³⁹ *Ibid.* Art 2.

*personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”*⁴⁰ This broad definition describes all possible activities concerning data, from the initial collection to their erasure.

This definition of “processing” described in the GDPR seems to imply a comprehensive scope. Such an interpretation has been confirmed by the European Court of Justice (CJEU), the highest judicial organ in the European Union. The CJEU has affirmed that even activities carried out by a search engine concern personal data processing.⁴¹ Moreover, it has equally asserted that loading a web page and all operations necessary to make a webpage accessible to people can be regarded as a processing operation.⁴² Just imagine you search for information on Google or accept cookies to view a webpage. Both examples can be considered “processing” under Art 4(2) of the GDPR.

Material Scope: ‘Processing’



Art 4(2): any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means

Examples: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data

Safe-DEED

3.2.3.1.2. Personal Data

However, mere “processing” is not enough. The GDPR only applies to the processing of *personal data*. This brings us to the second element of the regulation's material scope: what is personal data? The answer hereto can be found in Art 4(1) GDPR, which defines “personal data” as “*any information relating to an identified or identifiable natural person*”.⁴³

⁴⁰ *Ibid.* Art 4(2).





⁴¹ CJEU Judgment of 13 May 2014, *Google v. Agencia Española de Protección de Datos (AEPD)*, C-131/12, ECLI:EU:C:2014:317, paragraph 60.

⁴² CJEU Judgment of 6 November 2003, *Criminal Proceedings against Bodil Lindqvist* (reference for a preliminary ruling from the Göta hovrätt), Case C-101/01, ECLI:EU:C:2003:596, paragraph 25.

⁴³ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 4(1).

Material Scope: 'Personal Data'

Art 4(1): 'any information relating to an identified or identifiable natural person'.

-  Any Information...
-  Relating to...
-  An Identified/identifiable...
-  Natural person



Safe-DEED

The Regulation also explains that an “identifiable natural person” is one who can be “*identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*”.⁴⁴

This notion as such consists of several sub-elements, which ask for some further explanation. Let's unpack this one by one.

Any information - It has been clarified that the nature of information is not relevant to determine if it is personal or not: any data that identifies a person can be considered personal data. Also, to determine if the information is personal, it is irrelevant if this data relates to an individual's private sphere or his professional activity. Lastly, the format or medium where the info is contained (paper or digitally stored) does not make any difference for the qualification.

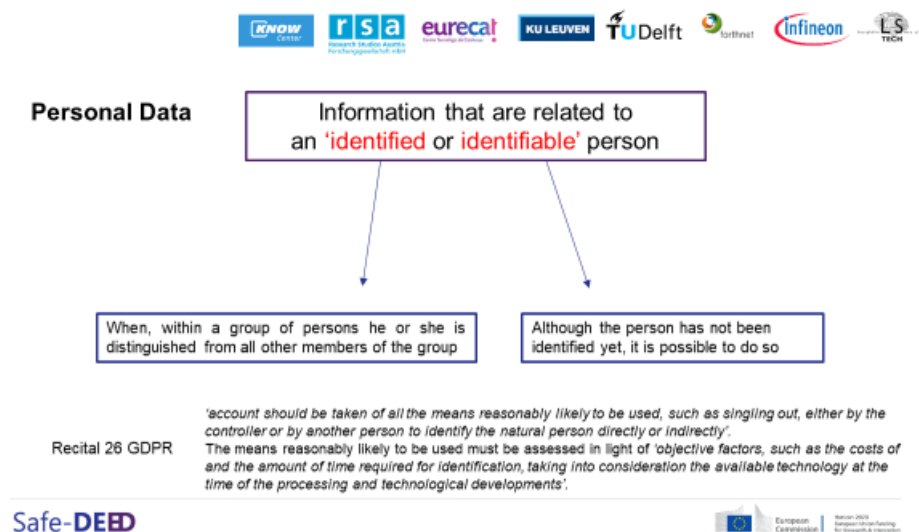
Relating to - There must be a relationship between a piece of specific information and a person. Such a link can be clear and direct but can also be not so self-evident. Elements to take into account are the content of the information (i.e., when it is about a person), its purpose (i.e., when the data are used or are likely to be used with the purpose to evaluate, treat in a certain way, or influence the status or behavior of that person) or result (i.e., when the data used are likely to have an impact on that person's rights and interests).

Identified/identifiable - An individual is identified when it is possible to pinpoint this individual within a group of people and distinguish him from the rest of the group. On the contrary, an individual is identifiable when he has not yet been identified but can be identified. Such identification process can occur directly, through the name (or additional information if the individual is not the only one with that name) or indirectly, using different pieces of information that combined could identify a

⁴⁴ *Ibid.*

specific individual. In general, it has been accepted that account should be taken of all the means reasonably likely to be used to identify the natural person, directly or indirectly. In turn, the means reasonably likely to be used must be assessed in light of objective factors, such as the costs of, and the amount of time required for identification, considering the available technology at the time of the processing and technological developments. In the latter context, it has been ruled that dynamic IP addresses, despite their randomness, constitute a piece of information that can allow the user's identification by the internet service provider.⁴⁵

Natural person - To fall into the scope of application of the GDPR, data must be related to a living person. Hence, the GDPR only offers protection to data related to flesh and blood persons, excluding companies or institutions. This natural person is the “data subject”.⁴⁶



3.2.3.2. Subjective Scope (of application): (Joint-) Controllers and Processors

After having identified the objective scope of application of the GDPR, it is necessary to shift the attention on the GDPR's subjective scope.

⁴⁵ CJEU Judgment of 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, C-582/14CJEU, ECLI:EU:C:2016:779, paragraphs 31-49.

⁴⁶ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 4(1).

Personal Scope



1. **Data Controller:** (Art 4(7)) 'The natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data.'
2. **Joint Controllers**
3. **Data Processor:** (Art 4(8)) 'natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.'

Safe-DEED

The GDPR lays down specific rules and obligations concerning actors involved in processing personal data, namely, the so-called “controller” and “processor”.⁴⁷ According to the different roles in personal data processing, the GDPR allocates responsibility for compliance and imposes specific rules to ensure the processing's security and confidentiality.

Controller - Art 4(7) of the GDPR defines a controller as “*the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*”⁴⁸ The controller thus determines “*the means and purposes*” (i.e. the “what” and the “why”) of the personal data processing.⁴⁹ The factual ability to control the processing should nevertheless be assessed since there might be cases where the controller's decision and activities might be made by someone else. Elements that should be taken into account when assessing one's capacity as “controller” include legal competence, implicit competence, and influence to control the natural or legal person empowered to make decisions. Situations may occur where multiple parties are involved as controllers with different degrees of participation. There are cases where several parties jointly decide the purpose and means of the processing. When this happens, the responsibility must be considered equally shared among the parties. We then speak of “joint controllers”.⁵⁰

Processor - The notion of processor is described in Art 4(8) GDPR. According to this provision, a processor is the “*natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.*”⁵¹ Controllers frequently assign parts of the operation to one or more processors. In some cases, they can also delegate the determination of the means of the whole

⁴⁷ *Ibid.* Art 5(1)(a).

⁴⁸ *Ibid.* Art 4(7).

⁴⁹ *Ibid.* Art 4(7).

⁵⁰ *Ibid.* Art 4(7).

⁵¹ *Ibid.* Art 4(8).

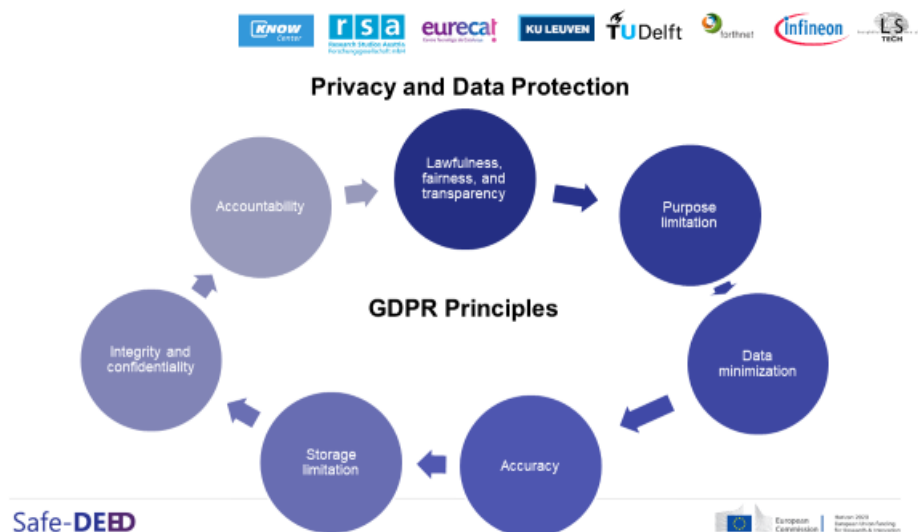
process to them. Considering the characteristics of the activities carried out by a processor, the EU legislator has imposed on them only limited obligations.

3.2.3.3. General Principles

In essence, the GDPR applies to all personal data processing, which is all information relating to an identifiable natural person. In the following subchapter, various rights and obligations will be discussed. Firstly, however, the fundamental general principles enshrined in the GDPR will be briefly presented.

The general principles in the GDPR include:

1. Lawfulness;
2. Fairness;
3. Transparency;
4. Purpose limitation;
5. Data minimization;
6. Accuracy;
7. Storage limitation;
8. Integrity and confidentiality; and
9. Accountability



Data controllers, while performing their activities, have to comply with these principles. The rationale behind these principles can be understood by referring to the ethical guidelines in the previous chapter.

General Principles



Lawfulness



Accuracy



Fairness



Storage limitation



Transparency



Integrity and confidentiality



Purpose limitation



Accountability

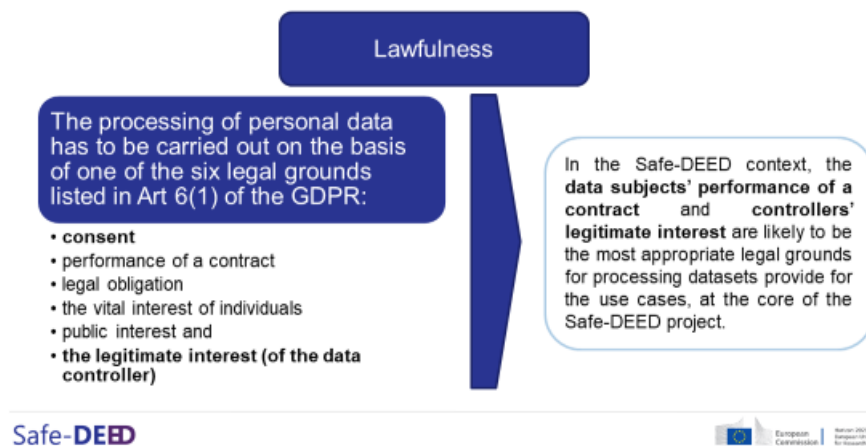


Data minimization



Safe-DEED

Lawfulness - To be lawful, the processing of personal data has to be carried out based on one of the six legal grounds listed in Art 6(1) of the GDPR: consent, the performance of a contract, legal obligation, the vital interest of individuals, public interest and the legitimate interest.⁵²



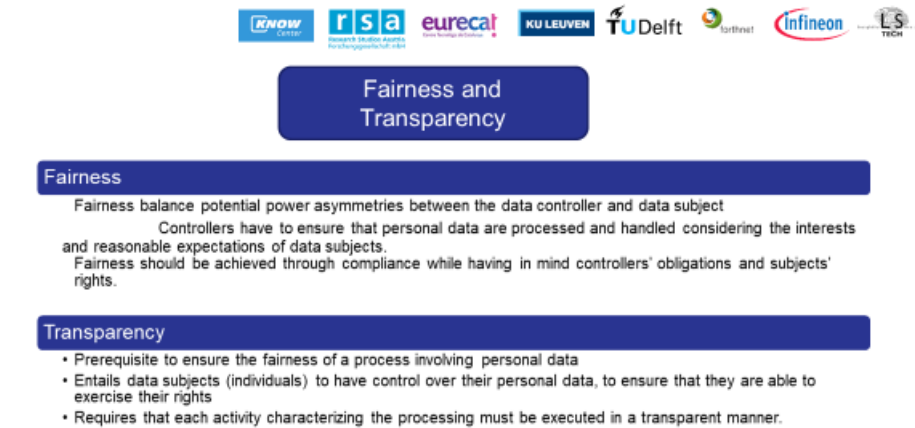
Fairness - Potential power asymmetries between the data controller and data subject need to be balanced, by striking a “*fair balance*” when applying data protection rules to a given situation.⁵³ Concretely, personal data must not be processed in a way which unreasonably infringes the fundamental rights and freedoms of data subjects and, in particular, their right to the protection of

⁵² Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 6(1).

⁵³ *Ibid.* Art 5(1)(a).

personal data. Therefore, fairness should be achieved through compliance while having in mind controllers' obligations and subjects' rights.

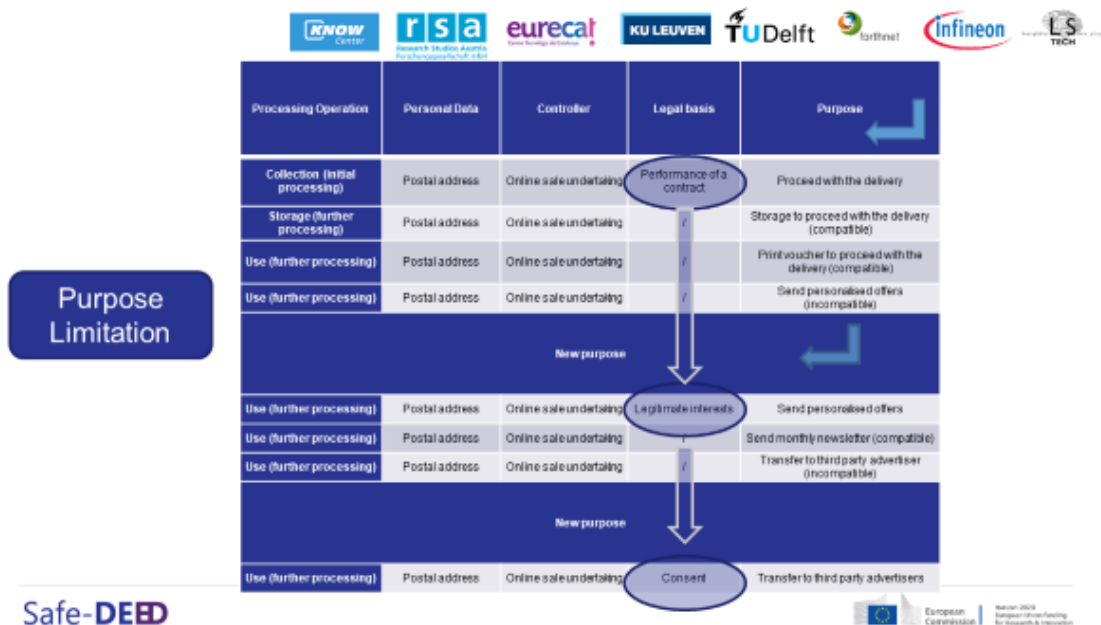
Transparency – This principle is strictly linked to fairness. To fulfil the transparency requirement, each activity characterizing the processing must be executed transparently.⁵⁴



Safe-DEED



Purpose Limitation - Personal data have to be collected for specified, explicit, and legitimate purposes: there must be a correspondence between data collection and the purpose activity when they are processed. Moreover, the purposes of collecting data and the purpose of processing the data must be compatible.⁵⁵



⁵⁴ *Ibid.* Art 5(1)(a).

⁵⁵ *Ibid.* Art 5(1)(b).

Data Minimization – The processing of personal data should be adequate, relevant, and limited to what is necessary about the purposes for which they are processed. To comply with this requirement, a necessity and proportionality test is indispensable.⁵⁶



Accuracy – Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Therefore, when collecting and processing data subjects' data, controllers need to verify the correctness of the data.⁵⁷



Storage Limitation - The controller has to identify the purpose of the processing and, consequently, the data retention period. Once the purpose has been fulfilled, data have to be securely anonymized or deleted. Nonetheless, the same data can be used for a different purpose, and in that case, instead of

⁵⁶ *Ibid.* Art 5(1)(c).

⁵⁷ *Ibid.* Art 5(1)(d).

being removed or anonymized, they can be retained for the time strictly necessary for achieving the new purpose.⁵⁸

Integrity and Confidentiality – Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures.⁵⁹



Accountability – Controllers shall be responsible for and demonstrate compliance with all the principles mentioned above. In addition, Art 25 GDPR requires that the controller, taking into account all the processing elements, puts in place adequate technical and organizational measures, which have to be demonstrated, to prove that the processing has been carried out in compliance with the GDPR requirements.⁶⁰

⁵⁸ *Ibid.* Art 5(1)(e).

⁵⁹ *Ibid.* Art 5(1)(f).

⁶⁰ *Ibid.* Art 5(2).



Accountability

Data Controller has to put in place adequate technical and organisational measures, which have also to be demonstrated, to prove that the processing has been carried out in compliance with the GDPR requirements

Safe-DEED



3.2.3.4. Obligations

These fundamental principles are the overarching cornerstones of the GDPR. The accountability principle makes clear that all principles stated should be respected and can be legally enforced in case of possible violations by data controllers. To facilitate and ensure the respect for the GDPR principles by controllers, the GDPR enlists a series of concrete obligations vis-à-vis data controllers.

Controllers' Obligations



Respect for General Principles



Specific Transparency Requirements



Assurance of Security

Safe-DEED

First of all, the data controller has to execute its tasks in compliance with the principles described in the previous section. It means that every processing activity has to be based on one of the lawful grounds listed in Art 6 GDPR. It has to be carried out following a specified, explicit, and legitimate purpose. As for the accountability principle, the controller must adopt and demonstrate that appropriate technical and organizational measures have been taken and implemented during the whole process. When carrying out its activities, it is crucial for the controller to choose processors “*providing sufficient guarantees to implement appropriate technical and organizational measures so that*

*processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject”.*⁶¹

Also, allocation of responsibilities and clear definitions of the tasks assigned to the processor should be defined in a written contract, as stated in Art 28(9) GDPR (this can also be done electronically).⁶² To comply with the transparency requirement, the controller has to keep a record of the processing activities that are carried out. Following Art 32 GDPR, controllers also have to ensure a level of security that is adequate to the risk for the rights and freedoms of data subjects that can occur during processing activities.⁶³

3.2.3.5. Rights

Data subjects have specific rights regarding activities that involve the processing of their personal data. The modalities for the exercise of these rights are listed in Art 12 GDPR.⁶⁴ These are:

1. The right to access
2. The right to ratification
3. The right to erasure of data
4. The right to the restriction of the processing
5. The right to data portability
6. The right to object

Data Subjects' Rights



The right to access



The right to the restriction of the processing



The right to ratification



The right to data portability



The right to erasure of data



The right to object

The right to access - Without access to personal data, many rights granted to data subjects could not be claimed. The right to access can also be introductory to verify data controller compliance with

⁶¹ *Ibid.* Art 28.

⁶² *Ibid.* Art 28(9).

⁶³ *Ibid.* Art 32.

⁶⁴ *Ibid.* Art 12.

GDPR provisions.⁶⁵ Art 15 GDPR gives data subject the right to obtain information from the controller as to whether his or her data are processed. If this is the case, the data subject has the right of access the data and the following information: *“(I) the purposes of the processing, (II) the categories of personal data concerned, (III) the recipients or categories of recipients to whom the personal data have been or will be disclosed, (IV) the retention period, (V) the existence of the right to rectification or erasure, (VI) the right to lodge a complaint with a supervisory authority, (VII) the source of the personal data and (VIII) the existence of automated decision-making.”*⁶⁶

The right to ratification - Data subjects the right to request the rectification of inaccurate personal data concerning him or her.⁶⁷ Considering the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including providing a supplementary statement. This right is complementary to the principle of accuracy of personal data.

The right to erasure of data – This right, also known as “the right to be forgotten”, gives data subjects the possibility, under certain circumstances, to *“obtain from the controller the erasure of personal data concerning him or her without undue delay”*.⁶⁸ Besides, the controller has an obligation to inform the data subject when the requirement has been fulfilled and the requested data erased.

The right to the restriction of the processing – The data subject has the right to obtain the restriction of the data processing when either: *“(I) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (II) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (III) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; or (IV) the data subject has objected to processing pursuant to his right to object, pending the verification whether the legitimate grounds of the controller override those of the data subject.”*⁶⁹

The right to data portability - This represents another novelty of the GDPR. This right gives data subjects the right to receive their data from a controller *“in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:(a) the processing is based on consent and the processing is carried out by automated means”*.⁷⁰ Also, the right to data portability gives data subjects the possibility, where technically feasible, to have personal data transmitted directly from one controller to another. With this right, the legislator intends to avoid lock-in situations by individuals. Nonetheless, the wording used in this provision has led to questions about the real effectiveness of the provision

⁶⁵ *Ibid.* Art 15.

⁶⁶ *Ibid.*

⁶⁷ *Ibid.* Art 16.

⁶⁸ *Ibid.* Art 17.

⁶⁹ *Ibid.* Art 18.

⁷⁰ *Ibid.* Art 20.

The right to object – This concerns the right to object to the processing of their personal data for reasons related to their specific situation.⁷¹ To overcome such objection, the controller has to demonstrate compelling legitimate grounds overriding the interests, rights, and freedoms of data subjects to establish, exercise, or defend legal claims.

Reinforcing data subjects' rights, the GDPR introduces a one-month time limit for the controller to address the requests made by data subjects, with a possible extension to two months if the claim's complexity requires more time. Also, controllers have to provide data subjects with the requested information about the processing free of charge, unless the requests are manifestly unfounded, in particular, because of their repetitive character. Nonetheless, the controller bears the burden of demonstrating the manifestly unfounded or excessive nature of the request. When the controller has reasonable doubts concerning the identity of the person making the request, the controller may seek additional information to confirm the identity of the data subject making the request.

3.2.3.6. Relevance

It speaks for itself that the GDPR's content is a lot more expansive. Nonetheless, this chapter has aimed to provide a concise overview of its main provisions. We have covered that the regulation applies uniformly in the entire European Union, as of 25 May 2018. Moreover, the GDPR solely applies to the "processing" of "personal data". Both terms are quite broad. Personal data includes all information related to an identifiable natural person, the data subject. In this scenario, the GDPR imposes obligations on the (joint) data controllers and (to a limited extent) on the data processors. On the flip side, it also grants rights to the data subject. These obligations and rights intend to protect natural persons' fundamental rights and freedoms and, particularly, their right to the protection of personal data, and aims to uphold the free movement of personal data within the Union. Hence, the GDPR lays out several general principles, based on which it equally stipulates specific rights and duties upon the data subjects and data controllers/processors respectively.

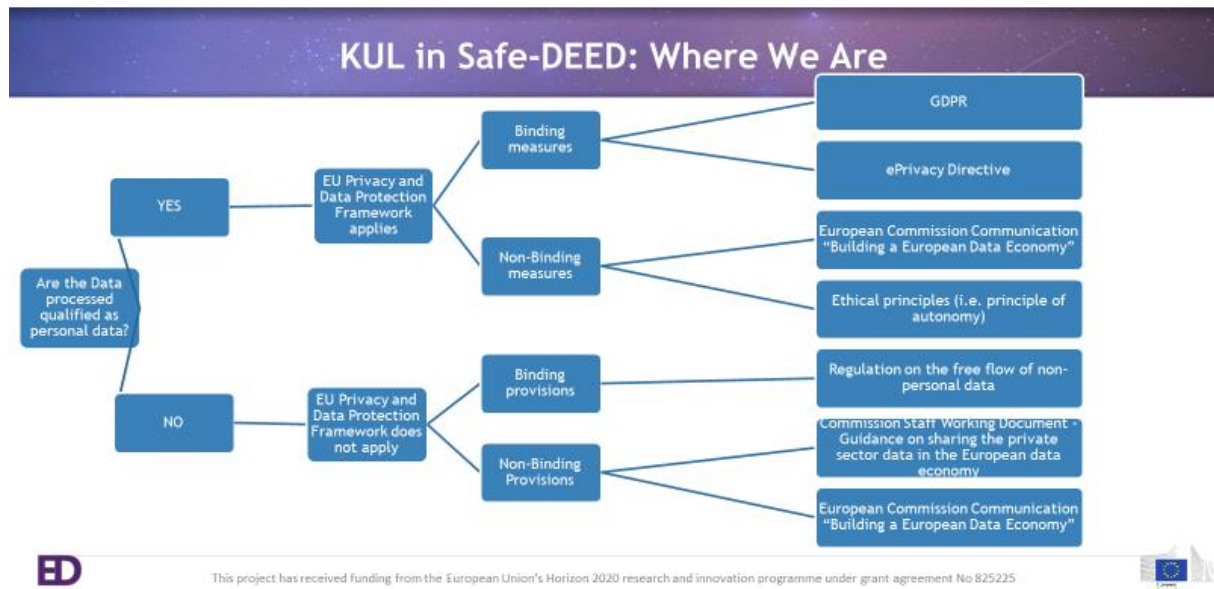
The GDPR is one of the chief instruments that should be considered whilst developing the EU data-driven economy. Given its aforementioned broad scope of application, the GDPR is relevant in numerous instances. Questions about its application may, for instance, arise in the context of data marketplaces. Can the aggregation or analysis of data be regarded as the processing of personal data? Does the encryption of data on the marketplace invalidate the "identifiability" requirement? Who can be appointed as the data controller in these instances? etc.

Numerous other legal instruments address personal data protection in specific scenarios (so-called "lex specialis"). A notable example concerns the E-privacy Directive⁷² (and its prospective successor, the proposed E-privacy Regulation), which deals with protecting privacy and the processing of personal data in the electronic communications sector. Nonetheless, this teaching module only deals with the moral rules embedded in the General Data Protection Regulation.

⁷¹ *Ibid.* Art 21.

⁷² Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

The distinction between personal and non-personal data is relevant concerning the applicable legal framework. Therefore, the subsequent chapter will deal with the legal frameworks on the protection of non-personal data.



3.3. CHAPTER 5. The protection of non-personal data

Within the Safe-DEED research, WP3 has extensively researched the protection of non-personal data. Hence, this chapter summarizes several key findings of this earlier research and transposes some writings of previous deliverables. These concern D3.1 and D3.3 and may be consulted at <https://safe-deed.eu/deliverables/>.

The foregoing chapter has put forward the main legal considerations on the protection of personal data in a data-driven economic context. Particular attention has been paid to the importance and relevance of the General Data Protection Regulation. It has *inter alia* been stated that personal data concerns “any information related to an identifiable natural person”⁷³, which in part triggers the applicability of the GDPR. On the flipside, all data that do not fall within this scope can be deemed “non-personal data”. Hence, “non-personal data” is a negatively formulated conception.

‘Non-Personal Data’?

Personal data = ‘any information relating to an identified or identifiable natural person’. Art 4(1) GDPR



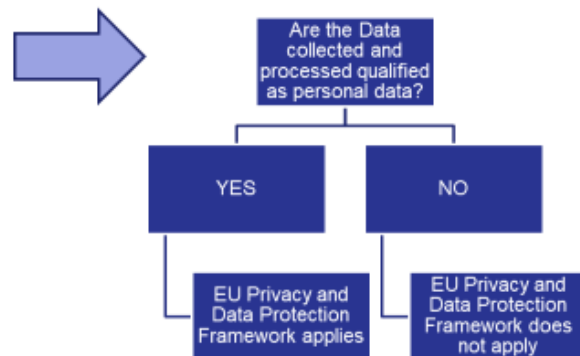
In the previous chapter, it has been discussed that the protection of personal data is predominantly aimed at protecting the fundamental rights of natural persons and the free movement of personal data through the Union. The rationales behind the protection of non-personal data are more fragmented, ranging from the safeguarding of the free flow of data, competition law concerns, and online platforms' fair usage. This chapter provides an insight into some of the most relevant legal instruments for the protection of non-personal data.⁷⁴

⁷³ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 4(1).

⁷⁴ Within the Safe-DEED research, WP3 has already extensively researched the subject matter of “the protection of non-personal data”. Therefore, this chapter merely summarizes the key findings of earlier research. D3.1, D3.2, D3.3 and D3.4 provide a more elaborate analysis of the ethical guidelines at issue. These deliverables can be consulted at: <https://safe-deed.eu/deliverables/>.



Personal vs. Non-Personal Data



Safe-DEED



Deliverable 3.3: Processing of non-personal data

Binding legislative initiative

- Regulation on the free-flow of non-personal data

Non-binding legislative initiatives

- European Commission Communication “Building a European Data Economy”
- Commission Staff Working Document – Guidance on sharing the private sector data in the European data economy

Safe-DEED



3.3.1. “Building a European Data-Economy”


On the 10th January 2017, the European Commission (EC) published a Communication and a Staff Working document on “Building a European Data Economy”.⁷⁵ The Communication focuses on the main legal challenges hampering the EU data-driven economy and aims to set the EC legislative agenda to fill the gap. Following the recommendations included in the Communication, the EC has subsequently developed legally binding measures to tackle some data economy issues, for example, national restrictions of data localization.

⁷⁵ 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-content/EN/TXT/?uri=COM:2017:9:FIN>>, accessed 5 December 2020.





“Building a European Data Economy”
EC Communication, 10/01/2017

What?
Towards a single data market in the EU 

Why?

-  citizen wellbeing
-  business opportunities
-  innovative public services

How? by overcoming:

-  Data localization restrictions
-  Obstacles by IT vendors
-  Complex legal framework
-  Lack of trust

Safe-DEED

First, the EC Communication defines data market places as the market “*where digital data is exchanged as products or services derived from raw data – on the economy as a whole. It involves the generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation of data enabled by digital technologies*”.⁷⁶ This definition has already been touched upon in chapter two of this syllabus. According to the EC Communication, if supported with adequate legislative measures, cooperation between different actors involved in the data marketplace can increase economic opportunities for the involved entities and, as a result, for EU citizens.

The Commission, recognizing the potential benefits that can come from the exploitation of data generated by machines, encourages removing any national restriction that could limit cross-border access to such data. Concerning the promoted legislative approach, the EC Communication calls for the development of new legislative initiatives to address some of the key barriers related to data economy instead of using existing national and European frameworks. The recently adopted Regulation on the Free Flow of non-personal data addresses some of the EC issues. Other potential solutions presented in the Communication, such as the one on the data producer’s right, mentioned in the EC Staff working document accompanying the Communication, have been included in the Digital Content Directive proposal.

Hence, these legal initiatives by the EC aim to (I) foster a data-driven EU economy whilst equally (II) providing adequate legal protection of data. A European data-economy can merely function with a sufficient legal framework to back it up and enable its advancement. The EC Communication on

⁷⁶ European Data Market study, SMART 2013/0063, IDC, 2016.

“Building a European Data-Economy”⁷⁷ thus clearly demonstrates the importance of this chapter within the overall theme of fostering data-enabled economic development in the EU.⁷⁸

The following subchapter shall introduce some of the initiatives taken in the aftermath of the EC’s Communication.

3.3.2. Free Flow of Non-Personal Data Regulation

In line with the Digital Single Market strategy, the EC has published a legislative proposal on the free flow of non-personal data in 2017.⁷⁹ In its General Approach on the Free Flow of Non-Personal Data Regulation (FFNPDR), the Council defined the EC proposal as a *“balanced compromise that gives Member States flexibility to address core public responsibilities while respecting the principles of the free flow of data”*.⁸⁰ The European Parliament on its side, also welcomed the initiative. The Committee for the Internal Market and Consumer Protection has defined the free flow of non-personal data as the 5th freedom of the EU Single Market after goods, people, services, and capitals. The FFNPDR was signed on the 14th November 2018 and entered into force at the end of December 2018 and applicable from 28 May 2019.⁸¹ The EC considers the free flow of non-personal data a fundamental building-block of the Digital Single Market Strategy. According to the EC, the FFNPDR, removing the national restrictions to the free flow of non-personal data, will boost the EU economy, generating up to 4% GDP by 2020.⁸²

The Commission has recognized four barriers to data mobility within the EU market:

1. Data localization restrictions by Member States’ public authorities;
2. Obstacles put in place by IT systems’ vendors;
3. Complex EU legal patchwork that leads to legal uncertainty; and
4. The lack of trust due to security risks and concerns about the cross-border availability of data for regulatory purposes.

The removal of these legal obstacles is considered preliminary not only for enhancing the economy but also for boosting innovation (with expected progress in the field of AI, IoT and autonomous

⁷⁷ 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-content/EN/TXT/?uri=COM:2017:9:FIN>>, accessed 5 December 2020.

⁷⁸ *Supra* Chapter 1. ‘Introduction to the value of data’.

⁷⁹ European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region – Commission Work Programme 2016 – No time for business as usual’, https://ec.europa.eu/info/sites/info/files/cwp_2016_en_0.pdf accessed 5 December 2020.

⁸⁰ For the version proposal as revised by the Council, see: <http://data.consilium.europa.eu/doc/document/ST15724-2017-REV-1/en/pdf> accessed 24 April 2019.

⁸¹ Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union O J L 303, 28.11.2018, p. 59–68.

⁸² Deloitte, “Measuring the Economic Impact of Cloud Computing in Europe”, final report prepared for the European Commission <https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloudcomputing-europe>, accessed 6 December 2020.

systems). Hence, a data-driven economy's advancement fundamentally hinges upon the free flow of data across the European Union.

Free Flow of Non-Personal Data Regulation


(FFNPDR) 28 May 2019

Core idea:

Free movement of non-personal data across borders

=

Every organisation should be able to store and process data
anywhere in the European Union



Safe-DEED

3.3.2.1. Scope

According to Art 2 FFNPDR, the provisions foreseen in this text apply to “*the processing of electronic data other than personal data in the Union, which is: (a) provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the Union; or (b) carried out by a natural or legal person residing or having an establishment in the Union for its own needs.*”.⁸³ Art 2(2) and Recital 10 FFNPDR clarify that when a set of data includes personal and non-personal data, the FFNPDR will only apply to non-personal data. If this differentiation is impossible, the FFNPDR should not prejudice the application of GDPR nor impose an obligation to store the different data diversely.⁸⁴

Art 3 explicitly states that, in the context of the regulation, data have to be considered as data other than personal data as referred to in the GDPR.⁸⁵ Hence, both the GDPR and the FFNPDR use the same notion of “personal data”.⁸⁶ Furthermore, the notion of “processing” of data is equally the same as in the GDPR.⁸⁷ Recital 10 makes the correspondence even more explicit by stressing that member states

⁸³ Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union O J L 303, 28.11.2018, p. 59–68, Art 2.

⁸⁴ *Ibid.* Art 2; Recital 10.

⁸⁵ *Ibid.* Art 3.

⁸⁶ *Ibid.*; Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 4(1).

⁸⁷ *Ibid.*; Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 4(2).

are prevented from putting in place measures that limit or prohibit the free movement of non-personal data within the Union.⁸⁸

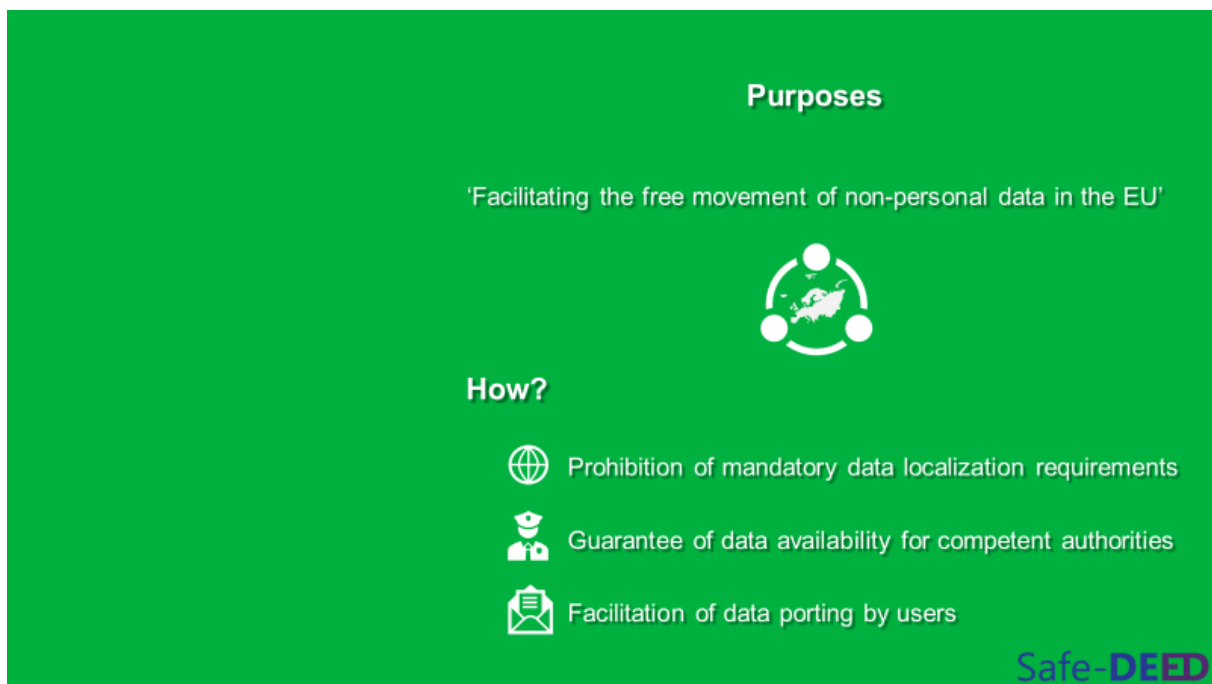
The geographical scope of application of the FFNPDR covers activities carried out by a natural or legal person residing or having an establishment in the EU, regardless of where the natural or legal person is established.⁸⁹ Therefore, activities taking place outside the EU fall out of the scope of the regulation.

3.3.2.2.Aims

To boost the Digital Single Market, the FFNPDR aims to remove all the barriers that hamper the free movement of non-personal data. Doing so, the FFNPDR identifies three main actions to achieve its purpose:

1. the prohibition of mandatory data localization requirements;
2. the guarantee of data availability for competent authorities; and
3. the facilitation of data porting by users.

These purposes mirror some of the European Commission's key barriers in its Communication on “*Building a European Data-Economy*”.⁹⁰

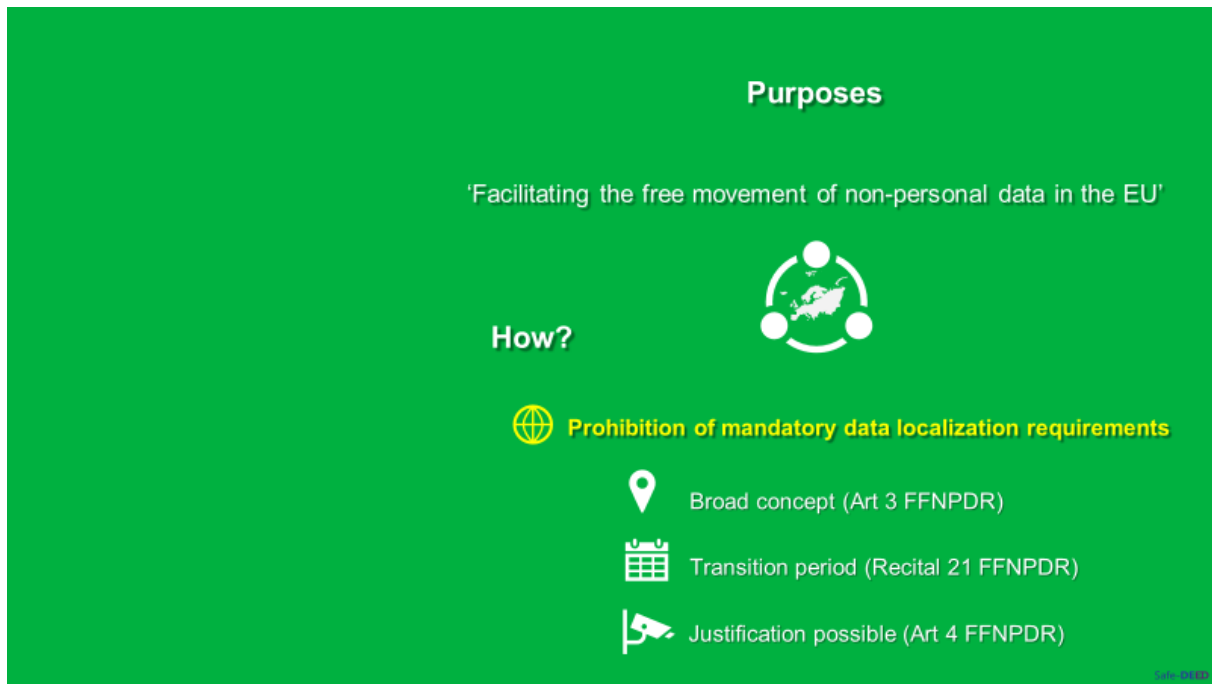


⁸⁸ *Ibid.* Recital 10.

⁸⁹ *Ibid.* Recital 2(3).

⁹⁰ European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region – Commission Work Programme 2016 – No time for business as usual', https://ec.europa.eu/info/sites/info/files/cwp_2016_en_0.pdf accessed 5 December 2020.

3.3.2.2.1. The Prohibition of Mandatory Data Localization Requirements



Art 3(1)5 FFNPDR defines data localization requirements as “any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public”.⁹¹ Recital 18 explains that these requirements “represent a clear barrier to the free provision of data processing services across the Union and the internal market”.⁹² As such, they should be banned unless they are justified on the grounds of public security, as defined by Union law, in particular within the meaning of Art 52 TFEU⁹³, and satisfy the principle of proportionality enshrined in Art 5 TEU.⁹⁴ In this context, these legal and administrative requirements are mainly related to accounting documents, invoices, commercial letters, criminal records, national registries, and archives.

Consequently, Member States have 24 months after the Regulation becomes applicable (approx. May 2021) to repeal the national provisions that are not in compliance with the FFNPDR. Member States can put in place data localization but have to inform the Commission immediately if they do so. Also, Member States are required to communicate all necessary information related to data localization requirements that are in place.

In the “data-driven economy” context, removing the national provisions on data localization might be advantageous. Since there will be no legal boundaries for nonpersonal data gathered from different

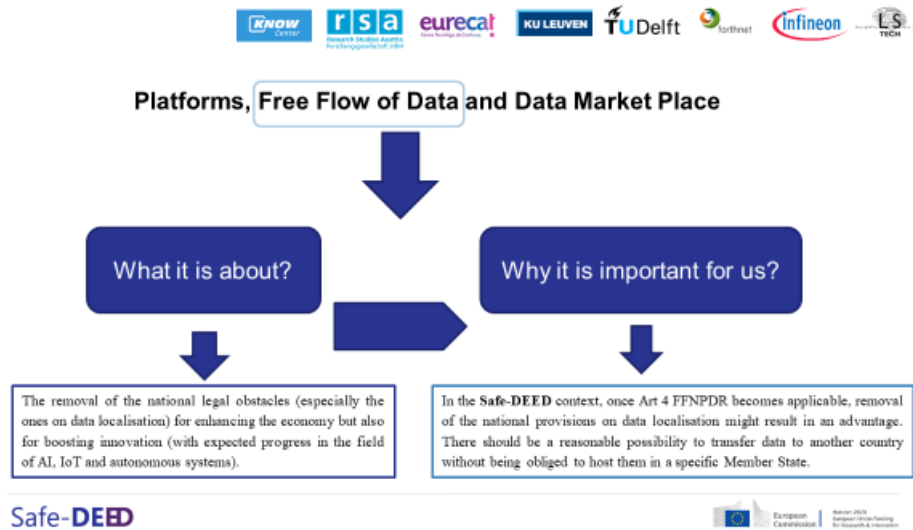
⁹¹ Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union O J L 303, 28.11.2018, p. 59–68, Art 3(1)(5).

⁹² *Ibid.*, Recital 18.

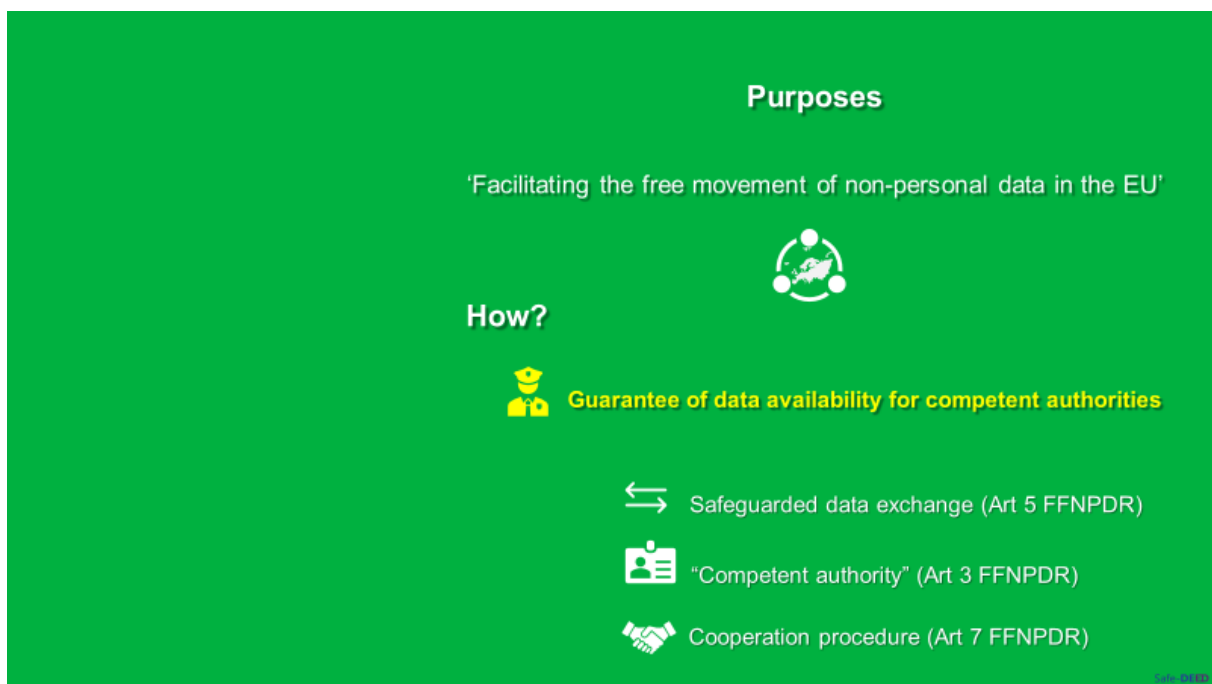
⁹³ European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, 13 December 2007, 2008/C 115/01, Art 52.

⁹⁴ European Union, *Consolidated version of the Treaty on European Union*, 13 December 2007, 2008/C 115/01, Art 5.

Member States, the situation will create a reasonable possibility to transfer data to another country without being obliged to host them in a specific Member State.



3.3.2.2. The Guarantee of Data Availability for Competent Authorities



With the provisions that will remove national legal and administrative requirements for the free flow of non-personal data, the FFNPDR foresees measures that will facilitate the cross-border access to non-personal data by public authorities. Art 5 states that the measures to enhance the exchange of the data across Member States “*shall not affect the powers of competent authorities to request and receive access to data for the performance of their official duties by Union or national law*”.⁹⁵ Consequently, “*Access to data by competent authorities may not be refused on the basis that the data are processed*

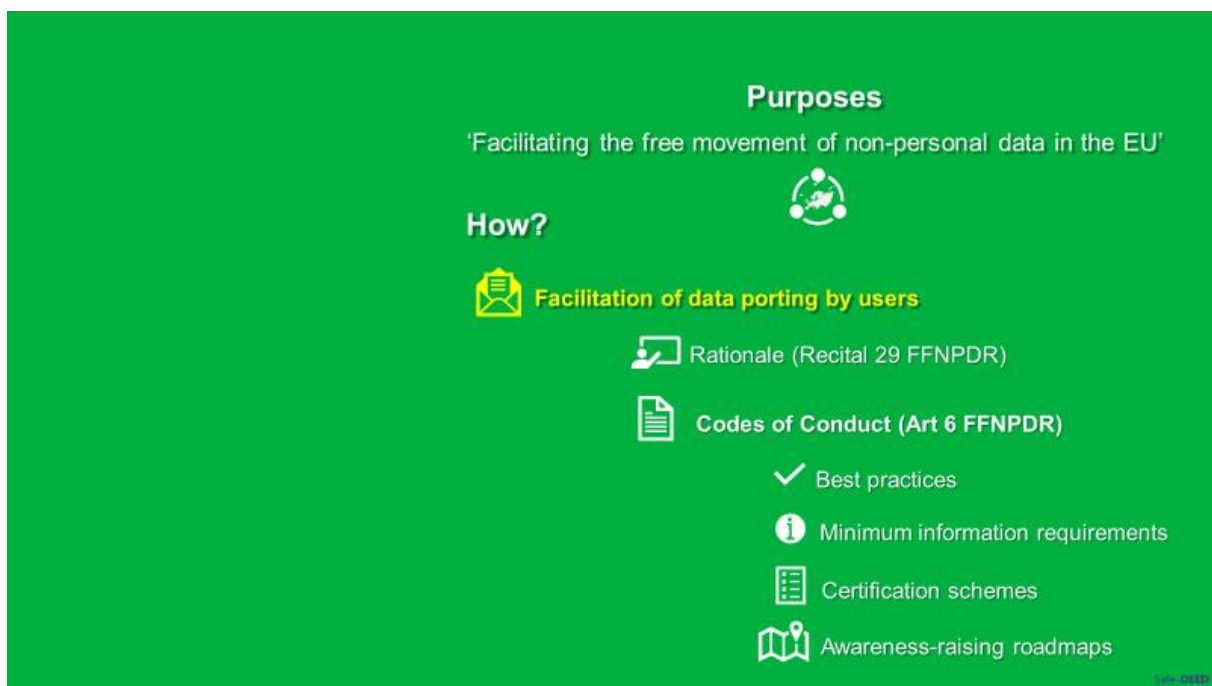
⁹⁵ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 5.

in another Member State”.⁹⁶ If a service provider does not comply with such requests, it will incur sanctions.

According to Art 3(1)(6) FFNPDR, a “competent authority”, is “an authority of a Member State or any other entity authorized by national law to perform a public function or exercise public authority that has the power to obtain access to data stored or processed by a natural or legal person for the performance of its official duties, as provided for by national or Union law”.⁹⁷ Additionally, to enhance the cooperation and efficiency of their activities, the Regulation foresees cooperation mechanisms, especially regarding the exchange of information and assistance when accessing cross border data.

In the overall context of this syllabus, this provision can be relevant in several occurrences. For instance, end-users and/or users exploiting data from the Safe-DEED platform may be asked by the competent national authority to access their non-personal data. Considering what is stated in the Regulation, they will have to comply with such a request, and they will not be able to refuse such demand because the requested data are stored in another country.

3.3.2.2.3. Porting of Data



Recital 29 FFNPDR stresses the importance of removing commercial practices that do not facilitate data porting, linking this need to the one that has to lead to the right to data portability in the GDPR.⁹⁸ Therefore, Art 6 FFNPDR encourages and facilitates the development of self-regulatory codes of

⁹⁶ *Ibid.* Art 5(1).

⁹⁷ *Ibid.* Art 3(1)(6).

⁹⁸ *Ibid.* Recital 29.

conduct at Union level (“Codes of Conduct”), to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards”.⁹⁹

To do so, relevant stakeholders should develop their code of conduct covering four key aspects:

1. Best practices in facilitating the switching of providers and the porting of data in a structured, common, and machine-readable format allowing sufficient time for professional users actually to switch or port the data;
2. Information, which should be detailed, precise, and shown in a transparent manner between parties before the contract is concluded;
3. Approaches to certification schemes that can facilitate the comparison between different products and services; and
4. Communications regarding roadmaps to raise awareness of the codes of conduct among relevant stakeholders.

Compliance with these requirements should enhance trust in all stakeholders and transparency in the whole process. In the overall context of advancing a data-driven EU market, the idea of developing a code of conduct that would facilitate compliance with the requirements in Art 6 should be strongly considered. The development of a code of conduct is equally of the essence concerning fostering organizational trust in data marketplaces, as shall be discussed in chapter seven.

3.3.3. Platform-to-Business Regulation

On 26th April 2018, the EC published its Proposal for a Regulation on promoting fairness and transparency for business users of online intermediation services (Platform-to-Business Regulation - P2BR).¹⁰⁰ The Regulation entered into force on the 11th of July 2019.

With this initiative, the EC has intended to legislate in the area of business platforms, which had, at that point, not been addressed by specific legislative initiatives. The P2BR is part of the legislative measures promoted by the EC for the Digital Single Market strategy. The proposal is the first legislative initiative in the field of platforms. It focuses only on a specific type of platform, namely, those offering services or products to the same users of their business clients. The P2BR foresees for them a list of measures ensuring transparency and fairness. Doing so, the EC aims to temper the natural asymmetries that characterize the relationship between platforms and their suppliers, establishing a fair and trustworthy innovation-driven ecosystem.

3.3.3.1.Scope

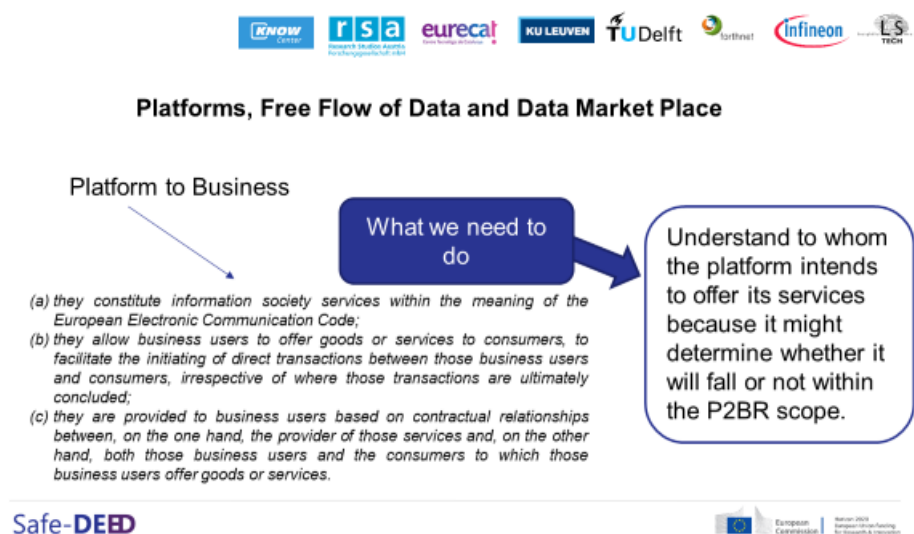
The P2BR regulates the area of Business-to-Business relations. Art 2 P2BR describes the requirements of the intermediation services (platforms) that fall into the scope of application of this Regulation: “(a)

⁹⁹ *Ibid.* Art 6.

¹⁰⁰ Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services O J L 186, 11.07.2019, p. 57–79.

they constitute information society services within the meaning of the European Electronic Communication Code; (b) they allow business users to offer goods or services to consumers, to facilitate the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users based on contractual relationships between, on the one hand, the provider of those services and, on the other hand, both those business users and the consumers to which those business users offer goods or services.”¹⁰¹

An online intermediation service falls into the scope of application of P2BR only if all these characteristics are present. The provided definition of intermediaries describes only the services directly with business users and their clients. The P2BR does not foresee a clear threshold, applying indistinctively to all types of platforms that fall in the criteria listed in Art 2 P2BR.



3.3.3.2. Purposes

The P2BR promotes two main principles: transparency and fairness. First of all, the P2BR foresees transparency obligations for intermediation services providers to inform, through clear, unambiguous, and readily available contractual terms and conditions, about the treatment, the criteria used to rank their products, and the requirements to suspend or terminate their services.

Moreover, the P2BR aims to achieve fairness by implementing effective out-of-court redress mechanisms such as internal handling systems for business users and mediation procedures. The intermediaries' contractual terms and conditions have to include a list of independent mediators that can be approached to settle disputes to facilitate the process.

In the data marketplace context, it is thus crucial to understand to whom the platform intends to offer its services because it might determine whether it will fall or not within the P2BR scope.

¹⁰¹

Ibid. Art 2.

3.3.4. Legal Considerations: Concluding Note

The two foregoing chapters have provided a brief insight into some of the core legal considerations which ought to be taken into account whilst assessing the development of a data-driven EU economy.

Though seemingly self-evident, it should be noted that the legal instruments covered merely concern a selection amongst a vast plethora of regulations and directives in EU law. Nevertheless, students are now acquainted with some of the main instruments in this regard, ranging from the GDPR to the FPNPDR and the P2BR.

Secondly, it should be underlined that in this syllabus, a distinct divergence has been made between personal and non-personal data. Though relevant with regard to the scope of application of many legal instruments, the differentiation is not always unequivocally relevant in all legal contexts.

Lastly, it seems to be clear that a comprehensive legal framework is indispensable in light of the further development of a data-driven EU economy. This relevance is twofold. In the first place, creating a safer digital space in which all users of digital services' fundamental rights are protected. However, a sound legal framework equally adds to establishing a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally. Thus, the advancement of an adequate legal framework functions as the motor and the anchor of the data-driven EU economy.

4. PART III. THE ADVANCEMENT TOWARD A EUROPEAN DATA-DRIVEN ECONOMY: CHALLENGES & OPPORTUNITIES

4.3. CHAPTER 6. The valuation of data

Within the Safe-DEED research, WP3 and WP4 have extensively researched the subject matter of data valuation. Hence, this chapter summarizes several key findings of this earlier research and transposes some writings of previous deliverables. These concern D3.4, D4.1, D4.2, D4.3, and D4.4, and may be consulted at <https://safe-deed.eu/deliverables/>.

There exists an interesting comparison that is usually made when illustrating the economic value of data¹⁰², as well as the difficulty in estimating it, especially when perceiving data as an economic asset, much like petrol: *“Facebook is now worth about \$200 billion. United Airlines, a company that actually owns things like airplanes and has licenses to lucrative things like airport facilities and transoceanic routes between the U.S. and Asia, among other places, is worth \$34 billion”*¹⁰³

According to estimates of their revenues, the US Department of Commerce found that between 2004-2014, data-driven businesses created a \$17 trillion economy, while the costs on data collection, processing and dissemination amounting to only \$3.7 billion annually a mere 0.02% of the value created.¹⁰⁴

A McKinsey study from 2013 estimated that public open data could help unlock between \$3.2 - \$5.4 trillion in economic value across seven economic areas (education, transportation, consumer products, electricity, energy, healthcare, consumer finance), together with five actions to achieve that: promoting transparency, exposing variability and encouraging experimentation, segmenting populations, automation, defining new products and services.¹⁰⁵

Concerning the use of personal data, a 2012 report by the Boston Consulting Group was estimating that its quantifiable benefits could reach €1 trillion per year by 2020 (approximately 8% of the EU's

¹⁰² Within the Safe-DEED research, WP3 and WP4 have already extensively researched the subject matter of “the valuation of data”. Therefore, this chapter merely summarizes the key findings of earlier research. D3.4, D4.1, D4.2, D4.3 and D4.4 provide a more elaborate analysis of the ethical guidelines at issue. These deliverables can be consulted at: <https://safe-deed.eu/deliverables/>.

¹⁰³ The market valuation in the quote refers to the year 2015. Baldwin, H. (2015). Drilling Into The Value Of Data. Forbes. URL: <https://www.forbes.com/sites/howardbaldwin/2015/03/23/drilling-into-the-value-of-data/>.

¹⁰⁴ Ballivian, A. and Fenohasina, R.M. (2015) Measuring the Value of Data. URL: https://statswiki.unece.org/download/attachments/117772954/World%20Bank_Ballivian_Mare_MeasuringtheValueofData_20151202.pdf?version=1&modificationDate=1473158675433&api=v2.

¹⁰⁵ Manyika, J. et al. (2013) Open Data: Unlocking innovation and performance with liquid information. McKinsey Global Institute, McKinsey Center for Government, McKinsey Business Technology Office.

GDP), a number that could well be an underestimation as its calculation was made based on the primary use cases from data at the time.¹⁰⁶ Similarly, the global economy based on personal data was estimated to be around \$3 trillion in 2017.¹⁰⁷

4.3.1. The Classification of “Data”: an economic approach

4.3.1.1. Data as a Commodity



Lecture 6: The valuation of data

The issue of data valuation
<ul style="list-style-type: none"> • The difficulties of data valuation • The data valuation process: overview
Economic value of data
<ul style="list-style-type: none"> • Data as a tangible asset: Methods of measuring data value • Data as a commodity • The ecosystem of personal data exchanges • Putting a price on personal data
Contexts for data valuation
Data quality assessment
<ul style="list-style-type: none"> • Methodologies • Data quality dimensions and metrics
Aggregating and reporting
Data valuation protocol: conclusion & future work

The valuation of data: an economic perspective

Classification of data → helps putting an economic value on it

1. Data as a commodity
2. Data Ownership
 1. Property
 2. Intellectual Property: Copyright
 3. Other related Intellectual Property Rights
 4. GDPR

It is likely that the major changes in the global economy, with data companies challenging energy companies, inspired comparisons between oil and data, including the over-used “data

¹⁰⁶ Scanapiecco, M., Virgillito, A., Marchetti, M., Mecella, M., and Baldoni, R. (2004). The DaQuinCIS architecture: a platform for exchanging and improving data quality in Cooperative Information Systems. In: Information Systems. 29, 7, 551–582.

¹⁰⁷ Vasudha, T., and Arvind, G. (2017). The value of data. World Economic Forum.
<https://www.weforum.org/agenda/2017/09/the-value-of-data/>.

is the new oil”. While this is useful to get across the point that data is a valuable resource in today’s world, the comparison can easily break along multiple perspectives:

- I. data is becoming increasingly more available with time, as opposed to fossil fuel, which is becoming scarcer;
- II. raw data comes in many different flavours (text, image, video, sound), across various formats that require a variety of extraction methods; raw oil is all the same and extracting it is done in the same way.

4.3.2. Data Ownership

The challenge of data valuation has a particular resonance in the data ownership debate. A certain degree of transparency concerning the value of data is needed to justify its ownership's desirability.¹⁰⁸ In recent years, data ownership has become a buzz word; however, there is a lack of consensus among scholars and no clear cut answer in the EU regulation landscape about this concept.¹⁰⁹

Today, in practice, we see a *de facto* data ownership functioning through the physical control over data and the conclusion of contracts.¹¹⁰ Such a situation has raised the question about the necessity to establish a data ownership right. While the scarcity of the resources has historically legitimized ownership, we see an increasing plethora of data nowadays. Therefore, some have strongly advocated *against* the introduction of such a right.¹¹¹ According to this view, it is reported that introducing data ownership was not necessary nor justified and risked creating chilling effects and legal uncertainties.¹¹² But could this *de facto* ownership be replaced by some form of legal ownership? Several elements explain why there is such a debate as to whether a legal regime for data ownership should be created. The uncertainty and lack of a clear position in data ownership discussion might influence data exchanges and the data valuation assessment.

Answering the ownership question is a sensitive political question. Who should be the owner, under which theory, how should the framework be set up? There are many competing interests in data; therefore, each answer will balance the ownership framework in one or another camp. Granting ownership entitles the individual or entity to provide access, restrict partially or

¹⁰⁸ Janeček V., ‘Ownership of Personal Data in the Internet of Things’ (2018) 34 Computer Law and Security Review 1039., p.13.

¹⁰⁹ Koutroumpis, P., & Leiponen, A. (2013). “Understanding the value of (big) data.” In 2013 IEEE International Conference on Big Data, Big Data 2013 (pp. 38–42). Silicon Valley, CA. <https://doi.org/10.1109/BigData.2013.6691691>; Koutroumpis, P., & Leiponen, A. (2013). “Understanding the value of (big) data.” In 2013 IEEE International Conference on Big Data, Big Data 2013 (pp. 38–42). Silicon Valley, CA. <https://doi.org/10.1109/BigData.2013.6691691>.

¹¹⁰ Swinnen K., ‘Ownership of Data : Four Recommendations for Future Research’ (2020) 5 Journal of Law, Property and Society 139.

¹¹¹ Drexel J., and others, ‘Data Ownership and Access to Data - Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate’ [2017] SSRN Electronic Journal.

¹¹² *Ibid.*

entirely, impose conditions or fees for access and use.¹¹³ From an industry perspective, ownership in data would protect the investments carried out to collect and select data. From an individuals' perspective, ownership will improve the control over their data from unauthorized collection and use¹¹⁴ and stimulate competition.¹¹⁵

The dilemma between private and public interests is also tangible. Additionally, data ownership raises ethical considerations in light of the personal data commodification debate. Data ownership is strictly linked to competition law as ownership can create monopolies and affect the public interest and individuals' fundamental rights.¹¹⁶ Parallely, some alternative vision for data markets starts developing, such as the commons theory.¹¹⁷ Opposite to the neo-liberal capitalism approach, the commons theory is a resource management model promoting the freedom to operate rather than the power to appropriate.¹¹⁸ Secondly, scholarly research on data ownership indicates no common understanding of the notion of ownership and no definition at the EU-law level either. Scholars give a wide variety of meaning to ownership and refer alternatively to different law areas that do not simplify the already complex ownership debate.¹¹⁹

Thus, ownership could be envisaged under different areas of law such as property, intellectual property, and data protection.

4.3.2.1.Data as Property

Concerning property law, the concept of ownership varies significantly from one legal jurisdiction to another. Indeed, while from a civil law tradition, ownership is envisaged as a *numerus clausus* (a limited number) of rights and legal objects, the common law tradition has a more flexible approach regarding the type of entitlements granted.¹²⁰ Furthermore, whereas civil law has an *erga omnes* approach to ownership (entitling ownership against everyone), common law has both approaches in *personam* (a specific right exigible against a specific person) and in *rem* (right attached to the object of ownership). Besides the need for a legal object, the principles of transparency, specificity, and publicity (about the object description and publicity) have to be fulfilled to grant ownership.¹²¹ These are complex elements to adapt and match with the different national data frameworks. Hence, the classification of data seems to fit into the rigid conception of “property hardly”, and would – given the

¹¹³ Scassa T., ‘Data Ownership’ [2020] Centre for International Governance Innovation, p. 2.

¹¹⁴ *Ibid.* p. 12.

¹¹⁵ (Malgieri, 2016), p.10.

¹¹⁶ Scassa T., ‘Data Ownership’ [2020] Centre for International Governance Innovation 1.

¹¹⁷ Fia T., ‘An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons’ [2020] Global Jurist (forthcoming)., published online 22 September 2020.

¹¹⁸ Benkler Y., ‘Between Spanish Huertas and the Open Road’., Governing Knowledge Commons (Oxford University Press 2014).

¹¹⁹ Swinnen K., ‘Ownership of Data: Four Recommendations for Future Research’ (2020) 5 Journal of Law, Property and Society 139, p. 146.

¹²⁰ Janeček V., ‘Ownership of Personal Data in the Internet of Things’ (2018) 34 Computer Law and Security Review 1039., p. 13.

¹²¹ Van Erp S., ‘Ownership of Digital Assets and the Numerus Clausus of Legal Objects’ [2017] SSRN Electronic Journal 1.

different legal traditions in civil and common law – arguably lead to many instances of legal uncertainty and non-uniformity across the Union.

4.3.2.2. Intellectual Property Law: Copyright

The intellectual property (IP) framework is an ancient legal regime which seems unfit to apprehend all the modern technicalities of data ownership. To be protected, data must constitute an original creation from the human intellect that has been expressed in a tangible form. Depending on the form and the characteristics of the creation, it will be protected under different regimes: copyright (literary and artistic works), trademarks (distinctive sign), patent (inventions), design, etc.

Copyright protects the original expression of an idea. The definition of data is still debated, and the legislative initiatives developed at the EU level have not provided enough clarifications. Therefore, it is still uncertain whether data can be protected under EU Copyright law. Machine-generated data seem to fall outside the scope of IP protection due to the lack of human involvement. A potential solution to such interpretation might occur by diminishing the threshold and protecting “*the mere fact that someone has somehow contributed to digital data creation, but this would have nothing to do with the original purpose of IP law*”.¹²² Such an approach is in contradiction with years of case-law and legislative developments. Consequently, among scholars, the choice to develop data ownership under the copyright law regime is still debated as fit for purpose.

4.3.2.2.1. Legal Regimes related to Intellectual Property

One may rely upon the Trade Secret Directive¹²³ as a legal classification of “data”. The Trade Secret Directive aims to harmonise the existing diverging national laws within the EU on the protection against the misappropriation of trade secrets so that companies can exploit and share their trade secrets with privileged business partners across the internal market their innovative ideas into growth and jobs. However, this Directive does not create an *erga omnes* right (i.e. a property rights that can be exercised vis-à-vis everyone else). Still, it provides some useful protective elements for the data-driven economy. According to the trade secret definition, scholars argue that while individual data can hardly qualify as a trade secret, data sets are more convincing even though several criteria still have to be met.¹²⁴

An alternative may be the Database Directive¹²⁵, which was created in 1996 and aimed to provide specific protection for the investment made in creating a database. Therefore it does not protect the creation of the data itself but solely the collection of data. Nevertheless, after some years into force,

¹²² (Swinnen, 2020), p.151-152.

¹²³ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance), OJ L 157, 15.6.2016, p. 1–18.

¹²⁴ Drexler J., and others, ‘Data Ownership and Access to Data - Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate’ [2017] SSRN Electronic Journal.

¹²⁵ Directive (EU) 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases OJ L 20, 27.3.1996, p. 20–28.

some argue that this specific IP right is already outdated. On such discussion, the Max Planck Institute argued that this framework is unsuitable for protecting individual data and should not be revised to integrate data ownership.

4.3.2.2.2. GDPR

Natural individuals own their personal data thanks to the European data protection framework, and in particular, the GDPR. Indeed, the GDPR was designed to give individuals a degree of control over their personal data. However, the type of control provided “*falls short of ownership*” even for the data portability right, right to access and to correct their personal data.¹²⁶ They constitute at their best a “*quasi ownership regime*”.¹²⁷

4.3.2.2.3. The economic approach: key insights

The foregoing economic approach to classify data ownership has proven to be challenging. In general, this difficulty seems to be rooted in six grounds:

1. the ownership question is a sensitive political question, as has been discussed before;
2. there is no common understanding of the concept “ownership”, as has equally been touched upon, illustrated best by the foregoing classification attempts;
3. providing an exact definition of data is complex: there will always be grey zones covering different sorts of data, governed by possibly different ownership regimes;
4. the data-economy develops rapidly. Though case law helps interpret the ownership regime, most cases before courts are business cases. Hence, we may therefore only expand a certain angle of the data ownership question, whilst public interest in access and use of data risks to be overlooked;
5. there are fundamental human rights concerns. Namely, if data’s definition would comprehend information and ideas, data ownership could constitute a restriction of freedom of expression, as information would not be able to be freely shared; and
6. Access and use of data are increasingly perceived as a crucial enabler for transparency, innovation, knowledge, accountability, expression, and privacy compliance. Therefore, developing and establishing a legal regime for data ownership is sensitive and may not be the policymakers’ path chosen for the years to come.

¹²⁶ Scassa T., ‘Data Ownership’ [2020] Centre for International Governance Innovation 1.

¹²⁷ *Ibid.*

Conclusion: data ownership? 😞

6 difficulties in classifying data as 'something that can be owned':

1. Political sensitivity
2. No common understanding of 'ownership'
3. No precise definition of 'data'
4. Rapid development data-economy
5. Fundamental rights concerns
6. Possible burden on transparency & innovation

Safe-DEED

In conclusion, the current de facto data ownership regime granted through contractual arrangement and physical control still have beautiful years to come before policymakers decide to take up this challenging ownership concept. In Europe, the debate starts to run out of steam, and the European Commission presenting its future initiatives now speaks about data governance.¹²⁸ In light of the COVID-19 pandemic, the need to share data for public interest has also changed the mindset regarding the necessity for a data ownership regime, demonstrating the intrinsic link between data value assessment and the context of their use.¹²⁹

4.3.3. Moving forward from the economic approach

It may be worth looking beyond the mere economic classification spectrum we are generally used to for the reasons mentioned.

Due to the existing asymmetries between entities processing personal data and customers providing such data, policymakers worldwide have started developing legislative initiatives to empower citizens and give them access to the wealth created by Big Data.¹³⁰

¹²⁸ European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM/2020/66 final, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data19feb2020_en.pdf ; European Commission, Data Governance and data policies at the European Commission, July 2020 https://ec.europa.eu/info/sites/info/files/summary-data-governance-data-policies_en.pdf.

¹²⁹ OECD, Data Driven Innovation: Big Data for Growth and Well-Being (OECD 2015) 197.

¹³⁰ Custers B. and Uršič H., 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection' (2016) 6 International Data Privacy Law 4.

Concrete examples of such an approach are provided in the GDPR. For example, the aforementioned data portability principle, embedded in Recital 68 and Art 20 GDPR, allows data subjects to take advantages by commercial offers and services of companies other than those that have processed their data.¹³¹ The data portability principle is a clear example of a legislative measure supporting the potential social benefits that might arise from the use and re-use of personal data. On the one hand, the possibility to change the data controller enables customers to choose a service which they evaluate as more favourable. On the other hand, data portability enhances competition and business opportunities between sellers and service providers.¹³²

Notwithstanding the possibilities and positive outcomes generated by the introduction of legislative initiatives like the GDPR, the new business model created by the advent of Big Data, on which data markets rely, requires to move forward some of the legislative measures foreseen so far. An approach that considers possible consequences beyond the ones related to security and data quality might help overcome the potential negative impact on various fundamental rights issues that might also involve businesses (right to run a business).

4.3.4. Remaining Open Questions

Legal perspectives related to data ownership are prevalent due to the heterogeneous definitions of personal data in jurisdictions worldwide. Considering personal data as part of our identities – “*digital selves*”¹³³ – raises great ethical questions about the dangers of buying and selling identities. From a technical perspective, these could be solved by applying solutions inspired by digital rights management (DRM), promoting privacy-enhancing technologies (PETs), or leveraging the features of new devices to promote the creation and management of personal data portfolios. Nevertheless, there still are societal challenges connected to privacy. Do the same privacy perspectives apply across cultures? Some believe that the data practices currently promoted by Western societies (aggregation, identification, secondary use) fully “*undermine and breach the notion of privacy*”.¹³⁴ Other researchers wonder whether members of the society will be willing to participate in data markets or, on the contrary, they will be willing to give up on some of the current data usage in exchange for increase privacy. And even when / if data ownership will be resolved, the question then further extends to the

¹³¹ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 20.

¹³² Custers B. and Uršič H., ‘Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection’ (2016) 6 International Data Privacy Law 4.

¹³³ Spiekermann, S., Acquisti, A., Böhme, R., and Hui, K.-L. (2015): The challenges of personal data markets and privacy. *Electron Markets* 25, 2 (June 2015), 161–167.

¹³⁴ Solove, D.J. (2005): A taxonomy of privacy. In: *University of Pennsylvania Law Review*; 154(3), 477-560.

“*trade of behavioural futures*”, as Shoshana Zuboff characterizes the prediction products developed with such data.¹³⁵

Zuboff proposes three actions¹³⁶: (I) New legal frameworks. It is clear that our current legal frameworks haven’t kept pace with the rapid development of digital technologies over the past 30 years, and even less over these last 10 years of “big data revolution”. This implies that governments need to assume a role, and this cannot be that of personal data broker, nor can it promote weak or fuzzy legislation¹³⁷; (II) New forms of collective actions. We need reactive mechanisms at a societal level, akin to the 20th-century institutions of strikes and collective bargains. As a society, we need to move past the economic domain and become more than users. (III) Give a chance to alternatives. Creating competitive solutions to the currently established actors and supporting their activity if they play by the good rules.

Within the overall context of this syllabus, we will i.a. be focusing on the enhancement of secure and reliable privacy-enhancing techniques to provide data market peers with secure and economically attractive solutions. A secure playing field could by itself enhance the creation of competitive solutions for businesses and individuals, and equally, foster trust in data marketplaces. We will further discuss these elements in the remaining three chapters.

¹³⁵ Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Profile Books Ltd., London.

¹³⁶ *Ibid.*

¹³⁷ Warner, M.R., and Hawley, J. (2019). Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data. Retrieved January 17, 2020 from <https://www.congress.gov/bill/116thcongress/senate-bill/1951/text>.

4.4. CHAPTER 7. Organizational trust

Within the Safe-DEED research, WP2 and WP3 have extensively researched the subject matter of organizational trust. Hence, this chapter summarizes several key findings of this earlier research and transposes some writings of previous deliverables. These concern D2.3, D2.4, and D3.6, and may be consulted at <https://safe-deed.eu/deliverables/>.

Trust in data marketplaces is vital, though challenging to guarantee. Users namely need to trust that *inter alia*: (I) the data is of high quality and dependable; (II) the supply will be consistent and not break processes; (III) the data will deliver value once it has started to be used; (IV) the consumer will not steal the data (or have it stolen from them); and that (V) the consumer will not use the data for non-permitted use cases.

As a result, the possible lack of trust in data marketplaces can be deemed one of the reasons why marketplaces fail. In its “Communication on Building a European Data-economy”, the European Commission has equally stated that “*Trust will allow the digital economy to develop across the internal market*”.¹³⁸ As a result, the Commission has allowed for interdisciplinary research on the conceptualization of trust in the data market context and the fostering thereof. In addition to the Safe-DEED research, other noteworthy projects concern the EU-funded TRUSTS project (“Trusted Secure Data Sharing Space”)¹³⁹, and the KRAKEN project (“Brokerage and Market Platform for Personal Data”)¹⁴⁰, in all of which the KU Leuven Center for IT&IP Law is involved.

The importance of a trust-enhancing marketplace thus seems clear-cut. This brings forth two ensuing questions: how can “trust” best be defined in this context, and how can this trust be ensured to the most viable extent?

¹³⁸ 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-content/EN/TXT/?uri=COM:2017:9:FIN>>, accessed 11 December 2020.

¹³⁹ This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 871481.

¹⁴⁰ This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 871473.



Methodology: goal and objectives

General goal: to explore how to increase the organizational (B2B) and individual/end-user (B2C) trust in the data markets.

- O1** • **Formulate a definition of trust** for the purpose of the scope of this project (WP 1)
- O2** • **Understand the existing challenges** in establishing, maintaining and/or potentially increasing trust in B2B and B2C settings in the data markets (WP 2)
- O3** • **Formulate and evaluate the existing challenges** in establishing, maintaining and/or potentially increasing trust in B2B and B2C settings in the data markets (WP 3)
- O4** • **Suggest potential solutions** that could facilitate the trust building between the B2B and B2C stakeholders as well as increase the level of trust in the data markets (WP 4)

Safe-DEED



Trust in Data Marketplaces is essential to safeguard:

1. Data quality
2. Consistent data supply
3. Data value
4. Fair acquisition of data
5. Fair use of data
- ...

Safe-DEED

4.4.1. What is Organizational Trust?

4.4.1.1. The Concept of Organizational Trust

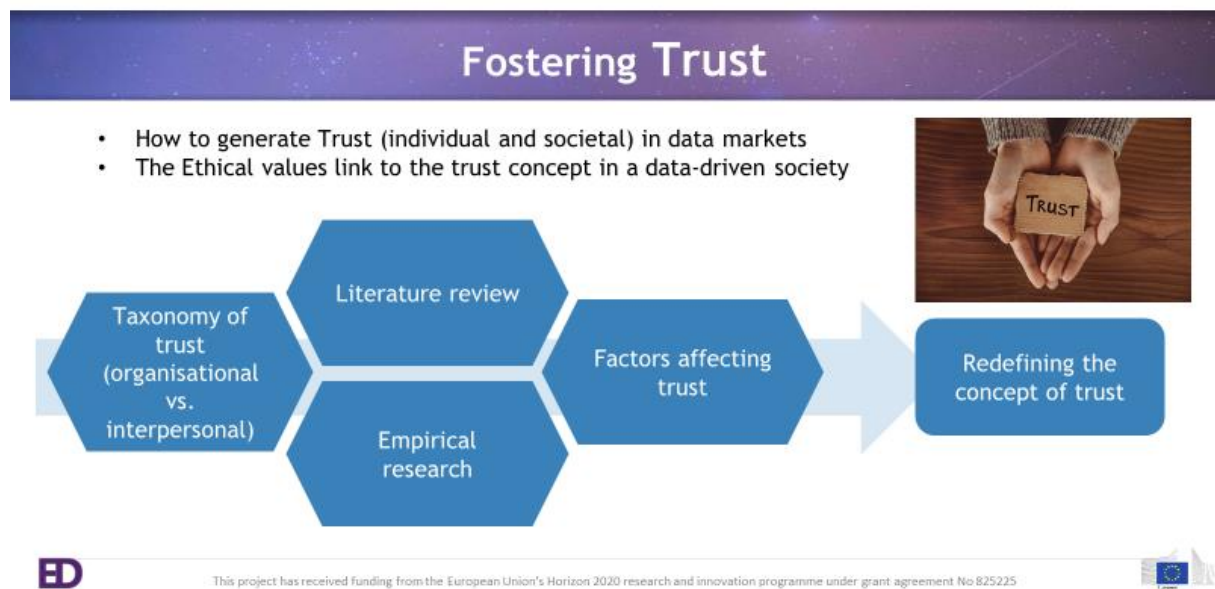
In the management context, trust can generally be discerned as being of relevance at three levels. Firstly, there is the concept of interpersonal trust, which refers to trust in a specific other or others.¹⁴¹ A second layer concerns “team trust”, which alludes to trust in interdependent people's collectivity

¹⁴¹ Lewicki, R. J., Tomlinson, E., Gillespie, N. 2006. Models of interpersonal trust development: Theoretical approaches, empirical evidence, and future directions. *Journal of Management*, 32: 991-1022; Rotter, J. B. 1980. Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35: 1-7.

pursuing a shared goal with inherently unique dynamics.¹⁴² Finally, “organizational trust” refers to trust in the entity of an organization.¹⁴³

For terminological reasons, it seems useful to point out that - in the organizational context -, the organization is the so-called “trustor”, whilst those interacting with it (both internally and externally) are “trustees”. Furthermore, organizational trust is relevant internally (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”.

Hence, in its simplest form, “organizational trust” can be defined as the trust in an organization, both internally and externally, build 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.¹⁴⁴



¹⁴² Guzzo, R. A., Dickson, M. W. 1996. Teams in organizations: Recent research on performance and effectiveness. *Annual Review of Psychology*, 47: 307-338; Serva, M. A., Fuller, M. A., Mayer, R. C. 2005. The reciprocal nature of trust: A longitudinal study of interacting teams. *Journal of Organizational Behavior*, 26: 625-648.

¹⁴³ Schoorman, F., Mayer, R. C., Davis, J. 2007. An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, 32: 344-354; Shockley-Zalabak, P., Ellis, K., Winograd, G. 2000. Organizational trust: What it means, why it matters. *Organization Development Journal*, 18: 35-48.

¹⁴⁴ Will Otto, ‘What is Organizational Trust (and how to build it)?’ The Predictive Index Blog, <https://www.predictiveindex.com/blog/what-is-organizational-trust-and-how-to-build-it/#:~:text=At%20its%20simplest%2C%20organizational%20trust,The%20organization's%20culture%20and%20values>, accessed 12 December 2020.

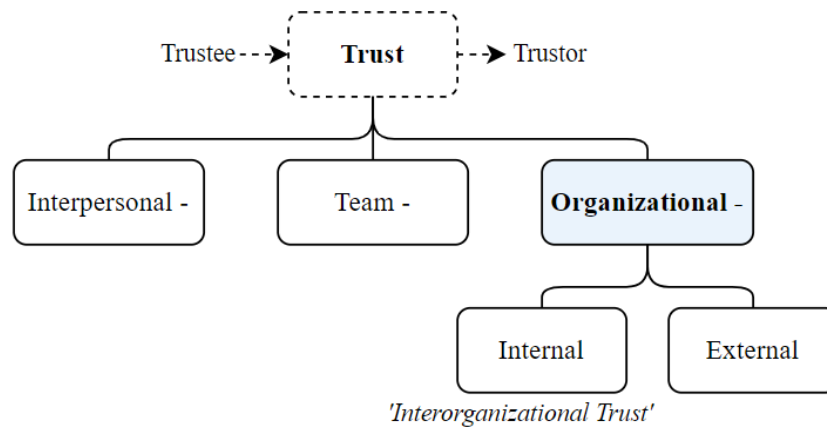


Figure 3. Organizational trust versus interpersonal trust ¹⁴⁵



The Structure and Focus of our Study on Trust



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



4.4.1.2. Antecedents of Organizational Trust

In its core - as with trust at all levels -, social exchange theory serves as a fundamental theoretical perspective to understand the underlying process of trust at the organizational level, with the specific aspects of the social exchange different from those at the lower levels.¹⁴⁶ It may be worth looking into these specific aspects to understand what antecedents organizational trust is built upon.

¹⁴⁵ Figure made by WP3, as part of the Safe-DEED research on organizational trust (D3.7).

¹⁴⁶ Ashley Fulmer & Michele Gelfand, 'At What Level (and in Whom) We Trust: Trust Across Multiple Organizational Levels' S.M.A. Journal of Management, 29 May 2012.

In the first place, it has been asserted that trustor characteristics undeniably go hand in hand with organizational trust. In this regard, it has been shown that both relationship satisfaction¹⁴⁷ and organizational identification¹⁴⁸ enhance trust. A climate of integrity¹⁴⁹ and leadership credibility¹⁵⁰ has unsurprisingly shown to add to trust in an organization. On a more inter-organizational level, it has been established that *inter alia* a common business understanding, shared by trustee and trustor, adds to the trust in the latter.¹⁵¹

Furthermore, communication is another essential antecedent to creating organizational trust.¹⁵² In virtual inter-organizational relations especially, trust is set to be higher when organizations can effectively communicate their trustworthiness.¹⁵³ Moreover, voluntary compliance with external regulations may equally add to trust in the organizational context.¹⁵⁴ Furthermore, so-called “asset specificity” of the exchanged resource (i.e., the extent to which the invested assets cannot be transferred, limiting the likelihood of contract breach) has been found to have a positive effect on trust as well.¹⁵⁵ Lastly, it may not come as a surprise that some organizational practices, such as fair, transparent, and coherent policies, also facilitate trust in organizations.¹⁵⁶ With regard to this, variables external to organizations such as unstable markets have been asserted to impact perceptions of organizational trustworthiness.¹⁵⁷

One last antecedent which may be worth mentioning at this stage, concerns the way in which organizations deal with trust breaches *ex post facto*, i.e. so-called “trust repair”. Though one single

¹⁴⁷ Davies, M. A. P., Lassar, W., Manolis, C., Prince, M., Winsor, R. D. 2011. A model of trust and compliance in franchise relationships. *Journal of Business Venturing*,26: 321-340.

¹⁴⁸ Maguire, S., Phillips, N. 2008. “Citibankers” at Citigroup: A study of the loss of institutional trust after a merger. *Journal of Management Studies*,45: 372-401.

¹⁴⁹ Palanski, M. E., Yammarino, F. J. 2009. Integrity and leadership: A multi-level conceptual framework. *Leadership Quarterly*,20: 405-420.

¹⁵⁰ Burton, R. M., Lauridsen, J., Obel, B. 2004. The impact of organizational climate and strategic fit on firm performance. *Human Resource Management*,43: 67-82.

¹⁵¹ Kasper-Fuehrer, E. C., Ashkanasy, N. M. 2001. Communicating trustworthiness and building trust in interorganizational virtual organizations. *Journal of Management*,27: 235-254.

¹⁵² Van Marrewijk, M. 2004. The social dimension of organizations: Recent experiences with great place to work assessment practices. *Journal of Business Ethics*,55: 135-146. doi:10.1007/s10551-004-1897-7. Gainey, T. W., Klaas, B. S. 2003. The outsourcing of training and development: Factors impacting client satisfaction. *Journal of Management*,29: 207-229.

¹⁵³ Kasper-Fuehrer, E. C., Ashkanasy, N. M. 2001. Communicating trustworthiness and building trust in interorganizational virtual organizations. *Journal of Management*,27: 235-254.

¹⁵⁴ Gillespie, N., Dietz, G. 2009. Trust repair after an organization-level failure. *Academy of Management Review*,34: 127-145.

¹⁵⁵ Katsikeas, C. S., Skarmeas, D., Bello, D. C. 2009. Developing successful trust-based international exchange relationships. *Journal of International Business Studies*,40: 132-155. doi:10.1057/palgrave.jibs.8400401. Gainey, T. W., Klaas, B. S. 2003. The outsourcing of training and development: Factors impacting client satisfaction. *Journal of Management*,29: 207-229.

¹⁵⁶ Pučetaité, R., Lämsä, A. 2008. Developing organizational trust through advancement of employees’ work ethic in a post-socialist context. *Journal of Business Ethics*,82: 325-337; Gillespie, N., Dietz, G. 2009. Trust repair after an organization-level failure. *Academy of Management Review*,34: 127-145.

¹⁵⁷ Hodson, R. 2004. Organizational trustworthiness: Findings from the population of organizational ethnographies. *Organization Science*,15: 432-445.

violation does not necessarily obliterate the trust relation¹⁵⁸, an early violation of benevolence in the inter-organizational context hampers trust significantly.¹⁵⁹ In addition, if a violation stems from the conduct at a high organizational level, trust repair becomes more challenging than when it occurs at a lower level within the organization.¹⁶⁰

Antecedents of trust

('What contributes to organizational trust?')

1. Relationship satisfaction
2. Organizational Identification
3. Climate of Integrity
4. Leadership Credibility
5. Common Business Understanding
6. Communication
7. Voluntary Regulatory Compliance
8. Asset Specificity
9. Fair, Transparent & Coherent Policies
10. Stable Markets
11. Trust Repair

Safe-DEED

4.4.1.3. Consequences of Organizational Trust

A high level of organizational trust has proven to ease the introduction of organizational change.¹⁶¹ Furthermore, it encourages knowledge sharing, especially when the knowledge is tacit or sensitive.¹⁶² Moreover, organizational trust in knowledge sharing becomes increasingly important in instances where organizations are high on interdependence and where the environment is competitive.¹⁶³

¹⁵⁸ Neergaard, H., Ulhøi, J. 2006. Government agency and trust in the formation and transformation of interorganizational entrepreneurial networks. *Entrepreneurship: Theory and Practice*, 30: 519-539.

¹⁵⁹ Bell, G. G., Oppenheimer, R. J., Bastien, A. 2002. Trust deterioration in an international buyer-supplier relationship. *Journal of Business Ethics*, 36: 65-78.

¹⁶⁰ Janowicz-Panjaitan, M., Krishnan, R. 2009. Measures for dealing with competence and integrity violations of interorganizational trust at the corporate and operating levels of organizational hierarchy. *Journal of Management Studies*, 46: 245-268.

¹⁶¹ Sonpar, K., Handelman, J., Dastmalchian, A. 2009. Implementing new institutional logics in pioneering organizations: The burden of justifying ethical appropriateness and trustworthiness. *Journal of Business Ethics*, 90: 345-359.

¹⁶² Wang, H. C., He, J., Mahoney, J. T. 2009. Firm-specific knowledge resources and competitive advantage: The roles of economic- and relationship-based employee governance mechanisms. *Strategic Management Journal*, 30: 1265-1285; Pablo, A. L., Reay, T., Dewald, J. R., Casebeer, A. L. 2007. Identifying, enabling and managing dynamic capabilities in the public sector. *Journal of Management Studies*, 44: 687-708.

¹⁶³ Sonpar, K., Handelman, J., Dastmalchian, A. 2009. Implementing new institutional logics in pioneering organizations: The burden of justifying ethical appropriateness and trustworthiness. *Journal of Business Ethics*, 90: 345-359.

Furthermore, collective perceptions that the organization is trustworthy can decrease internal conflicts. Such a downfall of conflicts *inter alia*¹⁶⁴ enhances contract flexibility¹⁶⁵, decreased negotiation costs¹⁶⁶, contract compliance¹⁶⁷, willingness to cooperate¹⁶⁸, positive interaction patterns¹⁶⁹, and continued cooperation.¹⁷⁰

Consequences of Trust

1. Organizational change
2. Knowledge-sharing
3. Less internal conflicts

Safe-DEED

4.4.2. Organizational Trust in Data Marketplaces

4.4.2.1. Trustee and Trustor

There is a growing need to foster trust amongst data providers and data users in the data marketplace context. Both can be regarded “trustees”, whilst the platform controller is the “trustor”. Other actors, such a complementary service provider, can be classified as “trustees” and play a role in ensuring trust

¹⁶⁴ Ashley Fulmer & Michele Gelfand, ‘At What Level (and in Whom) We Trust: Trust Across Multiple Organizational Levels’ S.M.A. Journal of Management, 29 May 2012.

¹⁶⁵ Faems, D., Janssens, M., Madhok, A., Van Looy, B. 2008. Toward an integrative perspective on alliance governance: Connecting contract design, trust dynamics, and contract application. *Academy of Management Journal*, 51: 1053-1078.

¹⁶⁶ Zaheer, A., McEvily, B., Perrone, V. 1998. Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science*, 9: 141-159

¹⁶⁷ Davies, M. A. P., Lassar, W., Manolis, C., Prince, M., Winsor, R. D. 2011. A model of trust and compliance in franchise relationships. *Journal of Business Venturing*, 26: 321-340.

¹⁶⁸ Stahl, G. K., Larsson, R., Kremershof, I., Sitkin, S. B. 2011. Trust dynamics in acquisitions: A case survey. *Human Resource Management*, 50: 575-603.

¹⁶⁹ Lado, A. A., Dant, R. R., Tekleab, A. G. 2008. Trust–opportunism paradox, relationalism, and performance in interfirm relationships: Evidence from the retail industry. *Strategic Management Journal*, 29: 401-423.

¹⁷⁰ Malhotra, D., Lumineau, F. 2011. Trust and collaboration in the aftermath of conflict: The effects of contract structure. *Academy of Management Journal*, 54: 981-998.

amongst data providers and data users. Hence, complementary service providers have a twofold role in this context. However, given that data providers and -users are the central actors in the data sharing process, this analysis will focus on them.

The data providers and users are essentially external actors to the marketplace. However, given that both data providers and users are active in the data market platform, it could be argued that both insights from an inter-organizational and external organizational trust can be deemed relevant in this specific context. In the data marketplace setting, the distinction between internal and external organizational trust is not as outspoken nor as crucial as in other frameworks. Consequently, the following brief analysis will not explicitly refer to this distinction.

4.4.2.2. Antecedents of Organizational Trust in Data Marketplaces

Several antecedents of trust have been outlined in the previous part of this overview. It may be worth applying these antecedents to the data market context. Therefore, the following synopsis will reiterate some of these antecedents and explain their relevance in fostering organizational trust in data marketplaces.

First is the antecedent of “Organizational Identification”, which can be defined as “*the propensity of a member of an organization to identify with that organization*”¹⁷¹, based on factors such as organizational support, communication, prestige and identity. In the data marketplace context, a clear organizational structure, clear communication on the data sharing processes, and sufficient support by complementary service providers may foster organizational identification and further enhance trust.

Another antecedent is integrity. Hence, there may be a need for a standardized code of conduct applicable in the data market context, which could be rooted in some of the ethical guidelines covered in chapter three. Such a code of conduct may also enhance leadership credibility (i.e. credibility of data market platform controllers), which was one of the enlisted antecedents. 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, which was marked as an antecedent of trust. Concretely, a code of conduct may thus enhance the conviction amongst data providers and – users that they are equal business partners, sharing and buying data in an integer setting.

Communication has been proven to be of the essence, especially in virtual settings. Hence, a clear visualized 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 hand in hand with the understanding that fair, coherent, and transparent policies add to trust.

One more antecedent concerned “asset specificity”. Thus, data marketplaces should limit the extents to which data can be transferred to restrict unwarranted data sharing scenarios. Against this backdrop, security- and privacy-enhancing techniques seem to be a must to safeguard organizational trust. Moreover, in the extent the GDPR applies to a concrete data sharing scenario, one could argue that

¹⁷¹ Albert, S., Ashforth, B. and Dutton, J. (2000). Organizational identity and identification: Charting new waters and building new bridges. *Academy of Management Review*, 25(1), 13-17.

asset specificity is already comprehensively governed by the principle of purpose-limitation in Art 5(1)(b) GDPR¹⁷², as discussed in chapter four of this syllabus.¹⁷³

It has equally been asserted that economically unstable sectors or markets negatively impact organizational trust. This instability factor does not seem to be of high relevance in the data market context, given that the business of data sharing is unequivocally expected to gain economic weight on a global scale.

Regarding trust repair, it is of the essence to safeguard and prevent – especially in the early stage – any security implications or contractual breaches. In this regard, privacy- and security-enhancing technologies seem to be of utmost importance as well.



4.4.2.3. Consequences of Organizational Trust in Data Marketplaces

These various antecedents may irrefutably foster organizational trust in data marketplaces, both amongst data providers and data users. In the data market context, the enhancement of trust is especially important, given that data usually concerns tacit and sensitive knowledge, especially in the case of personal data exchange. As mentioned before, the impact of organizational trust on an organisation's functioning is especially of the essence in these scenarios. It has also been pointed out that the weight of trustworthiness increases when an organization relies on interdependence and when the environment in which it operates is competitive. In the data market context, both elements are unquestionably present. Lastly, it has been stated 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.

¹⁷² Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 5(1)(b).

¹⁷³ *Supra* Chapter 4. 'The Protection of Personal Data'.

Therefore, it may be concluded that the impact of organizational trust on the enhancement of data marketplaces cannot be overstated. This adds to explaining why the European Commission put so much stress on fostering trust in its Communication on “Building a European Data-Economy”.¹⁷⁴

At this stage, we have discussed the various antecedents which may add to the enhancement of organizational trust. Henceforth, one final question remains: how should these antecedents be guaranteed in the particular data marketplace context? In other words, we now know a variety of elements which add to organizational trust (i.e., antecedents), but it remains questionable as to how these elements should best be substantiated to foster trust. The next part will briefly expand upon this issue.

4.4.3. Fostering Organizational Trust in Data Marketplaces

4.4.3.1. Three Pillars

The foregoing analysis has demonstrated that (I) clear communication, (II) a code of conduct, and (III) privacy- and security-enhancing technologies may add to enhancing antecedents of trust, including organizational identification, integrity, credibility, transparency, coherence, asset specificity, and trust repair.

In the particular data market context, the three pillars mentioned above (communication; code of conduct; privacy- and security-enhancing techniques) may be deemed most relevant, as this succinct analysis has shown. It is essential to safeguard a privacy-preserving data marketplace for the sharing of data regarding the latter. Moreover, there is a need for techniques which enable privacy-preserving data analytics. Following these two insights, encryption techniques seem to be essential to augment organizational trust further. This partly explains why the Safe-DEED project strongly focuses on secure multi-party computation (MPC) in the data market context. We will further discuss MPC in the two subsequent chapters. Nonetheless, at this stage, it may already be interesting to assess its impact on organizational trust.

4.4.3.2. MPC Encryption and Trust

Concerning MPC, one may raise the issue that encryption techniques' deployment brings forth fundamental legal issues. It is fair to state that the use of MPC raises particular legal challenges, amongst which liability issues, lacunae regarding the legal classification of the actors involved, and the ongoing uncertainty regarding the applicability of certain legal frameworks. One may thus play the devil's advocate and assert that these ensuing legal complications may, in their turn, impede the enhancement of organizational trust. In this light, the MPC-resolution thus seems to raise new fundamental trust challenges. Moreover, this decreases trust following from a lack of legal certainty that may lead to more conflicts and legal disputes, which will inadvertently hamper organizational trust to a large extent.

¹⁷⁴ 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-content/EN/TXT/?uri=COM:2017:9:FIN>>, accessed 22 December 2020.

The relationship between privacy- and security-enhancing techniques on the one hand, and organizational trust, on the other hand, seems to be a double-edged sword.

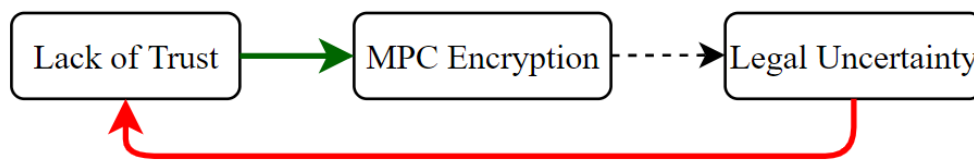


Figure 4. Organization trust and MPC encryption¹⁷⁵

4.4.4. Moving Forward

To prevent a potential negative impact on trust resulting from the use of MPC-encryption, three things seem of the essence.

Firstly, there is a need in academia to discuss and tackle some of the legal complications raised by the use of (MPC-) encryption techniques in the data sharing context. Within the Safe-DEED project, such a rudimentary attempt has been made, though more legal attention to this subject seems elemental with an eye on the future.

Secondly, this analysis has mentioned that (I) voluntary compliance with external regulations adds to organizational trust, and that (II) organizational trust is crucial for the advancement of data marketplaces. Merging these two insights makes it clear that respecting regulatory rules is not just important from a purely legal perspective but equally constitutes an economic incentive for data marketplaces. Hence, this analysis of trust should incentivize data markets to comply with the existing and future regulatory frameworks.

Thirdly, - though not mentioned in the previous parts of this analysis – (inter)organizational trust has been found to sustain cooperation when there is a lack of formal legal mechanisms, though can sometimes be substituted by thorough institutional forces. In other words, trust can sustain a lack of legal certainty, as well as the other way around. Hence, given that the use of MPC enhances organizational trust, the aforementioned ensuing legal cavities cannot be expected to *de facto* result in an impediment of organizational trust.

The relationship between legal certainty and organizational trust is thus ambiguous. On the one hand, both concepts can exist independently from one another, though it is not unequivocally clear to what extent. On the other hand, it is undeniable that legal certainty adds to organizational trust.

To guarantee the highest possible degree of organizational trust in data marketplaces, the usage of MPC encryption seems to be an invaluable asset, as long as there is sufficient attention to the forthcoming legal challenges arising from the usage of privacy- and security-enhancing techniques. Moreover, a code of conduct could indirectly foster organizational trust as well, and might be rooted in

¹⁷⁵ Figure made by WP3, as part of the Safe-DEED research on organizational trust (D3.7).

the ethical guidelines covered in the Safe-DEED Project. Lastly, clear communication is a straightforward yet essential trust-enhancing method as well. Certain communication standards could be included in the code of conduct. Furthermore, certain paradigms in the digital movement and social exchange theory may equally be considered, such as the aforementioned SSI concept. The following chart rudimentarily visualizes this succinct synopsis.

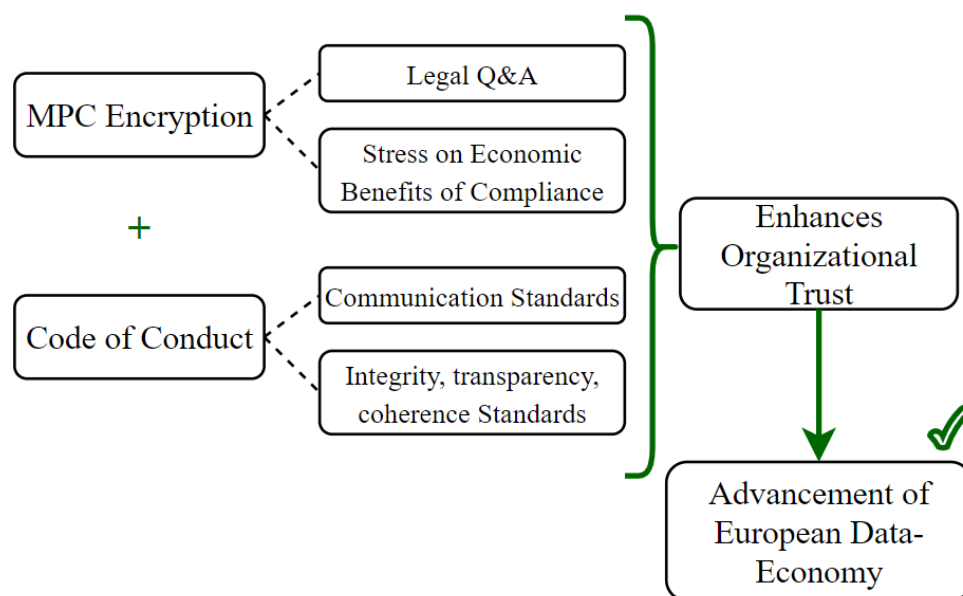


Figure 5. Organizational trust: summary¹⁷⁶

This analysis merely concerns an initial and rudimentary introduction to the concept of organizational trust in data marketplaces. Nevertheless, this chapter has demonstrated the importance of MPC encryption in the data market context. Hence, the following two chapters shall elaborate upon this subject. The first chapter will generally introduce encryption, the relevant legal framework and the particular MPC technique. The final chapter of this syllabus will ultimately assess some legal issues arising from the use of MPC encryption.

¹⁷⁶

Figure made by WP3, as part of the Safe-DEED research on organizational trust (D3.7).

4.5. CHAPTER 8. Secure Multi-party Computation (MPC)

Within the Safe-DEED research, WP2, WP3 and WP5 have extensively researched the subject matter of encryption. Hence, this chapter summarizes several key findings of this earlier research, and transposes some writings of previous deliverables. These concern D2.1, D2.2, D2.3, D2.4, D2.6, D3.1, and D5.1-D5.10, and may be consulted at <https://safe-deed.eu/deliverables/>.

As outlined in chapter two of this syllabus, data marketplaces' functioning profoundly relies on their ability to safeguard privacy and security.¹⁷⁷ The previous chapter has also demonstrated that both these elements play an intrinsic role in enhancing organizational trust.¹⁷⁸ In this new chapter, a particular encryption method will therefore be put forward, which may be of great value in guaranteeing privacy and security in the data market context.

Data should namely be encrypted to safeguard the privacy- and security-concerns innate to data sharing on marketplaces. Encryption can best be defined as the process of converting information or data into a code, especially to prevent unauthorized access. Thus, data encryption seems to be an essential means to guarantee privacy and security on the data marketplace platform. In this chapter, we shall first discuss the EU legal framework on encryption. Subsequently, a brief introduction shall be devoted to MPC encryption.

4.5.1. EU Encryption Framework

The European Union has recently included encryption provisions in different binding legislative initiatives, such as GDPR (Art 32)¹⁷⁹ and the European Electronic Communication Code, and Reports and Opinion Papers, such as the ENISA Opinion Paper Encryption.¹⁸⁰ In addition, the Council of the European Union has recently adopted a resolution on "*Security through encryption and security despite encryption*".¹⁸¹ Herein, the Council reiterates that "*encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society*".¹⁸² This statement reaffirms the importance of encryption in ensuring both the security and privacy of data marketplaces in the EU.

¹⁷⁷ *Supra* Chapter 2 'Data Marketplaces: an introduction'; 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-content/EN/TXT/?uri=COM:2017:9:FIN>>, accessed 22 December 2020.

¹⁷⁸ *Supra* Chapter 7 'Organizational Trust'.

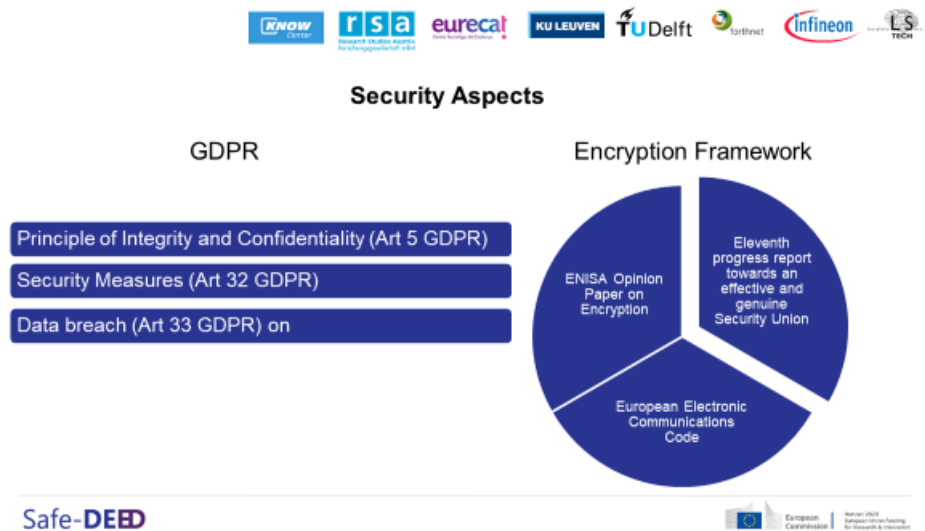
¹⁷⁹ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J.E.U., L119/1, Art 32.

¹⁸⁰ ENISA's Opinion Paper on Encryption <https://www.enisa.europa.eu/publications/enisa-position-papers-andopinions/enisas-opinion-paper-on-encryption>, accessed 14 December 2020.

¹⁸¹ Council of the European Union, 'Security through Encryption and Security despite Encryption', Council Resolution 13084/1/20, Brussels, 24 November 2020.

¹⁸² *Ibid.* page 2.

Ultimately, the end goal of encryption would thus be the enhancement of a secure European digital economy. One may wonder why mere legal measures are not sufficient to enforce a high level of security. In other words, why is there a need for technical security-enhancing techniques, such as encryption? The EU has dealt with this question in a series of documents, three of which shall briefly be presented hereunder.



4.5.1.1. ENISA Opinion Paper on Encryption

ENISA is the European Union Agency for Network and Information Security. It works closely with the EU Member States and other stakeholders to deliver advice and solutions and improve their cybersecurity capabilities. It also supports the development of a cooperative response to large-scale cross-border cybersecurity incidents or crises. Since 2019, ENISA has been drawing up cybersecurity certification schemes.

In 2016, ENISA published an Opinion Paper on encryption.¹⁸³ The purpose of the paper was to provide an overview of encryption and decryption protocols for security services. The ENISA's Opinion delivers key messages about encryption that policymakers should consider when discussing potential legislative initiatives in this field.

One of the main takeaways of ENISA's Opinion is related to the use of backdoors. The EU Agency strongly argues against the use of backdoors by law enforcement due to their inability to ensure users' security and confidentiality. Other key messages delivered by ENISA were that *“(I) judicial oversight may not be a perfect solution as different interpretations of the legislation may occur; (II) history has shown that technology beats legislation and criminals are best placed to capitalize on this opportunity; (III) It is very difficult to restrict technical innovation using legislation; and (IV) the*

¹⁸³

Ibid.

*experience in the US showed that limiting the strength of encryption tools inhibited innovation and left the competitive advantage in this area with other jurisdictions”.*¹⁸⁴

Hence, according to ENISA Opinion Paper, legal pathways may not always be the most well-suited to address security issues, which once again reaffirms the additional need for privacy- and security-enhancing technologies, such as MPC encryption in the data sharing context.

ENISA Opinion Paper on Encryption

ENISA = European Union Agency for Network and Information Security

1. Mere judicial oversight insufficient
2. Technology usually beats legislation
3. Technical innovation is hard to restrict
4. Limiting encryption inhibits innovation

4.5.1.2. Eleventh Progress Report: Towards an Effective and Genuine Security Union

In 2016, the EU Commission started publishing a series of monthly reports where the progress made in the area of security is described. The reports highlight the areas where additional legislative efforts are necessary. Every report follows the same structure: “(I) *tackling terrorism and organised crime and the means that support them*; and (II) *Strengthening our defenses and building resilience against them*”.¹⁸⁵

The Eleventh report (published on 12th October 2016) was mainly focused on anti-terrorism measures. The report provides a specific section dedicated to encryption and its use. In the report, the EC highlights the difficulties in balancing, on the one hand, the interests of citizens in having ensured the confidentiality and security of their personal data (Art 32 GDPR) and, on the other hand, the necessity for law enforcement and judicial authorities in prosecuting and investigating crimes. This conflict is a common thread in many instances within IT law. The balancing between individuals' fundamental rights and the public interest usually makes up for a rigorous assessment.

¹⁸⁴ *Ibid.* p.5.

¹⁸⁵ Communication from the Commission to the European Parliament, the European Council and the Council. First progress report towards an effective and genuine Security Union <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52016DC0670&from=EN>, accessed 13 December 2020.

Hence, the EU Commission has attempted to guide this balancing exercise. Its report namely provides a set of measures to support law enforcement and judicial authorities. The measures follow two main guidelines: (a) legal measures to facilitate access to encrypted evidence, (b) technical measures to enhance decryption capabilities. As a result, “*Member State authorities should have a toolbox of alternative investigation techniques at their disposal to facilitate the development and use of measures to obtain needed information encrypted by criminals.*”¹⁸⁶ The legislative initiatives described in the report relate to the cross-border access to electronic evidence and the development of a platform to exchange information, and the standardization of judicial cooperation between Member States (e-evidence Regulation proposal)¹⁸⁷. The report provides seven technical measures to enhance decryption capabilities. The measures focus on increasing the know-how among all Member States and their agencies and strengthening cooperation among all relevant stakeholders.

Thus, this report clearly demonstrates two key takeaways. Firstly, it emphasizes that cross-border threats require a concerted and multi-layered response. This can only be achieved through trust and joint work by all institutions and the Member States. Secondly, it shows that besides legal initiatives, there is a need for more uniform technical measures to ensure a secure Union. Henceforth, legislative measures and encryption techniques both have a role in enhancing security in the EU. This is similar to the overall conclusion of ENISA in its Opinion mentioned above.

EU Report ‘Towards an Effective and Genuine Security Union’

Balancing act between citizens’
interest & public security

Need for:

1. Legal measures to facilitate access to encrypted evidence
2. Technical measures to enhance decryption capabilities

4.5.1.3. European Electronic Communications Code

The Directive 2018/1972 establishing the European Electronic Code (EECC) has been adopted on the 11th of December 2018 and has been implemented in December 2020 by the Member States.¹⁸⁸ The

¹⁸⁶ *Ibid.* p.9.

¹⁸⁷ *Ibid.*

¹⁸⁸ Directive (EU) 2018/1972 establishing the European Electronic Communications Code (Recast) OJ L 321, 17.12.2018, p. 36–214.

EECC is considered crucial for the development of the EU Digital Single Market Strategy.¹⁸⁹ It amends four different Directives¹⁹⁰ and governs all aspects involving providers of electronic communication networks and their competent national authorities. In the security provisions, the EECC references to encryption protocols and, explicitly, to end-to-end encryption. First of all, it requires providers of public electronic communication networks to inform their users about any potential security threat that might affect their service, and the measures taken to ensure communications security. To comply with the requirement, Recital 96 EECC makes a specific reference to encryption.¹⁹¹ Moreover, the EECC provides that, where appropriate to guarantee safety and privacy of communication, the adoption of end-to-end encryption should be made mandatory by Member States.¹⁹² At the same time, the EECC leaves such a possibility to the discretion of Member States.¹⁹³

End-to-end encryption (E2EE) is a secure communication method that prevents third-parties from accessing data while transferring from one end system or device to another. In E2EE, the data is encrypted on the sender's system or device, and only the recipient is able to decrypt it. An example of an electronic communications provider that uses E2EE concerns WhatsApp, which provides its users with the message that their messages have been encrypted, merely allowing the sender and receiver to read them.

Thus, the EECC hammers on the usage of E2EE encryption, which indicates that the European Union acknowledges the importance of encryption to guarantee and safeguard a secure European digital economy. Furthermore, the ENISA Opinion Paper and the EC Progress Report have demonstrated the need for the uniform application of encryption (and decryption) techniques, in addition to any legal means to ensure security in the Union. Following this, we will now discuss a particular encryption technique, which may be of great importance in the data marketplace context: secure multi-party encryption, or shortly “MPC”.

4.5.2. MPC explained

4.5.2.1. Concept

MPC is a cryptographic technique where two or more parties perform a joint computation, which results in a meaningful output without disclosing the input provided by either party.¹⁹⁴ Conceptually, MPC makes it possible to balance the interest between different actors. On the one hand, data

¹⁸⁹ *Ibid.* Recital 3.

¹⁹⁰ Specifically, the Code amends Directive 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC.

¹⁹¹ Directive (EU) 2018/1972 establishing the European Electronic Communications Code (Recast) OJ L 321, 17.12.2018, Recital 96.

¹⁹² *Ibid.* Recital 97.

¹⁹³ *Ibid.* Recital 40.

¹⁹⁴ Bestavros, A., Lapets, A., & Varia, M. (2017). User-centric distributed solutions for privacy-preserving analytics. *Communications of the ACM*, 60(2), 37-39. Choi, J. I., & Butler, K. R. (2019). Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities. *Security Communication Networks*, 2019; Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., & Tan, Y.-a. (2019). Secure Multiparty Computation: Theory, practice and applications. *Information Sciences*, 476, 357-372.

consumers (i.e. businesses that use data or insights) can gain insights from providers' data securely. On the other hand, data providers can also get security assurance because they can retain the data's secrecy.

In other words, secure multi-party computation is a subfield of cryptography to create methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptographic tasks, where cryptography assures security and integrity of communication or storage, and the adversary is outside the participants' network, the cryptography in this model protects participants' privacy from each other. In the data market context, this would thus entail that data providers cannot be aware of one another's exact data, especially of the essence with regard to personal data.

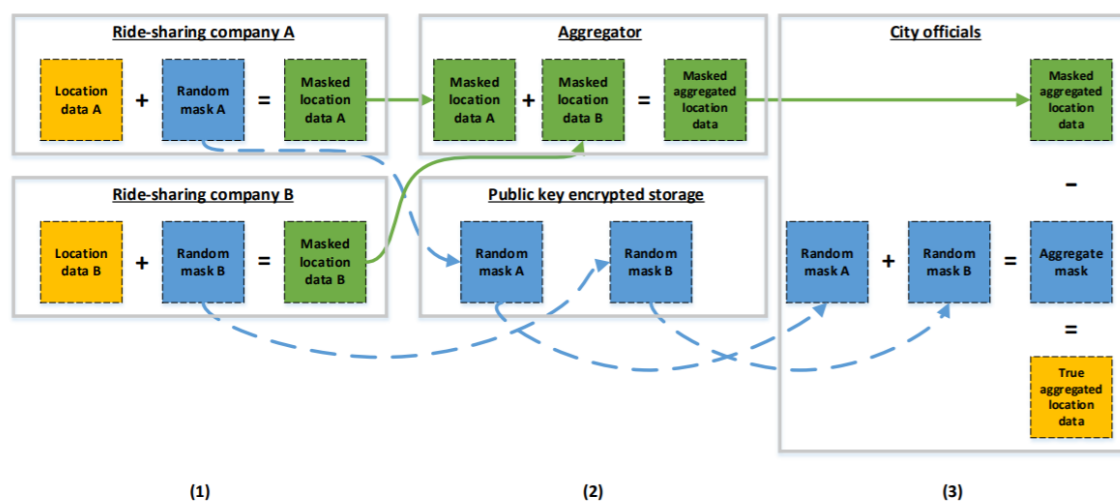


Figure 6. MPC explained¹⁹⁵

This figure shows the illustration of how MPC works.¹⁹⁶ To contextualize this illustration in a real-life setting, consider an example use case where city officials (column (3) in Figure 2) are trying to understand the influence of ride-sharing vehicles on traffic congestion. Therefore, some essential data held by ridesharing companies (column (1) in Figure 2) are needed. This data includes, for example, popular pickup spots and the number of cars in service during rush hour. However, this is confidential and sensitive data, meaning that releasing such information may result in adverse effects such as losing a competitive advantage over rivals.

In this case, we can then use the MPC-based solution to allow the aggregation of ride-sharing data from companies without disclosing the individual data point. For the MPC-based solution, the ride-

¹⁹⁵ Figure adapted from, Bestavros, A., Lapets, A., & Varia, M. (2017). User-centric distributed solutions for privacy-preserving analytics. Communications of the ACM, 60(2), 37-39. Initially presented in Safe-DEED D2.2, https://safe-deed.eu/wp-content/uploads/2020/12/Safe-DEED_D2_2.pdf, p. 10.

¹⁹⁶ Bestavros, A., Lapets, A., & Varia, M. (2017). User-centric distributed solutions for privacy-preserving analytics. Communications of the ACM, 60(2), 37-39.

sharing companies will apply a random number to mask/protect their data. In this way, we ensure that the actual value of the data cannot be read anymore. An aggregator then aggregates this masked data. At the same time, the public key encrypted storage aggregates only the different random masks, which do not hold any data, used by the companies (see column (2) in Figure 2). Finally, the requester party (in this case city officials) then receives the aggregated masked data and the aggregated mask. They can then use the aggregated mask to transform the masked aggregated results into the plain-text aggregated results (see column (3) in Figure 2).

In this stage, the city officials now hold the plain text aggregated data, for example, to build heat-maps, without any party involved in the computation having access to other parties' plain text data.

4.5.2.2.MPC in the data marketplace context

We can apply this illustration to the sharing of data on data marketplaces. In chapter two of this syllabus, the overall functioning of data markets was presented. Against this backdrop, the following visualization was used:

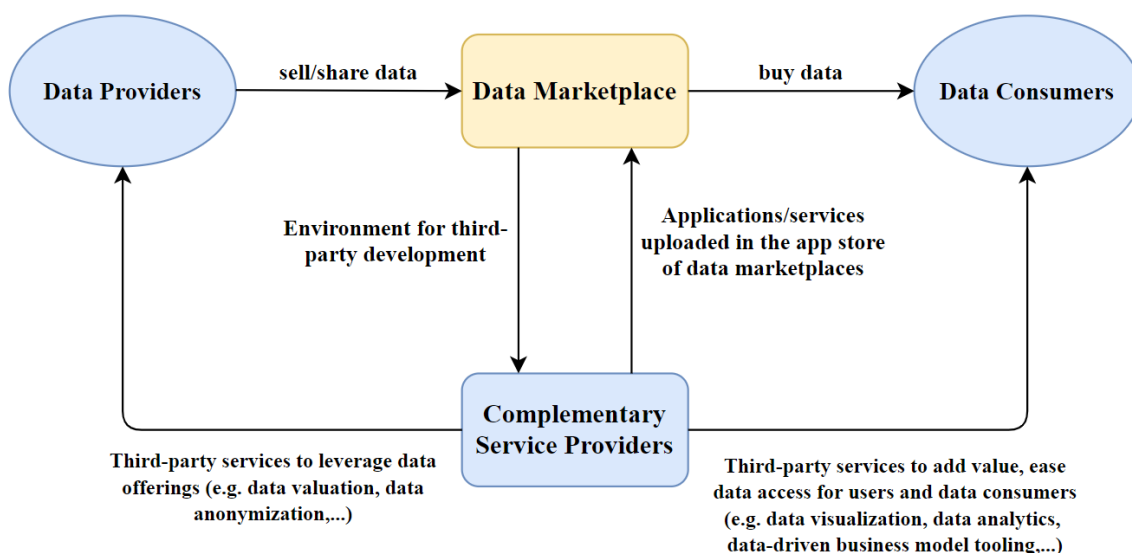


Figure 7. Roles in data marketplaces ecosystems, adapted from Spiekermann (2019)¹⁹⁷

Hence, on a data marketplace, numerous data providers share their (personal) data. Using MPC encryption, each dataset will be encrypted with a “random mask”, and will result in a masked dataset. These masked datasets will then be aggregated and eventually end up with the data user (or “data consumer”), which could be city officials, as was the case in the illustration above. The data consumer will then be able to use the aggregated mask to decrypt the masked aggregated data. Hence, the data consumer has no way of knowing what data belonged to what data provider; they namely only receive

¹⁹⁷ Figure made by WP3 for the Safe-DEED project in light of D3.5, based on: Spiekermann, M. (2019). Data Marketplaces: Trends and Monetization of Data Goods. *Intereconomics*, 54(4), 208-216

the aggregated data in the end. By the same token, no data provider knows what data belongs to other data providers. This is the big asset of MPC as an encryption technique: it guarantees the security and privacy of individual data providers, both vis-à-vis the data consumer and all other external actors, as well as vis-à-vis all other data providers as well.

4.5.2.3.Relevance

MPC could overcome barriers of data sharing in the business-to-business context. By using MPC, data providers could regain control over their data since it is not necessary to exchange data. Instead, data consumers will only receive insights from the computation of multiple datasets. This is a value proposition that MPC offers: allowing data sharing safely and securely. In such a way, MPC can also help to deal with compliance, depending on the way it is implemented.

Ultimately, MPC could potentially increase trust in sharing data via data marketplaces. It is important to be aware that massive implementations of MPC in real-life settings are yet to happen and still limited to only a few applications, such as auction-based pricing¹⁹⁸, tax fraud detection¹⁹⁹ and satellite collision prevention.²⁰⁰ There are multiple barriers to this lack of implementation, such as usability issues (e.g. too complex to understand by non-experts, suspicion in the computation results), technical issues (i.e. performance limitations and scalability) and legal aspects (i.e. current regulations discourage cooperation).²⁰¹ Furthermore, to the best of our knowledge, the application of MPC within the data marketplaces setting is still scarce.

¹⁹⁸ Bogetoft, P., Christensen, D. L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., . . . Pagter, J. (2009). Secure multiparty computation goes live. Paper presented at the International Conference on Financial Cryptography and Data Security.

¹⁹⁹ Bogdanov, D., Jõemets, M., Siim, S., & Vaht, M. (2015, January). How the estonian tax and customs board evaluated a tax fraud detection system based on secure multiparty computation. In International conference on financial cryptography and data security (pp. 227-234). Springer, Berlin, Heidelberg.

²⁰⁰ Hemenway, B., Lu, S., Ostrovsky, R., & Welser Iv, W. (2016, August). High-precision secure computation of satellite collision probabilities. In International Conference on Security and Cryptography for Networks (pp. 169-187). Springer, Cham.

²⁰¹ Choi, J. I., & Butler, K. R. (2019). Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities. Security Communication Networks, 2019.

4.6. CHAPTER 9. Secure Multi-party Computation: Legal Questions & Answers

In the data-market context, different actors and entities are interacting and complying with multiple regulatory frameworks. In particular, the entities involved in the data-market value chain can be divided into three macro-groups, where multiple actors interact at different levels. In such a transaction context, main discussion concerns who has ownership over such data and how such a right can be turned into legal protection. Unfortunately, civil law, which includes property law, contractual law, and liability law, represents is massively regulated at the national level within the EU area.

Contrary, other aspects such as competition law, data protection and privacy law, and consumer protection are areas where the EU legislator has the competence to legislate. Therefore, data markets legal challenges are affected by the tension between EU and national legislation and between those entities' economic efficiency relying on data as an economic asset and individual legitimate interest to retain personal information.

Hence, this last chapter will succinctly analyze some of the most stringent legal questions arising from MPC encryption. The structure of this chapter is Q&A-based. Hence, each subchapter will assess one legal question and its corresponding answer. This chapter aims to give an insight into the various challenges resulting from the use of MPC and the overall issues hindering the advancement of a data-driven EU economy.²⁰²

4.6.1. Liability for Wrongful Data-sharing

In an MPC context, what happens if the data provider shares incorrect data, and I make a wrong decision: who is to blame?

The answer to this question depends on a cascade of subsequent questions:

1. Is there any particular EU harmonization on liability in the context of the sharing of data to MPC protocols?

There exists **no** specific liability regime concerning the concrete scenario of data sharing using MPC protocol. Therefore, reference ought to be made to the general liability regimes in the EU and domestic tort laws.

²⁰² Taking into account the European Commission's suggestions, and after having received input from interested parties, KUL has decided to develop a 'legal question and answer' style analysis of secure multi-party computation. This assessment provides an elemental insight in some relevant yet persistent legal issues arising from the use of MPC. A full overview of the "legal FAQ on MPC" can be accessed here: <https://safe-deed.eu/legal-faq-on-multi-party-computation/>. Moreover, some of the content includes extracts from KUL deliverable D3.4. The full deliverable is available at https://safe-deed.eu/wp-content/uploads/2020/12/Safe-DEED_D3_4.pdf.

2. Is there any general EU harmonization on liability, which may be applicable in this context?

Firstly, it ought to be stated that the liability regime within the EU is mostly non-harmonized, with the exclusion of i.a.:

- product liability law under Directive 85/374/EC;
- certain aspects of liability for infringing data protection law (Art 82 of the General Data Protection Regulation (GDPR);
- liability for breaching competition law (Directive 2014/104/EU);
- liability insurance concerning damage caused by the use of motor vehicles (Directive 2009/103/EC); and
- conflict of tort laws, in the veil of the Rome II Regulation.
- Sectoral legislations (i.e. EU consumer protection framework)

Given that this question does not relate to data protection or competition law concerns, the only potentially applicable regime concerns the product liability directive. The question then arises whether data could be regarded as a product under Directive 85/374/EC. If this is the case, our answer will be embedded in the harmonized liability regime innate to this Directive. Unfortunately, specialized literature chiefly rejects such an interpretation. Hence, based upon both the materially limited notion of “product” under the Directive, as well as on internal Safe-DEED research, it seems that Directive 85/374/EC shall not be applicable in establishing the liability regime in this case scenario.

To conclude it is possible to affirm there exists no harmonized liability regime concerning damage stemming from the provision of incorrect plain text to an MPC protocol.

3. Are there any domestic liability rules that could be applied to the MPC case scenario?

The existing domestic liability regimes may not always be unequivocally applied *mutatis mutandis* to the MPC context. In other words, these rules may not always plainly fit the very nature of MPC protocols; nor may they be adapted to new technologies in general. In conclusion, due to the substantial divergences between all member states' liability regimes, the outcome of cases will often be different depending on which jurisdiction applies.

4. Which are the most common forms of liability in domestic laws applicable to this use case?

Despite these substantial differences between the liability regimes in EU member states, most states' fault-based regimens are generally rooted in the same criteria (most commonly distinguished as “fault”, “damage”, and “causal relation”). Our concrete case scenario relates to the “fault”-criterion (“would committed the wrongful act?”).

Fault-based liability

Most EU domestic laws share the same legal conception of “fault” under their respective liability laws. To establish “fault”, two aspects should be determined: (I) it ought to be identified that the duties of

care of the perpetrator have been discharged, and (II) it should be proven that the conduct of the perpetrator of the damage did not discharge those duties as stressed by H Koziol.

The duties at issue are determined by a plethora of (non-)legal factors. Occasionally, they are defined beforehand by statutory language prescribing or prohibiting certain specific conduct. Still, they must often be reconstructed after the court's fact based on social beliefs about the prudent and reasonable course of action in the circumstances (i.e., the principle of good neighbourliness, or *bonus pater familias*). In other words: can it be expected – from an average and reasonable data provider in similar circumstances – that he or she would share correct data? If the answer to this question is affirmative, it could be argued that the data provider has committed wrongful conduct on this occasion. If it can then subsequently be established that the data user's (economic) damage can be causally attributed to this wrongful conduct, the data provider can be held liable for these damages.

This entire question rests on what can be expected from an average and reasonable data provider in similar circumstances. Suppose the nature of the data is f.i. to be properly understood and correctly shared by the average, suitable data provider, it would be difficult to attribute them the liability to be properly understood and correctly shared by the average, suitable data provider. Consequently, we should question what can be expected from an average, reasonable data provider whilst providing data to an MPC protocol. These sorts of questions usually depend on the court's interpretations and their respective balancing exercise. Given the non-existence of relevant case law, it seems necessary regulators need to focus on filling this gap in ascertaining liability in these complex contexts.

Strict liability (i.e. non-fault based liability)

When it comes to strict liability occurs when the action put in place is intended generate a tort. Consequently, the claimant need only prove that the tort occurred and that the defendant was responsible. Notwithstanding overall understanding across the EU, its precise conditions strongly differ depending on the Member State, though its conditions are generally more restrictive than a fault-based liability. Moreover, imposing strict liability in the scenario of data trading may have its pitfalls. Strict liability namely implies that one can be held liable without having committed a fault. Such an easy acceptance of liability would undeniably frighten data providers from sharing their data. In turn, this would hamper the advancement of data marketplaces.

Vicarious liability

Vicarious liability is a situation in which one party is held partly responsible for a third party's unlawful actions. The third party also carries his or her own share of the liability. Vicarious liability typically arises when one party is supposed to be responsible for (and have control over) the third party. It is correspondingly negligent in carrying out that responsibility and exercising that control. Nonetheless, in this MPC scenario, no such relationship or responsibility seems to be at play whatsoever. Hence, it seems highly unlikely that this third form of liability would apply to our case scenario.

Therefore, it can be concluded that there is not a harmonized regulation that deals with the liability occurring in an MPC scenario. Therefore, it is necessary to refer to the domestic laws of the EU Member States. Similarly, also at a national level, a liability regime tailored on MPC protocols has not been developed yet. Thus, the precise liability when providing data to an MPC protocol is still

somewhat unclear (*de lege lata*). Still, it is possible to list down general considerations on liability regimes.

Generally, in the EU domestic liability regimes, a differentiation is made between fault-based, strict and vicarious liability.

The allocation of liability thus generally relies on two factors:

- 1) the particular domestic law that applies – which depends on the facts of the case; and
- 2) what can be expected from an average, reasonable data provider (*bonus pater familias*) in similar circumstances – which strongly depends on what courts consider the norm in each scenario.

4.6.2. Liability in Decentral MPC Protocol

When running an MPC protocol decentrally by both the data provider and user, who is liable if things go wrong?

The question on who is liable (data provider or user) whilst running a decentralized MPC protocol generally depends on what is meant with “when things go wrong”. Usually, the parties’ potential respective liabilities can be ascertained by answering the following steps:

- If the damage can be attributed to one of the parties (i.e. the data provider OR the data user), and this party did not behave in line with the *bonus pater familias* criterion, this party has committed a misconduct fault. If this misconduct can then be established to have causally resulted in damage pursuant to the applicable domestic laws, then this party can be held liable.
- Suppose no misconduct can be attributed to neither (or one) party. In that case, no liability can be concluded for the ensuing damage unless there is a form of strict liability under the domestic law that applies in the concrete case scenario.
- Suppose a fault can be attributed to both parties. In that case, both parties can be held liable if their national laws recognize joint liability (i.e. both data provider and user are fully liable for all damage) or several liabilities (i.e. the parties are merely liable for their respective proportionate obligations).

Scenario	Data provider liable?	Data user liable?	Both liable?
<u>Data Provider</u> : no fault <u>Data User</u> : no fault	strict liability	strict liability	joint (or several) strict liability
<u>Data Provider</u> : fault <u>Data User</u> : no fault	Fault-based liability	strict liability	joint (or several) strict liability

<u>Data Provider</u> : no fault <u>Data User</u> : fault	strict liability	Fault-based liability	joint (or several) strict liability
<u>Data Provider</u> : fault <u>Data User</u> : fault	Fault-based liability	Fault-based liability	joint (or several) liability

4.6.3. The Trustworthiness of MPC Protocol

How can I know that the protocol that is running is indeed a trustworthy MPC one?

The perceived trustworthiness of MPC chiefly depends on the perceived transparency and perceived coherence of such a protocol. Both transparency and perceived coherence mainly rely upon respectively the MPC applications' transparency on data protection and the coherence regarding the intent of the application. Nonetheless, transparency and coherence merely add to perceived trustworthiness.

For an MPC cryptographic protocol to be considered trustworthy, these transparency and coherence guarantees ought to have legal value so that any false claims can be legally challenged. Consequently, it is necessary to focalize on the EU privacy and data protection framework since it embeds the two principles. In Art.5 GDPR, the EU legislator has listed both transparency and coherence (of the processing- purpose limitation) as crucial principles of the EU privacy and data protection framework. The compliance of an MPC protocol with both principles of transparency and purpose limitation needs to be verified throughout a tailored assessment on the implications such protocols have for data subjects.

In the MPC context, such assessment has to mainly focus on the nature of encrypted data (personal vs non-personal) and consequent applicable legal regime depends; in other words, on whether or not such data can be related and identify a natural person. In fact, according to Art 4.1, GDPR defines "personal data" and stipulates its core elements, being: (I) any information, (II) relating to, (III) identified or identifiable, and (IV) a natural person. The first and last elements do not seem to be controversial in the MPC context, while the others require additional considerations. Given that the "related to" element is generally accepted as being broad and encompassing all (in)direct references to a natural person, encryption does not seem to hinder this element. The identifiability criterion seems slightly more disputable. Over the years, the EU data protection regulators and the European Court of Justice have tried to substantiate further the notion of "identifiable" under the GDPR.

If the MPC protocol meets specific criteria listed both by the Court of Justice and the EU data protection regulators data-set containing personal data cannot be identified by entities other than the one in possession of the encryption key. Still, such an activity, determining the anonymization of personal data through the use of encryption protocols, falls into the definition of "processing (of personal data)" of the GDPR and, thus, needs to comply with the EU privacy and data protection framework. Consequently, encrypted data can be classified anonymous only after (and not yet during) they have been fully encrypted. Consequently, only those entities processing anonymous and non-

identifiable data will not have to comply with legal and ethical requirements stemming from such a framework. The others, involved in such a process will always have to ensure the respect of privacy and data protection principles, consequently providing the necessary safeguards for the data subjects. Such protocols, once the respect of certain technical criteria is secured, can be fairly defined trustworthy.

The level of transparency and coherence are usually regarded as indicators of trustworthiness. Nonetheless, this merely concerns perceived trustworthiness and might – albeit being an initial indicator – not guarantee a protocol’s actual trustworthiness. Therefore, one may opt to consult the trustworthiness of the protocol running an MPC. Personal data encryption can be classified as personal data processing under Art 4 GDPR. Hence, the institutions backing the encryption are under a legal obligation to adhere to the transparency and data protection obligations in the GDPR. Consequently, in case of a lack of transparency or apparent trustworthiness, data subjects may use the legal remedies foreseen in the GDPR (Art 77-82).

4.6.4. Reliability of MPC Protocol

As a data subject, how can I know that the MPC protocol does not share my raw data?

In order to assess whether the MPC protocol is indeed not sharing my raw personal data, as data subject, I can rely upon my right to transparent information embedded in the GDPR. Moreover, suppose I believe my data has not been properly encrypted. In that case, I can ultimately rely on the remedies foreseen in the GDPR, such as the right to lodge a complaint with a supervisory authority or the right to an effective judicial remedy against a controller or processor.

4.6.5. Assurances of Non-Identification

What if a data user runs the MPC algorithm so many times that he can ‘guess’ my input data from it? (i.e., differential privacy). Are there any assurances against this?

This question relates to the case where the data user runs the algorithm so many times that the data provider’s input can be guessed. In other words: the data now is identifiable again and therefore can be regarded as “personal”.

From a legal-technical standpoint, the argument can then be made that the body backing the MPC algorithm (i.e. the data processor) has not been able to sufficiently guarantee its security obligation pursuant to Art 32 GDPR and Rec. 83.

Moreover, it could be argued that the entity managing the processing activity of personal data through MPC (the data controller) has not met his “lawfulness of processing” obligation. If this processing is

carried out to ultimately identify the input of the data subject, then the (now) personal data have been obtained in violation of the GDPR principles and consequently not ensuring data subjects' rights.

Nonetheless, it should be stated that the first safeguard only holds if it can demonstrate that the data processor could have done more to ensure the security of personal data. If the MPC algorithm functioned according to expectation and the processor could not know any further risks, this safeguard can hardly be applied. Moreover, the second safeguard vis-à-vis the data controller can only be put forward if the data market peer intentionally processed the data to identify the data provider's input. Any "accidental" discoveries in this regard do not seem to be sufficiently grave to trigger the data user's failed responsibility under Art 6(4)e GDPR. Still, the data provider can enforce these two safeguards by relying upon the remedies in chapter VIII GDPR.

4.6.6. Legal Safety of MPC Protocol

Is this MPC method safe to use from a legal perspective?

The wording "safe to use from a legal perspective" is rather broad. Hence, it seems that this question comprises two consequent issues:

1. Does MPC respect the data providers' fundamental rights?

Whether or not a cryptographic technique is "safe to use from a legal perspective" relies upon its ability to protect the data provider's fundamental rights. These are most commonly grounded in several fundamental rights protection schemes, most predominantly consisting of the United Nations Universal Declaration of Human Rights, the European Convention of Human Rights, and the Charter of Fundamental Rights of the European Union. Still, a mere focus on fundamental rights protection does have its innate shortcomings.

The use of MPC, if meeting certain technical and legal requirements, might represent "a fair measure" to balance on the one hand fundamental rights of data owners and the other legitimate business expectations of those entities involved in the data-markets' activities. MPC namely does not merely guarantee the protection of these rights vis-à-vis adversaries, but with regard to other participants to the algorithm as well, making it especially adequate in the data marketplace context.

2. Can this adherence to fundamental rights be legally guaranteed?

The MPC is a rather secure cryptography technique with an eye on fundamental rights protection. Nonetheless, the answer to this question is twofold: it should first be considered whether the data shared using an MPC protocol can be deemed "personal data" under the GDPR, as well as whether this activity can be classified as the "processing" thereof (idem. Art 2.1 GDPR). To do so, it is necessary to assess the nature of data processed and whether or not data available to parties other than the data controller can fall into the definition of personal data.

According to Art 4.1, GDPR defines "personal data" and stipulates its core elements, being: (I) any information, (II) relating to, (III) identified or identifiable, and (IV) a natural person. When such criteria have met the encryption of data using an MPC protocol could be classified as the processing of personal data under Art 4 GDPR. Hence, data providers are protected under the umbrella of the

GDPR. In the event also data available to other data market peers fall into the definition of personal data, we will have a joint controllership, with shared responsibilities among those entities in charge of the processing activities. Consequently, if an MPC application is backed by an institution that does not adequately provide or respect privacy and data protection principles, the data subject may rely on the complaints and judicial remedies laid down in GDPR. This is a legal backbone to ensure the respect of an MPC protocol for the data owner's fundamental rights.

This question can be interpreted in two interlinked ways. Firstly, the question is whether an MPC algorithm can be applied in line with the respect for the data owner's fundamental rights. On a subsequent level, it could be questioned whether there exist any legal guarantees to this adherence to data owners' fundamental rights.

Both sub-questions have been answered in the affirmative. In fact, concerning the right to data protection, an MPC that meets the technical criteria developed by the European Court of Justice and the EU body of data protection regulators ensures respects to the GDPR guiding principles and provides data subjects with necessary remedies.

4.6.6.1. Certification of MPC Processes

If an MPC method is safe from the legal perspective, will there be a certification process of the MPC implementation for the users to know which implementation complies most?

The EU Cybersecurity Act Regulation (hereafter “EU Cybersecurity Act”) foresees the implementation of an EU cybersecurity certification scheme for ICT products, ICT services, and ICT processes. This Act entered into force in June 2019 and was established under the mandate of the European Union Agency for Cybersecurity (ENISA). In light of the large diversity and many uses of ICT products, services and processes – the European Cybersecurity Certification framework enables the creation of tailored and risk-based EU certification schemes. In particular, each European scheme should specify: a) the categories of products and services covered, b) the cybersecurity requirements, for example by reference to standards or technical specifications, c) the type of evaluation (e.g. self-assessment or third party evaluation), and d) the intended level of assurance (e.g. basic, substantial and/or high).

At this point in time there is no explicit clarification as to whether the implementation of MPC encryption will fall within the ambit of the certification process innate to the EU Cybersecurity Act. Nonetheless, there are two indications that MPC encryption indeed falls within the material scope of application of the Regulation:

1. The Regulation applies to the certification of “ICT-services”. Under the autonomous definition, these include all services consisting fully or mainly in the transmission, storing, retrieving or processing of information through network and information systems. The encryption of personal data does fall within the scope of “processing of information”.²⁰³ Subsequently, it can hardly be contested that MPC encryption falls within the scope of application of the Regulation.

²⁰³

Supra Chapter 4. ‘The Protection of Personal Data’.

2. Rec. 40 of the Cybersecurity Act explicitly mentions that the promotion of basic multi-factor authentication – such as encryption – is part of ENISA’s goals.

Momentarily, it seems that the EU Cybersecurity Act does provide a legal basis for the certification of MPC encryption, which seems to have been confirmed by ENISA in its latest report. However, any further arrangements (on certification requirements, evaluation,...) regarding the certification schemes mainly rests on the ECCG, which has not explicitly reported on the certification of MPC encryption as of yet.

4.6.6.2.Evaluation of Encrypted and Personal Data

Can Personal and Encrypted Data be evaluated?

Data are nowadays considered precious production factors. When it comes to data, there is a strong link between the power of use and transfer of data on the one hand and the economic value associated with such data on the other hand. Consequently, the possibility to transfer data is linked to the possibility to confer commercial use of such data or data sets, without necessarily having the exclusive property right. Notwithstanding such a context, there are additional considerations we should do if the transfer interest personal data. Privacy and data protection law, in fact, do not foresee a comprehensive transfer of right to use. Data subjects always maintain certain rights over their data since this would go against the data subject's fundamental rights and ethical principles linked to such data.

Whether or not personal or encrypted data can be evaluated depends on what is being understood under “evaluation”. Notwithstanding the necessity to understand the monetary value of data, scholars, policymakers, and interested businesses should also consider other matters. All actors and entities providing and processing personal data assign them a specific value. Such value might be economic, ethical, normative and societal. In a scenario where consumers and businesses interact with each other, we should primarily assess such a relationship's characteristics and, subsequently, which are the values that lead such interactions. The main reason underlines the interaction and exchange of personal data between data subjects and business is represented by the reciprocal benefits they gain from such exchange. While business motivations are strictly economic, the data owner motivations can be economical (i.e. personalized service) and psychological (reduced time to find goods or services that might meet our interest).

Encryption does play a valuable role in preserving confidentiality and fundamental rights that embeds all listed values. In particular, the use of MPC protocol guarantees a substantial reduction of risks linked to personal data processing as requested by the GDPR. To achieve such a purpose, compliance of such cryptographic measures with the EU framework will be ensured following the measurable criteria listed by the European Court of justice and EU body of national data protection regulators. In concrete MPC likewise, other cryptographic measures should ensure the extreme difficulty (in terms of economic and personal effort) for third parties to identify data subjects from the available information. Concretely, the identification process should require third parties a disproportionate effort in terms of time, cost and workforce applicable to the whole data process. To conclude, the use of MPC will support activities of parties involved in data processing activities in complying with the

EU law, respect fundamental rights and individual ethical values, with a consequent overall positive outcome for society.

Concluding Note

This syllabus predominantly aimed at familiarizing the reader with some key insights, hoping that this may trigger their curiosity and their own critical thinking. The progression towards a data-driven economy in the European Union will be an everlasting process. Nonetheless, it is an exciting and intriguing challenge, which we hope has equally managed to captivate the reader of this syllabus. For more information on the content of this syllabus, do not hesitate to contact the Safe-DEED consortium. Thank you for your interest and curiosity.

References

Doctrine

- Albert, S., Ashforth, B. and Dutton, J. (2000). Organizational identity and identification: Charting new waters and building new bridges. *Academy of Management Review*, 25(1), 13-17.
- Bell, G. G., Oppenheimer, R. J., Bastien, A. (2002). Trust deterioration in an international buyer–supplier relationship. *Journal of Business Ethics*, 36, 65-78.

- Bello-Orgaz et al (2016). Social Big Data: Recent achievements and new challenges. *Information Fusion*, 28, 45–59.
- Benkler Y., ‘Between Spanish Huertas and the Open Road’:, *Governing Knowledge Commons* (Oxford University Press 2014).
- Bestavros, A., Lapets, A., & Varia, M. (2017). User-centric distributed solutions for privacy-preserving analytics. *Communications of the ACM*, 60(2), 37-39.
- Bogdanov, D., Jõemets, M., Siim, S., & Vaht, M. (2015, January). How the estonian tax and customs board evaluated a tax fraud detection system based on secure multiparty computation. In *International conference on financial cryptography and data security* (pp. 227-234). Springer, Berlin, Heidelberg.
- Burton, R. M., Lauridsen, J., Obel, B. (2004). The impact of organizational climate and strategic fit on firm performance. *Human Resource Management*, 43, 67-82.
- Choi, J. I., & Butler, K. R. (2019). Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities. *Security Communication Networks*, 2019.
- Cumbley and Church (2013). Is “Big Data” creepy? *Computer Law & Security Review*, 29, 601–609.
- Custers B. and Uršič H., ‘Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection’ (2016) 6 *International Data Privacy Law* 4.
- Davies, M. A. P., Lassar, W., Manolis, C., Prince, M., Winsor, R. D. (2011). A model of trust and compliance in franchise relationships. *Journal of Business Venturing*, 26, 321-340.
- Dhar, V. (2013). "Data science and prediction". *Communications of the ACM*. 56(12), 64–73.
- Drexl J., and others, ‘Data Ownership and Access to Data - Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate’ [2017] SSRN Electronic Journal.
- Faems, D., Janssens, M., Madhok, A., Van Looy, B. (2008). Toward an integrative perspective on alliance governance: Connecting contract design, trust dynamics, and contract application. *Academy of Management Journal*, 51, 1053-1078.
- Fulmer A. & Gelfand M. (2012). ‘At What Level (and in Whom) We Trust: Trust Across Multiple Organizational Levels’ *S.M.A. Journal of Management*, 38, 1167-1230.
- Gainey, T.W., Klaas, B.S. (2003). The outsourcing of training and development: Factors impacting client satisfaction. *Journal of Management*, 29, 207-229.
- Gillespie, N., Dietz, G. (2009). Trust repair after an organization-level failure. *Academy of Management Review*, 34, 127-145.

- Guzzo, R. A., Dickson, M. W. (1996). Teams in organizations: Recent research on performance and effectiveness. *Annual Review of Psychology*, 47, 307-338.
- Hodson, R. (2004). Organizational trustworthiness: Findings from the population of organizational ethnographies. *Organization Science*, 15, 432-445.
- Janeček V., ‘Ownership of Personal Data in the Internet of Things’ (2018) 34 *Computer Law and Security Review* 1039., p.13.
- Janowicz-Panjaitan, M., Krishnan, R. (2009). Measures for dealing with competence and integrity violations of interorganizational trust at the corporate and operating levels of organizational hierarchy. *Journal of Management Studies*, 46, 245-268.
- Kasper-Fuehrer, E. C., Ashkanasy, N. M. (2001). Communicating trustworthiness and building trust in interorganizational virtual organizations. *Journal of Management*, 27, 235-254.
- Katsikeas, C. S., Skarmas, D., Bello, D.C. (2009). Developing successful trust-based international exchange relationships. *Journal of International Business Studies*, 40, 132-155.
- Koutroumpis, P., & Leiponen, A. (2013). “Understanding the value of (big) data.” 2013 IEEE International Conference on Big Data, Big Data 2013 (pp. 38–42).
- Lado, A. A., Dant, R. R., Tekleab, A. G. (2008). Trust–opportunism paradox, relationalism, and performance in interfirm relationships: Evidence from the retail industry. *Strategic Management Journal*, 29, 401-423.
- Lewicki, R. J., Tomlinson, E., Gillespie, N. (2006). Models of interpersonal trust development: Theoretical approaches, empirical evidence, and future directions. *Journal of Management*, 32, 991-1022.
- Maguire, S., Phillips, N. (2008). “Citibankers” at Citigroup: A study of the loss of institutional trust after a merger. *Journal of Management Studies*, 45, 372-401.
- Malgieri G., ‘Trade Secrets v. Personal Data: a possible solution for balancing rights’ (2016) 6(2) *International Data Privacy Law*, p. 102-116.
- Malhotra, D., Lumineau, F. (2011). Trust and collaboration in the aftermath of conflict: The effects of contract structure. *Academy of Management Journal*, 54, 981-998.
- Neergaard, H., Ulhøi, J. (2006). Government agency and trust in the formation and transformation of interorganizational entrepreneurial networks. *Entrepreneurship: Theory and Practice*, 30, 519-539.
- Pablo, A. L., Reay, T., Dewald, J. R., Casebeer, A. L. (2007). Identifying, enabling and managing dynamic capabilities in the public sector. *Journal of Management Studies*, 44, 687-708.
- Palanski, M. E., Yammarino, F. J. (2009). Integrity and leadership: A multi-level conceptual framework. *Leadership Quarterly*, 20, 405-420.

- Pučetaité, R., Lämsä, A. (2008). Developing organizational trust through advancement of employees' work ethic in a post-socialist context. *Journal of Business Ethics*, 82, 325-337.
- Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35, 1-7.
- Sadiku, M. *et al.* (2016). 'Data Visualization'. *International Journal of Engineering Research and Advanced Technology (IJERAT)*. 12. 2454-6135.
- Scanapiecco, M., Virgillito, A., Marchetti, M., Mecella, M., and Baldoni, R. (2004). The DaQuinCIS architecture: a platform for exchanging and improving data quality in Cooperative Information Systems. In: *Information Systems*. 29, 7, 551–582.
- Scassa T., 'Data Ownership' [2020] Centre for International Governance Innovation, p. 2.
- Schoorman, F., Mayer, R. C., Davis, J. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, 32, 344-354.
- Serva, M. A., Fuller, M. A., Mayer, R. C. (2005). The reciprocal nature of trust: A longitudinal study of interacting teams. *Journal of Organizational Behavior*, 26, 625-648.
- Shockley-Zalabak, P., Ellis, K., Winograd, G. (2000). Organizational trust: What it means, why it matters. *Organization Development Journal*, 18, 35-48.
- Solove, D.J. (2005): A taxonomy of privacy. In: *University of Pennsylvania Law Review*; 154(3), 477- 560.
- Sonpar, K., Handelman, J., Dastmalchian, A. (2009). Implementing new institutional logics in pioneering organizations: The burden of justifying ethical appropriateness and trustworthiness. *Journal of Business Ethics*, 90, 345-359.
- Spiekermann, M. (2019). Data Marketplaces: Trends and Monetization of Data Goods. *Intereconomics*, 54(4), 208-216.
- Spiekermann, S., Acquisti, A., Böhme, R., and Hui, K.-L. (2015): The challenges of personal data markets and privacy. *Electron Markets* 25, 2 (June 2015), 161–167.
- Stahl, G. K., Larsson, R., Kremershof, I., Sitkin, S. B. (2011). Trust dynamics in acquisitions: A case survey. *Human Resource Management*, 50, 575-603.
- Swinnen K., 'Ownership of Data : Four Recommendations for Future Research' (2020) 5 *Journal of Law, Property and Society* 139.
- Van Erp S., 'Ownership of Digital Assets and the Numerus Clausus of Legal Objects' [2017] *SSRN Electronic Journal* 1.
- Van Marrewijk, M . (2004). The social dimension of organizations: Recent experiences with great place to work assessment practices. *Journal of Business Ethics*, 55, 135-146.

- Wang, H. C., He, J., Mahoney, J. T. (2009). Firm-specific knowledge resources and competitive advantage: The roles of economic- and relationship-based employee governance mechanisms. *Strategic Management Journal*, 30, 1265-1285.
- Zaheer, A., McEvily, B., Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science*, 9, 141-159.
- Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., & Tan, Y.-a. (2019). Secure Multiparty Computation: Theory, practice and applications. *Information Sciences*, 476, 357-372.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Profile Books Ltd., London.

Case law

- CJEU Case C-101/01 Bodil Lindqvist, ECLI:EU:C:2003:596.
- CJEU Case C-131/12 Google v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317.
- CJEU Case C-582/14 Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779.

Legislations

- Article 29 Working Party, ‘Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector’ (WP 211).
- Article 29 Working Party, ‘Opinion 03/2013 on purpose limitation’ (WP 203).
- Article 29 Working Party, ‘Opinion 1/2010 on the concepts of controller and processor’ (WP169).
- Article 29 Working Party, ‘Opinion 3/2010 on the principle of accountability’ (WP 173).
- Article 29 Working Party, ‘Opinion 4/2007 on the concept of personal data’ (WP 136).
- Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407.
- Commission decision COMP/M.7217 – Facebook/WhatsApp, 3 Oct. 2014. Commission Notice on the definition of relevant market for the purposes of Community competition law, OJ L 372, 9.12.1997
- Commission Regulation (EC) No 802/2004 of 21 April 2004 for the notification procedure.
- Commission Regulation (EU) No 316/2014 of 21 March 2014 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of technology transfer agreements, OJ L 93, 28.3.2014, p. 17–23

-
- Commission Regulation (EU) No 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices, OJ L 102, 23.4.2010, p. 1-7.
 - Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, OJ C 11, 14.1.2011, p. 1-72.
 - Communication from the Commission to the European Parliament and the Council, First progress report towards an effective and genuine Security Union, (COM/2016/0670) final).
 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ICT Standardisation Priorities for the Digital Single Market, (COM/2016/0176 final).
 - Communication from the Commission to the European Parliament, the European Council and the Council. First progress report towards an effective and genuine Security Union (COM(2016) 670 final).
 - 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).
 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, (COM(2012) 9 final).
 - Communication from the Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region – Commission Work Programme 2016 – No time for business as usual' (COM/2015/0610 final).
 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).
 - Council Regulation (EC) No 1/2003 of 16 Dec. 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 4.1.2003, p. 1-25.
 - Council Regulation (EC) No 139/2004 of 20 Jan. 2004 on the control of concentrations between undertakings (the EC Merger Regulations). OJ L 24, 29.1.2004, p. 1-22.
 - Council Resolution (EC) No 13084/1/20, 'Security through Encryption and Security despite Encryption', Brussels, 24 November 2020.
 - Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 31.7.2002.
 - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194, 19.7.2016 p. 1–30.
 - Directive (EU) 2018/987 establishing the European Electronic Communications Code (Recast) OJ L 321, 17.12.2018, p. 36–214.
-

- Directive (EU) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data OJ L 281, 23.11.1995 p. 31–50.
- EDPS Ethics Advisory Group 2018 Report, Towards a digital ethics. ENISA's Opinion Paper on Encryption 2016.12.12 European Convention of Human Rights, Council of Europe, 1953.
- European Union, Consolidated version of the Treaty on the Functioning of the European Union, 13 December 2007, 2008/C 115/01, Art 52.
- European Union, Consolidated version of the Treaty on the Functioning of the European Union, 13 December 2007, 2008/C 115/01, Art 52.
- OECD, Data Driven Innovation: Big Data for Growth and Well-Being (OECD 2015) 197.
- Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, (COM/2015/0635 final).
- Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, (COM(2015) 634 final).
- Proposal for a Regulation of the Parliament and the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). (COM/2017/0477 final - 2017/0225).
- Protocol 27 on the internal market and competition, annexed to the TFEU, OJC 115, 09.05.2008.
- Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services O J L 186, 11.07.2019, p. 57–79.
- Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 Oct. 2012 on European Standardisation, OJ L 316, 14.11.2012.
- Regulation (EU) No 2018/1807 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.
- Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

Others

- Baldwin, H. (2015). Drilling Into The Value Of Data.
<https://www.forbes.com/sites/howardbaldwin/2015/03/23/drilling-into-the-value-of-data>

- Ballivian, A. and Fenohasina, R.M. (2015) Measuring the Value of Data. URL: https://statswiki.unece.org/download/attachments/117772954/World%20Bank_Ballivian_Mare_MeasuringtheValueofData_20151202.pdf?version=1&modificationDate=1473158675433&api=v2.
- Blake Morgan, ‘100 Stats on Digital Transformation and Customer Experience’, <https://www.forbes.com/sites/blakemorgan/2019/12/16/100-stats-on-digital-transformation-and-customer-experience/?sh=357f12d73bf3>.
- Deloitte, “Measuring the Economic Impact of Cloud Computing in Europe”, final report prepared for the European Commission <https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloudcomputing-europe>, accessed 6 December 2020.
- European Data Market study, SMART 2013/0063, IDC, 2016.
- Evodevo srl and the European Economic and Social Committee, ‘Study on the Ethics of Big Data: Balancing Economic Benefits and Ethical Questions of Big Data in the EU Policy Context’, p. 15-20, 36.
- information. McKinsey Global Institute, McKinsey Center for Government, McKinsey Business Technology Office.
- Manyika, J. et al. (2013) Open Data: Unlocking innovation and performance with liquid
- OECD Glossary of Statistical Terms. OECD. 2008.
- Safe-DEED Project Goals Visualization, <https://safe-deed.eu/>.
- Statistical Language - What are Data?. *Australian Bureau of Statistics*. 13-07-2013., <https://www.abs.gov.au/websitedbs/D3310114.nsf/Home/Statistical+Language+-+what+are+data>.
- Vasudha, T., and Arvind, G. (2017). The value of data. World Economic Forum. <https://www.weforum.org/agenda/2017/09/the-value-of-data/>
- Verhenneman G, Vedder A, WITDOM, D6.1 – Legal and Ethical framework and privacy and security principles, p. 39, 2015, available at: <http://www.witdom.eu/deliverable>.
- Warner, M.R., and Hawley, J. (2019). Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data. Retrieved January 17, 2020 from <https://www.congress.gov/bill/116thcongress/senate-bill/1951/text>.
- Will Otto, ‘What is Organizational Trust (and how to build it)?’ The Predictive Index Blog, <https://www.predictiveindex.com/blog/what-is-organizational-trust-and-how-to-build-it/>.

Annex

This annex provides an overview of the PowerPoint slides that have been used throughout the video lecture series.

Chapter 1. The Value of Data

KU LEUVEN

Lecture 1 – The Value of Data

Safe-DEED

Top publicly traded companies by market capitalization (fourth quarter of 2020)

1. **Apple**
2. **Microsoft**
3. **Amazon**
4. **Alphabet (Google)**
5. **Facebook**
6. **Tencent Holdings**
7. Tesla
8. **Alibaba**
9. TSMC
10. Berkshire Hathaway



Safe-DEED

1. What is data?
2. Why is it valuable?



Safe-DEED

What is data?



= “characteristics or information that are collected through observation.”



Safe-DEED

Big Data

4 Characteristics (“4 V’s”)

1. Volume
2. Velocity
3. Variety
4. Veracity

Safe-DEED

Data Value

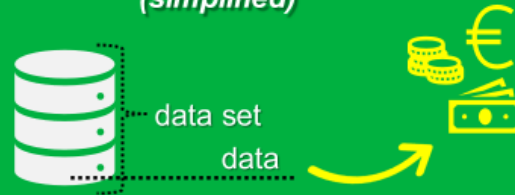


Data Science

Safe-DEED

Extracting Value from Data

(simplified)



1. Collection
2. Storage
3. Cleansing
4. Analysis
5. Visualization

Safe-DEED

Extracting Value from Data

(simplified)



Source: Dynamicfieldwork.com

- 1. Collection**
2. Storage
3. Cleansing
4. Analysis
5. Visualization

Safe-DEED

Extracting Value from Data

(simplified)



Source: Antillonline.com

1. Collection
- 2. Storage**
3. Cleansing
4. Analysis
5. Visualization

Safe-DEED

Extracting Value from Data

(simplified)



Source: AnalyticsindiaMag.com

1. Collection
2. Storage
- 3. Cleansing**
4. Analysis
5. Visualization

Safe-DEED

Extracting Value from Data

(simplified)



data set
data



Source: Monkeyvision.nl

1. Collection
2. Storage
3. Cleansing
- 4. Analysis**
5. Visualization

Safe-DEED

Extracting Value from Data

(simplified)



data set
data



Source: Boostlabs.com

1. Collection
2. Storage
3. Cleansing
4. Analysis
- 5. Visualization**

Safe-DEED

Extracting Value from Data



Source of picture: Acention.com

Safe-DEED

The Exchange of Data



Data Marketplaces

Safe-DEED

Building a European Data Driven Economy

Challenges:

1. Lack of coordination
2. Lack of infrastructure/funding
3. Shortage of expertise/skills
4. Legal Complexity

Safe-DEED

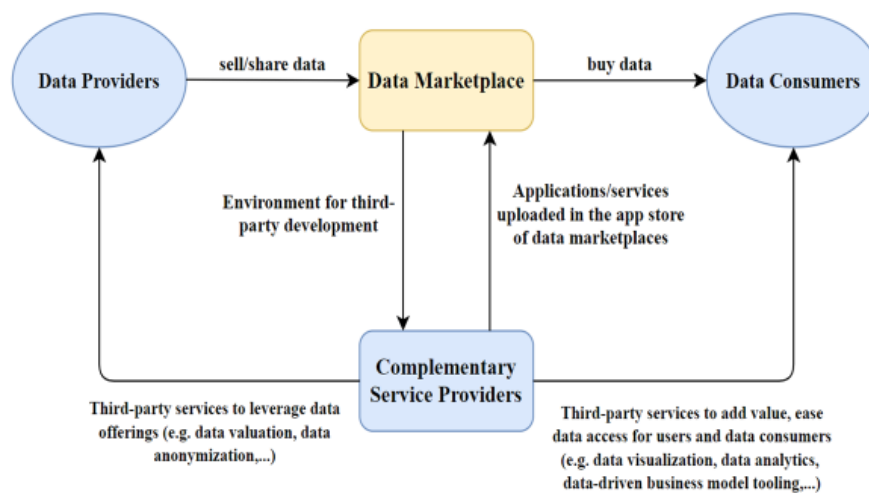
Chapter 2. Data Marketplaces

KU LEUVEN

Lecture 2: Data Marketplaces

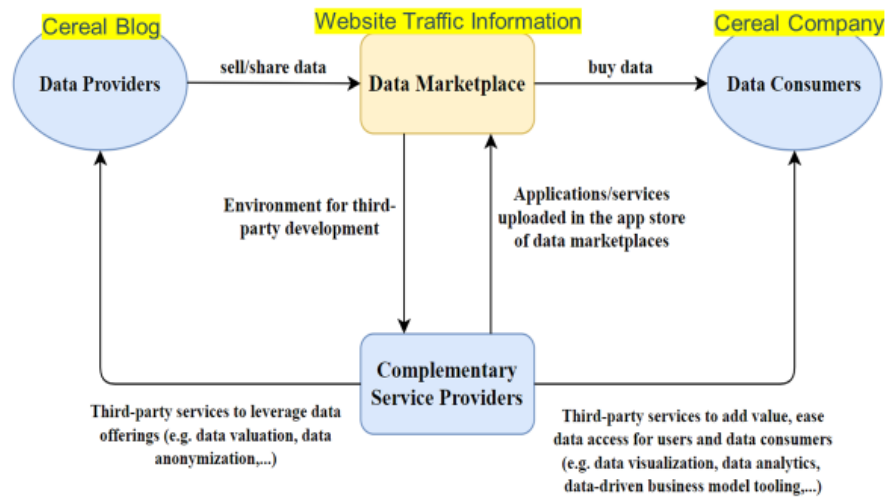
Safe-DEED

Structure of a Data Marketplace



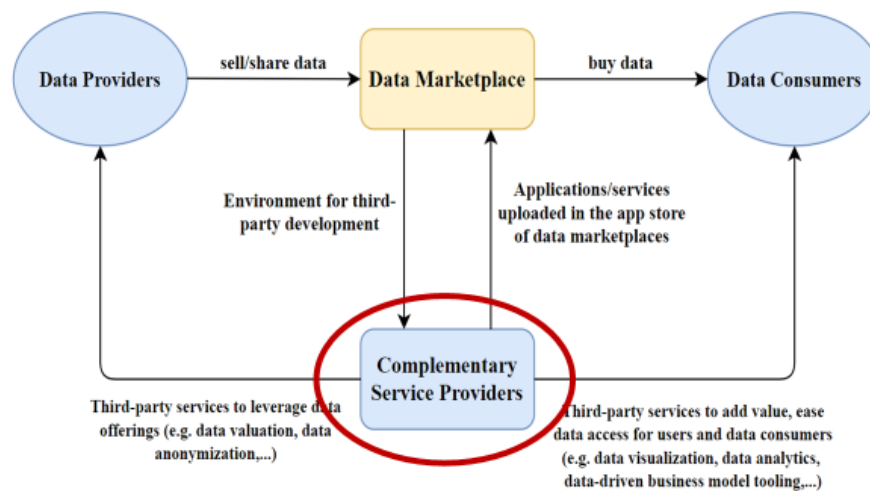
Safe-DEED

Structure of a Data Marketplace



Safe-DEED

Structure of a Data Marketplace



Safe-DEED

Benefits of Data Marketplaces

Safe-DEED

Benefits for Data Providers

1. Lucrative
2. Long-term economic benefits
3. Support to new companies



Safe-DEED

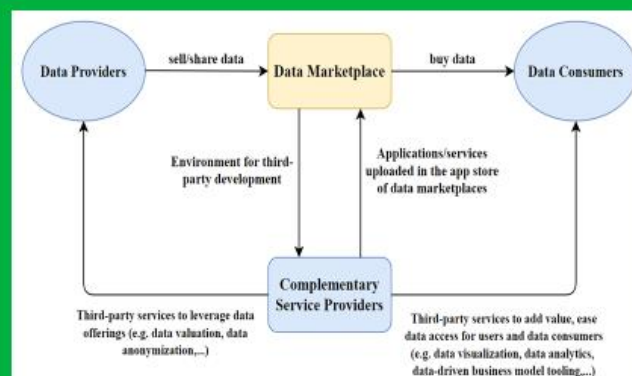
Benefits for Data Users

1. Access to outside data
2. Speed
3. Safety, however:
 1. Trust problems
 2. Security issues



Safe-DEED

Conclusion



Safe-DEED

Chapter 3. Ethical Guidelines

KU LEUVEN

Lecture 3 – Ethical Guidelines

Safe-DEED

**Ethical Guidelines to be
considered in moving toward a
more data-driven economy**

Safe-DEED

Fundamental Moral Principles



Autonomy



Justice



Beneficence



Non-maleficence



(Responsibility)

Safe-DEED

European Data Protection Supervisor (EDPS)



Source: edps.europa.eu

Safe-DEED

Seven shifts that urge the need to redefine digital ethics



Safe-DEED

Five Recommendations

No compromises can ever be made regarding:

-  Human dignity
-  Personhood
-  Freedom of choice
-  Accountability
-  Moral values

Safe-DEED

Chapter 4. The Protection of Personal Data

KU LEUVEN

Lecture 4 – The Protection of Personal Data

Safe-DEED

The General Data Protection Regulation

- 25 May 2018
- Aims:
 - The regulation of the processing of personal data
 - The regulation of the free movement of personal data

Safe-DEED

Scope

Art 2(1): 'The processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'

Safe-DEED

Material Scope: 'Processing'



Art 4(2): any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means

Examples: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data

Safe-DEED

Material Scope: 'Personal Data'

Art 4(1): 'any information relating to an identified or identifiable natural person'.



Any Information...



Relating to...



An Identified/identifiable...



Natural person



Safe-DEED

Personal Scope



1. **Data Controller:** (Art 4(7)) 'The natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data.'
2. **Joint Controllers**
3. **Data Processor:** (Art 4(8)) 'natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.'

Safe-DEED

General Principles



Lawfulness



Accuracy



Fairness



Storage limitation



Transparency



Integrity and confidentiality



Purpose limitation



Accountability



Data minimization



Safe-DEED

Controllers' Obligations



Respect for General Principles



Specific Transparency Requirements



Assurance of Security

Safe-DEED

Data Subjects' Rights



The right to access



The right to the restriction of the processing



The right to ratification



The right to data portability



The right to erasure of data



The right to object

Safe-DEED

Chapter 5. The Protection of Non-Personal Data

Lecture 5 – The Protection of Non-Personal Data

‘Non-Personal Data’?


Personal data = ‘any information relating to an identified or identifiable natural person’. Art 4(1) GDPR




“Building a European Data Economy”

EC Communication, 10/01/2017


What?

Towards a single data market in the EU 

Why?

 citizen wellbeing

 business opportunities

 innovative public services

How? by overcoming:

 Data localization restrictions

 Obstacles by IT vendors

 Complex legal framework

 Lack of trust

Safe-DEED

Free Flow of Non-Personal Data Regulation

(FFNPDR) 28 May 2019

Core idea:

Free movement of non-personal data across borders

=

Every organisation should be able to store and process data
anywhere in the European Union



Safe-DEED

Scope

Applies to “the **processing** of electronic data **other than personal data** in the Union, which is provided as a service to users residing or having an establishment in the Union”.
(Art 2 FFNPDR)

Material Scope: ‘Processing’



Art 4(2): any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means

Examples: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data

Safe-DEED

Purposes

‘Facilitating the free movement of non-personal data in the EU’



How?



Prohibition of mandatory data localization requirements



Guarantee of data availability for competent authorities



Facilitation of data porting by users

Safe-DEED

Purposes

'Facilitating the free movement of non-personal data in the EU'

How?



Prohibition of mandatory data localization requirements



Broad concept (Art 3 FFNPDR)



Transition period (Recital 21 FFNPDR)



Justification possible (Art 4 FFNPDR)

Safe-DEED

Purposes

'Facilitating the free movement of non-personal data in the EU'

How?



Guarantee of data availability for competent authorities



Safeguarded data exchange (Art 5 FFNPDR)

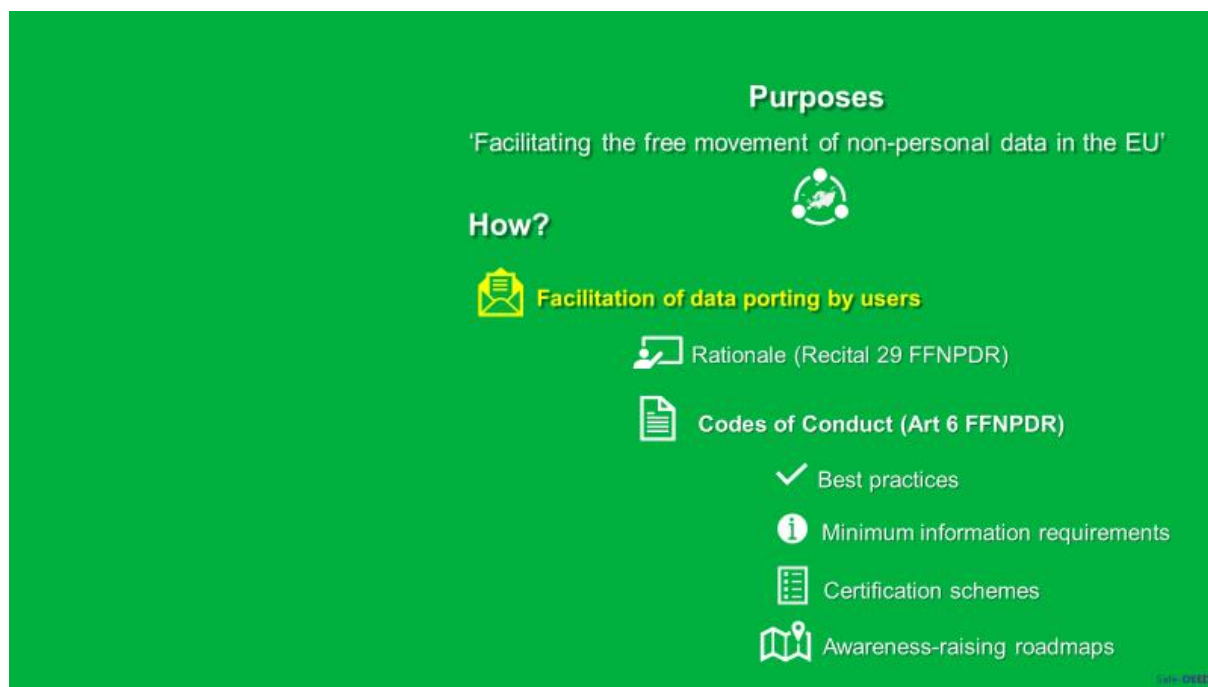


"Competent authority" (Art 3 FFNPDR)



Cooperation procedure (Art 7 FFNPDR)

Safe-DEED



Chapter 6. The Valuation of Data

KU LEUVEN

Lecture 6 – The Valuation of Data

Safe-DEED

The valuation of data: an economic perspective

Classification of data → helps putting an economic value on it

1. Data as a commodity

2. Data Ownership

1. Property
2. Intellectual Property: Copyright
3. Other related Intellectual Property Rights
4. GDPR

Safe-DEED

Data as a Commodity?

Commodity = An economic good with substantial fungibility (gold, oil,...)

Is data the new oil? 😞

- Increasing availability over time
- Variety in types, formats, methods,...

Safe-DEED

Data Ownership?



1. Political Sensitivity
2. Fundamental Rights Concerns
3. Lack of Common Understanding

Safe-DEED

Data as a Property



- **Civil law:** ownership = limited number of rights
- **Common law:** more flexible
- **Civil law:** *erga omnes* approach
- **Common law:** *in personam* & *in rem*

Safe-DEED

Data as a Copyright?



Legal Uncertainty

Safe-DEED

Alternative pathways for data ownership?

Trade Secret Directive? 

No *erga omnes* right

Database Directive ? 

Only protects the *collection* of data

Safe-DEED

GDPR?



No real ownership rights

Safe-DEED

Conclusion: data ownership? 😞

6 difficulties in classifying data as 'something that can be owned':

1. Political sensitivity
2. No common understanding of 'ownership'
3. No precise definition of 'data'
4. Rapid development data-economy
5. Fundamental rights concerns
6. Possible burden on transparency & innovation

Safe-DEED

A look beyond the economic approach

Alternative legislative initiatives to empower citizens: GDPR...

Big impact on current business models

Safe-DEED

A look ahead: the trade of behavioral futures



1. New legal frameworks
2. New forms of collective action
3. Become more than users

Safe-DEED

Chapter 7. Organizational Trust

KU LEUVEN

Lecture 7 – Organizational Trust

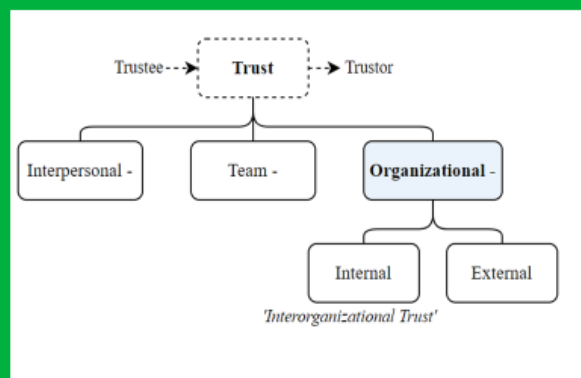
Safe-DEED

Trust in Data Marketplaces is essential to safeguard:

1. Data quality
 2. Consistent data supply
 3. Data value
 4. Fair acquisition of data
 5. Fair use of data
- ...

Safe-DEED

What is 'trust'?



Safe-DEED

Antecedents of trust

("What contributes to organizational trust?")

1. Relationship satisfaction
2. Organizational Identification
3. Climate of Integrity
4. Leadership Credibility
5. Common Business Understanding
6. Communication
7. Voluntary Regulatory Compliance
8. Asset Specificity
9. Fair, Transparent & Coherent Policies
10. Stable Markets
11. Trust Repair

Safe-DEED

Consequences of Trust

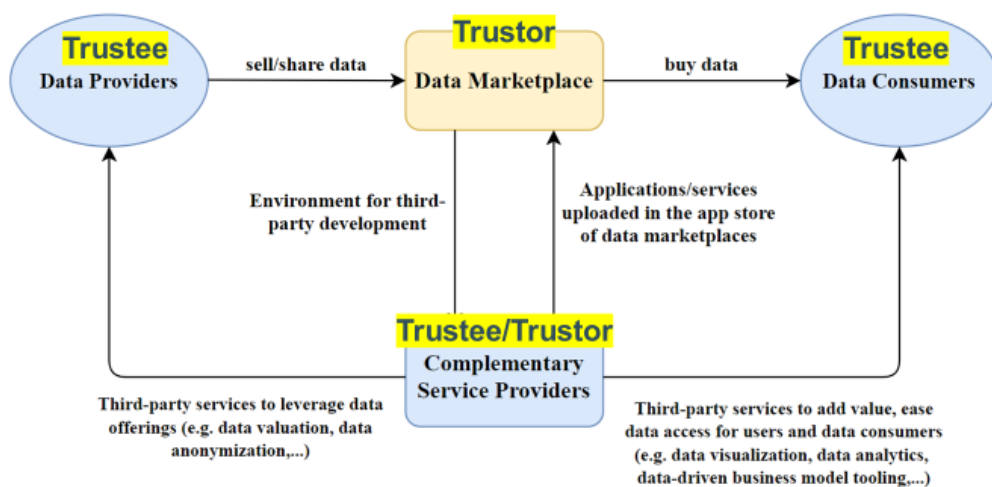
1. Organizational change
2. Knowledge-sharing
3. Less internal conflicts

Safe-DEED

Organizational Trust in Data Marketplaces

Safe-DEED

Organizational Trust in Data Marketplaces



Safe-DEED

Antecedents of Trust in Data Marketplaces

1. Organizational Identification
2. Integrity
3. Communication
4. Asset Specificity
5. Sector Stability
6. Trust Repair

Safe-DEED

Fostering trust in data marketplaces

Safe-DEED

Fostering Trust in Data Marketplaces



Safe-DEED

Chapter 8. Secure Multi-Party Computation

KU LEUVEN

Lecture 8: Secure Multi-Party Computation (MPC)

Safe-DEED

Encryption

‘the process of converting information or data into a code, especially to prevent unauthorized access’

e.g. Secure Multi-Party Computation (MPC)

Why is encryption necessary to ensure security and privacy?

ENISA Opinion Paper on Encryption

ENISA = European Union Agency for Network and Information Security

1. Mere judicial oversight insufficient
2. Technology usually beats legislation
3. Technical innovation is hard to restrict
4. Limiting encryption inhibits innovation

EU Report 'Towards an Effective and Genuine Security Union'

Balancing act between citizens' interest & public security

Need for:

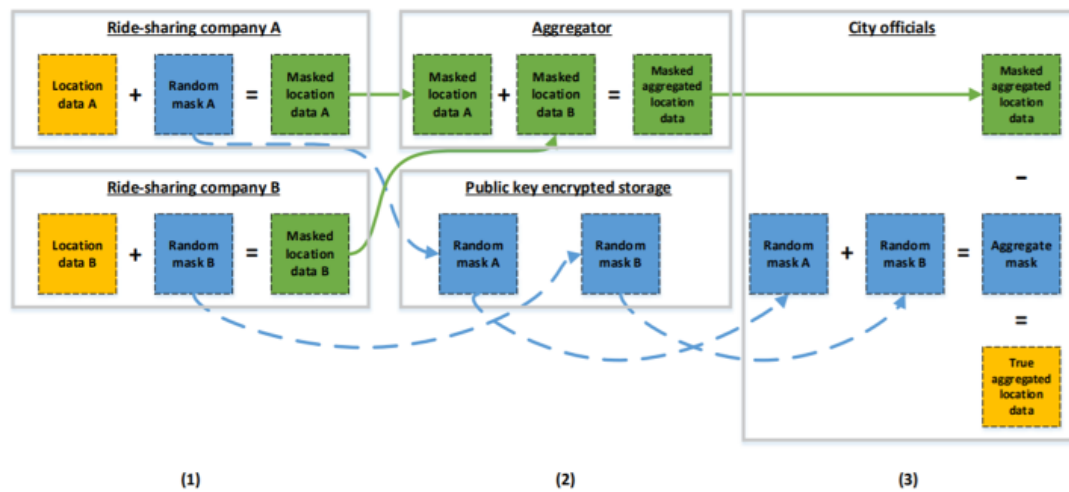
1. Legal measures to facilitate access to encrypted evidence
2. Technical measures to enhance decryption capabilities

**European Electronic
Communications Code (EECC)**

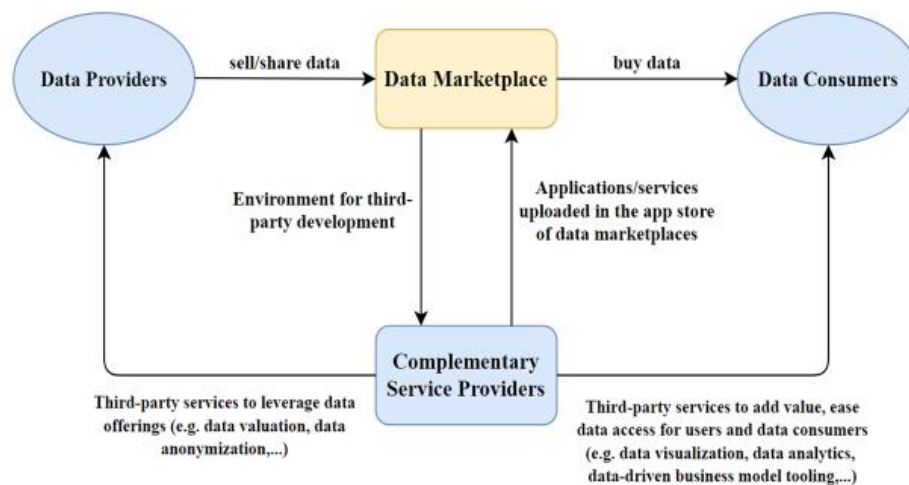
End-to-end encryption (E2EE)

**Secure Multi-Party
Computation (MPC)**

Secure Multi-Party Computation (MPC)



Secure Multi-Party Computation (MPC)



Chapter 9. Secure Multi-Party Computation: Legal Q&A

KU LEUVEN

Lecture 9: MPC Encryption, legal Q&A

Safe-DEED

Legal questions arising in
the data marketplace context

Safe-DEED

First legal issue: How can a data provider/user know that an MPC protocol is trustworthy?

Trustworthiness =
transparency + coherence

Safe-DEED

First legal issue: How can a data provider/user know that an MPC protocol is trustworthy?

Trustworthiness =
transparency + coherence

→ GDPR

Safe-DEED

Second Legal Issue: Assurance of Non-Identifiability

→ GDPR

Safe-DEED

Third Legal Issue: Is there a certification process for the MPC implementation?

EU Cybersecurity Act Regulation:
Certification schemes for IT products, IT
services and IT processes

1. Encryption is an IT service
2. Encryption is part of ENISA's goals

→ It can be expected that certification
schemes will apply to MPC encryption

Safe-DEED