Grant Agreement Number: 825225

Safe-DEED

www.safe-deed.eu

D3.4 Ethical and Normative Valuation in Data Markets

Deliverable number	*D3.4*
Dissemination level	***Public***
Delivery date	*19 Novemeber 2020*
Status	*Final*
Author(s)	*Alessandro Bruni, Noémie Krack, Dieter Decraene, Emre Bayamlıoğlu*

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

Changes Summary

Date	Author	Summary	Version
02/11/2020	**Alessandro Bruni, Noémie Krack**	First draft	0.1
03/11/2020	**Dieter Decraene**	Internal Review	0.2
06/11/2020	**Emre Bayamlıoğlu**	Internal Review	0.3
16/11/2020	**Gert Breitfuss**	Consortium Review	0.4
18/11/2020	**Lukas Helminger**	Consortium Review	0.5
19/11/2020	**Alessandro Bruni, Noémie Krack**	Final Version	1.0

Executive summary

This deliverable D3.4 explores the emerging body of literature on impact assessments in the digital realm. Moving forward from the structure of the Data Protection Impact Assessment, (DPIA) D3.4 explores the potential benefits that might arise from an assessment that takes into account not only privacy and data protection normative aspects, but also ethical values and social norms that are usually not considered in a DPIA. As a result, the deliverable aims to move forward from a Data Protection Impact Assessment to a more comprehensive Data Valuation Impact Assessment.

To create a DPIA, deliverable D3.4 surveys relevant literature, legislative initiatives, as well as a body of literature investigating the value of data, with a specific emphasis on the values such data have in a data-market context.

Carrying out a Data Value Impact Assessment (DVIA) is a burdensome activity. Taking into account the comprehensive approach such analysis requires, any company developing such an analysis will have to devote a significant amount of time and resources to conclude the assessment. Nonetheless, there are numerous positive economic outcomes that should convince companies in embracing such an approach.

First, a DVIA considering ethical, normative and social instances will allow a more close alignment between companies procedures and those factors considered by judicial and administrative authorities when assessing a certain data processing activity. For example, the judicial process takes into account ethical and societal aspects when assessing compliance with privacy and data protection principles. Knowing which are the societal and legal criteria considered by the Court to assess the fairness and legitimate purpose of a certain activity might result in having a beneficial economic effect within a company. Second, knowing entity exchanging data in a data-market had to carry out a DVIA might represent attractive factor for entities interested in joining the data-market, enhancing economic positive outcomes as a result of their overall compliance with legal and ethical norms and principles.

Table of Contents

Executive summary **3**

1 Introduction **7**

2 Deliverable Structure **7**

3 Data Protection Impact Assessment **8**

3.1 What is a Data Protection Impact Assessment **8**

3.3 DPIA Process **10**

4 From a Data Protection Impact Assessment to a Data Protection Value Assessment **13**

4.1 Non-economic considerations of data valuation **13**

4.2 The problem in assessing values in data-market context **14**

4.3 Context base outcomes from surveys and empirical studies on the evaluation of data by individuals **16**

4.4 Data Ownership **17**

4.5 Property law 18

4.5.1 Intellectual Property law and Copyright 18

4.5.2 Legal regimes related to Intellectual Property 19

Trade Secret Directive 19

Database Directive 19

4.5.3 European Data Protection Framework 20

4.6 Moving forward from the economic approach **21**

4.7 Remaining open questions **23**

5 Safe-DEED Data Protection Value Impact Assessment **24**

5.1 Context **24**

5.1.1 Economic Consideration 24

5.1.2 Legislative Considerations 26

5.1.3 Normative and Ethical Considerations 26

5.2 Fundamental Rights and Values **28**

5.2.1 Normative, Ethical and Social Values 28

5.2.1.1 Legal Values 28

5.2.1.2 Ethical and social values 29

5.2.1.3 Economic Values 30

5.3 Risks **30**

5.3.1 Normative, Ethical and Social Risks 31

5.3.2 Economic Risks 32

5.4 Mitigation Measures **32**

5.4.1 Safe-DEED approach: The use of Multi-Party-Computation 32

5.4.2 Safe-DEED approach in practice: COVID-19 use case 33
5.4.2.1 Context 33
5.4.2.2 Fundamental Rights 34
5.4.2.3 Risks 35
5.4.2.4 Mitigation Measures: Use of Cryptography Protocols 37
6 Conclusion 38
References 40
Legislation 40
Jurisprudence 41
Other documents 41
EU Bodies and Agencies 41
OECD 41
European Commission 41
Academia 42
Others 45

List of Figures

Figure 1: WP29: Guidelines on Data Protection Impact Assessment.....10
Figure 2: WP29: When a DPIA should be carried out.....11
Figure 3: Estimate of Value of Personal data by OECD.....16
Figure 4: Details regarding EC projections on the EU Data Market Value 25

1 Introduction

Assessing and evaluating the "value of data" and in particular personal data is a challenging exercise. Economists, politicians and academics have been developing multiple theories to overcome such difficulties. Yet, methodologies and protocols to assess have not provided comprehensive and agreeable solutions. In this deliverable KUL supporting latest initiatives developed by multiple academics have attempted to provide its contribution to the discussion.

Moving from the structure of the EU Data Protection Impact Assessment, the deliverable describes how to enrich such an assessment to take into account elements that are usually not considered in such an assessment. As a result of such theoretical exercise, the deliverable provides a real use-case where such protocol is implanted. To achieve such an ambitious goal, specific attention is paid to Multi-Party Computational protocols, already used in the Safe-DEED context.

2 Deliverable Structure

D3.4 is divided into three main parts.

The *first part* (section 5) summarises (1) key aspects related to data protection impact assessment, (2) its structure and evolution.

The *second part* (section 6) presents crucial factors limiting the possibility to assess in a unique manner an economic value to data. Consequently, the *third part* (section 7) offers a possible solution to overcome some of the challenges highlighted in the previous sections. The described approach, foreseeing the development of a DVIA intends to support both businesses and consumer activities when processing personal data.

To substantiate the approach, the last part of section 7 provides an overview of a concrete use-case where the described data value assessment approach is put into practice.

3 Data Protection Impact Assessment

In 2018, the General Data Protection Regulation[1] (hereafter the GDPR) replaced the Data Protection Directive 95/46[2] and brought important changes to the European data protection regime. The Data Protection Impact Assessment (hereafter DPIA) is one of the novelties introduced by the GDPR. The rapid evolution of technology came along with an increase of risk for violation of data protection rights. This, combined with the Directive's reactive approach led *'to poor compliance practices and data losses as recurring problems'*.[3] Willing to remedy these issues, the EU policymakers decided to revise the Directive to provide more effective protection of personal data in practice thanks to a shift towards more accountability.[4] The data protection principles present in the Data Protection Directive remain valid and relevant. However, measures and mechanisms were adapted and adopted for a better application of the data protection principles.[5] The new legal dispositions promote an ex-ante analysis of the risks in relation to data processing.

3.1 What is a Data Protection Impact Assessment

According to Art. 35 GDPR, when data processing operations are *'likely to result in a **high risk** to the rights and freedoms of natural persons'*, a DPIA must be conducted by the controller **prior to such processing**.[6] This new legal obligation operates a shift from a reactive data protection approach to a preventive and pro-active approach.[7] It is therefore connected to the privacy by default and by design obligation (Art. 25 GDPR).[8] The importance of DPIA for entities processing data is significant when

1 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

2 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

3 Demetzou Katerina, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of 'High Risk' in the General Data Protection Regulation' (2019) 35 Computer Law and Security Review 105342., p.14.

4 The accountability principle requires that the entity processing the personal data are able to demonstrate its compliance with all the GDPR principles. It has been characterized as one of the most remarkable innovations of the GDPR. See European Data Protection Supervisor (hereafter EDPAS), 'Opinion 3/2015 (with Addendum) Europe's Big Opportunity - EDPS Recommendations on the EU's Options for data protection reform', 27 July 2015 (updated with addendum, 9 October 2015), 3.

5 (Article 29 Working Party 2016, p.6).

6 Art. 35(1) GDPR : *'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.'.*

7 (Demetzou, 2019), p.3.

8 Art. 25(1) GDPR: *'1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'*

we look at the broad scope of the GDPR (especially territorial: Art. 3 GDPR) and the potential heavy fines incurred (Art. 83(4) GDPR). Controllers are legally responsible for conducting the DPIA even if the assessment may be done by someone else, inside or outside the organisation.[9]

Substantiating Art. 35 of the GDPR, the Article 29 Working Party (hereafter WP29)[10] has provided guidelines for carrying out a DPIA. According to WP29 a DPIA is *'a process designed to **describe the processing**, **assess the necessity and proportionality of a processing** and to **help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data** (by assessing them and determining the measures to address them). DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation'*.[11]

DPIA forces the controller to take into account the GDPR principles and obligations at an **early development stage**. Following the assessment, the issues considered as high risk would have to be documented, solved or mitigated.

Somehow, shadow zones remain concerning the exact scope of DPIA. Scholars defend different interpretations, on the one hand, a narrow interpretation under which the obligation could be seen as a legal compliance checklist.[12] On the other hand, a broad interpretation according to which a thorough, real and meaningful assessment must be conducted of the processing impact for individuals' rights and freedoms.(Yordanov, 2017) This last interpretation would mean that we should take into account the Charter of Fundamental Rights of the European Union (hereafter ECFR). More and more scholars argue that to comply with the spirit of the law, the DPIA assessment of the risk should be broad.[13]

9 Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purpose of Regulation 2016/679, April 2017, p.13.

10 Article 29 Working Party is the predecessor of the European Data Protection Board (EDPB).

11 Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purpose of Regulation 2016/679, April 2017.

12 (Wright and de Hert, 2012)

13 (Yordanov, 2017), p.495.

3.3 DPIA Process

There are ten foreseen steps for conducting DPIA.[14] These steps are broken down below. The purpose is to help structure and guide the assessment as well as the documentation to provide for this GDPR obligation.

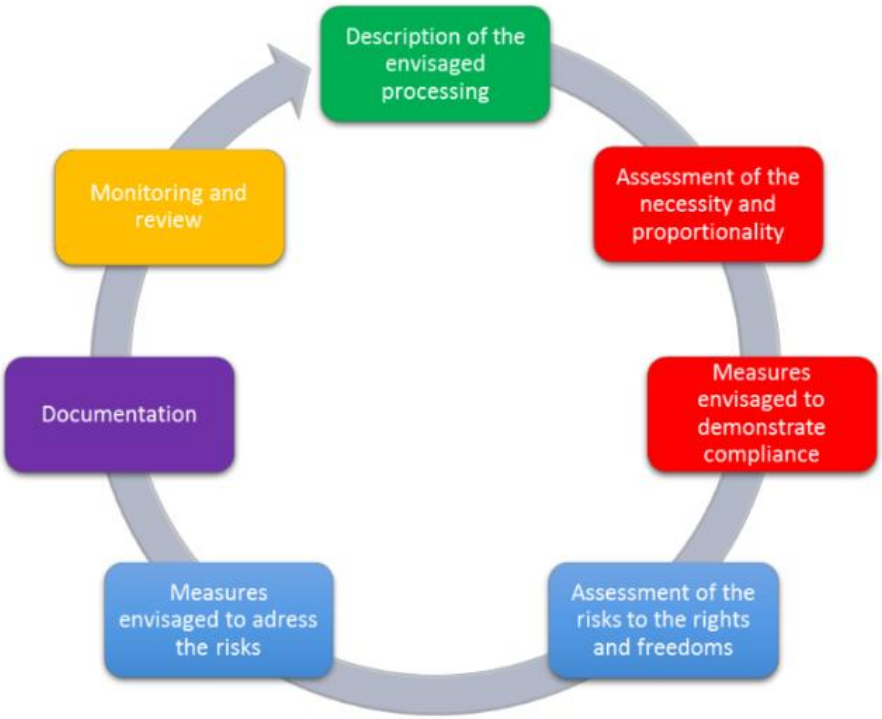

Figure 1: WP29: Guidelines on Data Protection Impact Assessment[15]

1. Assessing the necessity of a DPIA

Conducting a DPIA is not mandatory for all data processing activities. It must occur only when they are likely to result in a **high risk** to the rights and freedoms of natural persons. Consequently, the first step is to conduct a triple assessment: risk identification, likelihood and severity analysis.[16] This evaluation conducted must be objective,[17] and the conclusions drawn by the controller should be *'reliable, verifiable, trustworthy and contestable'*[18].

However, the GDPR does not provide objective and shared legal criteria for the notion of high risk. Due to the lack of a common definition and understanding on the concept of legal risk in the EU data

14 The different steps are based on the work of A Yordanov.

15 Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purpose of Regulation 2016/679, April 2017

16 Rec. 75 and Art.76 GDPR.

17 Rec. 76 GDPR.

18 (Demetzou, 2019), p.5.

protection law may lead to a variety of approaches taken by controllers and a variety of GDPR implementations.[19]

Some guidance emanates from GDPR recitals which provide a non-exhaustive list of the type of data processing that might create risk for fundamental rights and freedoms.[20] Furthermore, national Data Protection Authorities also can establish a list of processing activities susceptible to triggering a DPIA.[21] However, the opportunity of conducting a DPIA has to be assessed case by case in light of the nature, scope, context and purposes of the processing.[22]

The following figure illustrates the basic principles related to the DPIA in the GDPR:

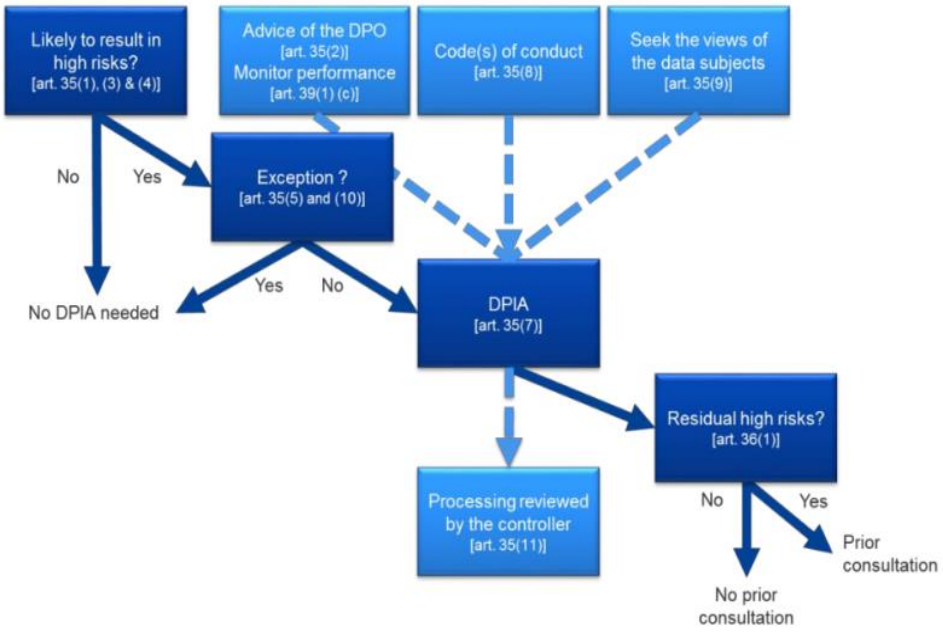

Figure 2: WP29: When a DPIA should be carried out

Conducting a DPIA where not mandatory can be extremely useful; especially regarding the rapid evolution of technology, the assessment could become mandatory following the development of the controller's activities. Furthermore, with a DPIA, the controller has a better knowledge of his activities and can *'make an informed decision regarding the future of the processing activities'*. [23]

2. Description of the data processing – Art. 35 (7)(a) GDPR

The second step is to describe extensively and systematically *'the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the*

19 Centre for Information Policy Leadership, 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR', CIPL GDPR Interpretation and Implementation Project, 21 December 2016, 13.

20 Rec. 75 GDPR, Rec. 89 and 91 combined with Art. 35 (3 which outline by default processing activites presenting high risks.

21 Art. 35(4) GDPR.

22 Art. 35(1) GDPR.

23 (Yordanov, 2017), p.491.

controller'.[24] The description should take into account: the nature, scope, context and purposes of the processing[25], the type of personal data, recipients and period for which the personal data will be stored and recorded, the compliance of the processing with approved codes of conduct[26]. Consequently, it is necessary to provide a functional description of the processing operation and identify the assets on which personal data are stored (hardware, software, networks, people, paper or paper transmission channels).[27]

3. Assessing the necessity and proportionality of the data processing concerning the purposes – Art. 35, (7) (b) GDPR

The DPIA must contain an assessment of the necessity and proportionality of the processing operations with the purposes. The assessor must check if the data processing is necessary and proportional regarding specific GPDR provisions such as Art. 5: principles governing data processing, Art. 6: lawfulness of the processing, chapter III data subjects rights, chapter V safeguards about international transfers,… This step ensures the compliance of the processing with basic GDPR legal requirements.[28]

4. Assessing the risks to the rights and freedoms of data subjects – Art. 35(7)(c)

Assessment of risk represents the DPIA's **cornerstone**. It comprehends the **identification** of every risk for the fundamental rights and freedoms of natural individuals and the **evaluation** of the origin, nature, particularity and severity of that risk while taking into account the scope, the context of the processing.[29] The risk will determine the measures to be taken in the following step.

5. Measures to address the risk – Art. 35, (7)(d)

This step deals with the treatment and mitigation of the risks. Appropriate remedies which would principally eliminate and subsidiarily mitigate the risks should be identified and documented to demonstrate the GDPR compliance of the processing[30][31]

6. Data Protection Officer consultation – Art. 35(2)

This step only applies where the controller has appointed a Data Protection Officer (hereafter DPO). If there is one, he has to be involved throughout the whole DPIA process. It's important to take him on board since the very beginning to enable him to deliver sound advice.[32]

7. Data Subjects consultation – Art. 35(9)

According to Art. 35(9) *'where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing'*. There is no precision in the GDPR regarding the exact interpretation to be given to 'where appropriate'. However, scholars argue that in light of the spirit of the law, it is necessary to consult with data subject after identifying the risk and having designed the

24 Art. 35, (7)(a) GDPR.

25 Rec. 90 GDPR.

26 Art. 35(8) GDPR.

27 Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purpose of Regulation 2016/679, April 2017, p.21.

28 (Yordanov, 2017), p.492.

29 Rec. 84 GDPR.

30 Art. 35, (7, d): 'the assessment should contain at least (…)the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.'

31 (Yordanov, 2017), p.493.

32 (Yordanov, 2017), p. 493.

measures to solve or mitigate such risks. [33] With this approach, the controller also ensures his compliance with the transparency principle.[34]

8. Supervisory Authority consultation

According to Art. 36 GDPR, *'the controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Art. 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk'*.[35]

9. Documentation obligation

Not explicitly stated in Art. 35 GDPR, the controller should demonstrate he is aware of his DPIA obligation. Consequently, the data controller has to provide a clear description of the risks, explanation of the measures and their implementation plan. The best is to draft a report concerning the DPIA.

10. Monitoring and review

Art. 35(11) GDPR provides that where necessary, the controller shall carry out a review evaluating if the processing is performed following the DPIA at least when there is a change of the risk presented by the processing operations. Here again, 'where necessary' is not further defined in the GDPR, however, to be fully compliant a revision is more than necessary to assess if the measures taken based on the DPIA are still fit for purpose.[36]

To conclude, the DPIA has filled a gap in the previous data protection regime by setting up a legal obligation to take into account the potential risks for fundamental rights and freedoms of natural persons linked to the processing activities. However, this instrument can appear not to be fully adapted when it comes to data markets and data valuation.

4 From a Data Protection Impact Assessment to a Data Protection Value Assessment

4.1 Non-economic considerations of data valuation

Before we answer questions regarding what is the value of data, we need a proper understanding of what is "data value". While it is clear that data generates value, the mechanisms in which this happens are still very much unclear. A tentative definition by Short and Todd[37] refers to the value of data as the composite between the value of the asset itself, the value resulting from its use and its expected or future value.

33 (Yordanov, 2017), p. 493.

34 Art. 5, (1, a) GDPR: 'Personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')'.

35 Art. 36 GDPR

36 (Yordanov, 2017), p.494.

37 Short, J.E., and Todd, S. What's Your Data Worth? MIT Sloan Management Review. Retrieved October 24, 2019 from https://sloanreview.mit.edu/article/whats-your-data-worth/, acessed 09/11/2020

According to our colleagues from EUT (WP4), a practical definition of data value refers to four elements (see Deliverable 4.3):

i. the dependency on the context in which data is used,

ii. the qualitative assessment of data (both intrinsic and contextual),

iii. the performance/usability of data given its purpose, as stated in the context and

iv. a method for aggregating or reporting on the value of data, such that the result is actionable.

This view is distilled in their approach to implementing a Data Valuation Component, which is part of deliverables 4.2 and 4.4.

Attempts to put a price tag on data up have failed thus far, since analogies with either tangible (oil) or intangible assets (patents, intellectual property) break at the point where the mapping between features and assigned value becomes less clear. And perhaps this is normal, since rules that apply to old commodities possibly don't even apply to this new kind of resource.

Slotin notes that the difficulty of assessing data comes from its comparison to intangible assets. She argues that data are also in the part public good, which shouldn't have a market price.[38] Data are also non-rival, meaning that the use and value it has to one stakeholder may be different from that of another. The author's review of approaches to establish the value of data points to the efficiency of impact based approaches – as opposed to cost, market or income-based approaches – to deliver the point through narratives that stress the human impact of data and connect to the context of the valuation. Making a similar point, Spiekermann et al. observe that personal data are akin to *'free commons: non-rival, cheap to produce, cheap to copy, cheap to distribute'*.[39]

4.2 The problem in assessing values in data-market context

The massive use of data in the form of big data have resulted in an extensive use of personal data, now considered an extremely valuable asset for a multitude of stakeholders. Together with the traditional players such as companies, governments and organisations, also new players such as data brokers (i.e. Acxiom) have arisen. Due to the difficulties in mapping the number of actors whose activities touch upon the processing of personal data, it is difficult to have a clear understanding of the global dimension of the economic value of data markets.[40] 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. Therefore, KUL has performed an investigation to understand whether or not values other than economic ones should be taken into account when developing a specific technological solution.[41]

38 Slotin, J. (2018): What Do We Know About the Value of Data? Global Partnership for Sustainable Development Data. Retrieved from http://www.data4sdgs.org/sites/default/files/services_files/Value%20of%20Data%20Report_Final_compressed_0.pdf, accessed 09/11/2020

39 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.

40 Angwin J. Online tracking ramps up e popularity of user-tailored advertising fuels data gathering on browsing habits. Wall Str J June 18 2012:B1. See also (Spiekermann *et al.*, 2016)

41 (OECD, 2013)

Due to the characteristics of personal data, all analysed authors tackling the value of personal data agree on the necessity to apply a context-specific approach to any evaluation of data. According to multiple surveys and academics, the context where data processed activities take place, is crucial to determine actors, data exchanged, and consequently, values shared. As stressed by Acquisti et al. *'Depending on context and conditions, privacy can either increase or decrease individual as well as societal welfare'*.[42]

In a scenario where consumers and businesses interact with each other, we should primarily assess first of all, which are the characteristics of such a relationship and subsequently, which are the values that lead such interactions. The main reason that 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. personalised service), but also psychological (reduced time to find goods, or services that might meet our interest).[43]

Together with the benefits for a consumer there are multiple drawbacks that might result from such exchanges. Individuals disadvantages resulting from lack of knowledge about the use of their data by an indefinite number of private entities might be economic, ethical (i.e. discrimination) and societal (i.e. surveillance). A significant unbalance characterises the relationship between businesses and individuals in terms of information asymmetries.

In the Business-to-Business (B2B) data markets context, we differentiate two macro-levels of interactions and actors involved. The first level of interaction involves businesses and individuals. The second is instead characterised by interactions between firms, overseen or not by a third independent entity. Consequently, interactions between (i.e. data collections) individuals and private entities offering services require additional analysis due to the interplay between individual evaluation of data and business/market evaluation of the same data.[44] The two-level of data exchange characterising the B2B data-market has a detrimental effect on data subjects. The absence of individuals from the data market level where their data are exchanged between businesses hamper individuals from having a better understanding about the economic valuation of their personal data.[45]

Regardless of the effort of policymakers across the globe to reduce asymmetries between customers and vendors processing their data, such discrepancy still exist. The businesses themselves might introduce a potential mitigation measure to reduce such gap. To overcome tangible difficulties individuals encounter in assessing a fair value to their data, a proactive approach is necessary on the side of the entities engaged in the personal data processing activities. As stressed by Spiekermann, *'users need to be forced to actively engage with the settings of their agents and browsers'*.[46] Entities sharing personal data with other private entities need to have already processed individuals' personal data. Therefore, to demonstrate proactive approach in complying with normative, ethical and societal principles and values,

42 (Acquisti, Taylor and Wagman, 2016) See also Taylor, C. and L. Wagman (2014). Consumer privacy in oligopolistic markets: Winners, losers, and welfare. International Journal of Industrial Organization 34, 80-84.

43 (Acquisti, Taylor and Wagman, 2016)

44 (Acquisti, Taylor and Wagman, 2016)

45 (Acquisti, Taylor and Wagman, 2016)

46 (Spiekermann and Korunovska, 2017)

businesses aiming to participate in a data-market should list down such requirements in a code of conduct. Such business self-regulatory instrument should be then used as precondition to participate in a data market participatory data market platform.

To conclude, notwithstanding the effort of policymakers, due to the lack of knowledge individuals have in regard to the purpose and process undergoing, it is difficult to reduce the existing level of asymmetries between consumers and the entities managing data. In addition, the intangible and subjective perception affecting individuals when assessing a specific economic value to their data makes it difficult for them to assign a proper value to their personal data. The broader perspective offered by an assessment focusing on fundamental rights helps to consider and evaluate at the same time social groups principles such those enshrined in Chapter IV of the European Charter of Fundamental Rights (i.e. Art.31 on fair and just working conditions).

4.3 Context base outcomes from surveys and empirical studies on the evaluation of data by individuals

One of the main challenges economists are facing concerns the economic valuation of personal data. Such a challenge is related not only to the value businesses assign to data but also the value assigned by individuals to their data. Different methodologies and approaches have been used and considered. According to the OECD,[47] five main methods have been developed to assess the economic value of personal data. On the one hand, from a business perspective, to assess the economic value of data we analyse four main methodologies have been used. The first method focuses on the market cap and revenues of companies that base their business model on the processing of personal data (i.e. Facebook). Another approach analyses the market prices assigned by data brokers to personal datasets. A third approach considers the cost of data breaches, while a fourth one assesses the price specific sets of personal data on the illegal market (credit cards' details). Contrary, the methodologies used to measure the value individuals give to their data consist of surveys' outcomes and individuals' willingness to pay to protect their data.[48]

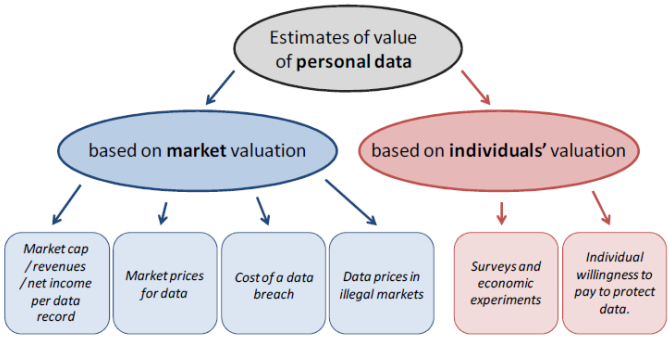

Figure 3: Estimate of Value of Personal data by OECD

[47] The Organisation for Economic Co-operation and Development is an international economic organisation established in the 1961 and based in Paris to stimulate economic progress across the globe. The forum develops studies comparing policy experiences, and aimed to provide policy solutions to common problems, with the identification of good practices.

48 (OECD, 2013)

Unfortunately, none of these methodologies is per se bias-free: each one of the listed approaches has benefits and drawbacks. When it comes to the individuals' indicators, it is possible to highlight two main drawbacks. Due to the strict context-dependent evaluation of their data (i.e. financial, health), it is not possible to detect clear trends in the individuals' economic assessment of their own personal data. Besides, individuals' willingness to protect their data is not an unambiguous factor. According to economists like Acquisti[49] and OECD researchers, two factors determine the inconsistency and consequent failure of the measuring features.

First, there is a proven inconsistency between what people state in regard to their own personal data and their behaviour when it comes to exchanging such data (so-called privacy paradox).[50] Second, there is a clear differentiation in the surveys analysed[51] between the value people give to their data (value of personal data) and the one resulting from the price they are willing to pay for services designed to protect their privacy (value of privacy).[52] As a result, surveys carried out focus on the individual economic assessment have proven shown inconsistency when it comes to which personal data are more valuable for individuals (data of birth and address vs financial data).[53]

Considering this, a parallel approach that considers not only the economic dimension of personal data but also the ethical, societal and normative one, is necessary.

4.4 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 the desirability of its ownership.[54] 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. Today, in practice, we see that there is a de facto data ownership functioning through the physical control over data and the conclusion of contracts.[55] Such a situation has raised the question about the necessity to establish a data ownership right. While, the scarcity of the resources has historically legitimised ownership, nowadays, we see an increasing plethora of data. Therefore, some -such as the Max Planck Institute- have strongly advocated against the introduction of such a right.[56] The Institute reported that introducing data ownership was not necessary nor justified and risked creating chilling effects and legal uncertainties.[57] But could this de facto ownership be replaced by some form of legal ownership? Several elements contribute to 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 the discussion on data ownership might influence data exchanges and data valuation assessment.

Firstly, 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;

49 (Acquisti, Taylor and Wagman, 2016)

50 (Spiekermann and Korunovska, 2017)

51 (OECD, 2013; Spiekermann and Korunovska, 2017; Péga, 2019)

52 (OECD, 2013)

53 (OECD, 2013)

54 (Janeček, 2018), p.13.

55 Kkect Swinnen, 'Ownership of Data : Four Recommendations for Future Research' (2020) 5 Journal of Law, Property and Society 139., p.140

56 (Drexl *et al.*, 2017)

57 (Drexl *et al.*, 2017)

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 entirely, impose conditions or fees for access and use.[58] From an industry perspective, ownership in data would protect the investments carried out in the collection/selection of data. Still, from an individuals' perspective, ownership will improve the control over their data from unauthorised collection and use[59] and stimulate competition.[60] The dilemma between private and public interests is also tangible. Additionally, data ownership raises ethical considerations in light of the personal data commodification debate.[61]

Data ownership is strictly linked to compet´ition law as ownership can create monopolies and affect the public interest and individuals' fundamental rights.[62] Parallelly, some alternative vision for data markets starts developing, such as the commons theory.[63] 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.[64]

Secondly, scholarly research on data ownership indicates that there is **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 areas of law which do not simplify the already complex ownership debate.[65] Ownership could be envisaged under a different area of law such as property, intellectual property and data protection.

4.5 Property law

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.[66] 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.[67] These are complex elements to adapt and match with the different national data frameworks.

4.5.1 Intellectual Property law and Copyright

The intellectual property 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

58 (Scassa, 2020), p.2.
59 (Scassa, 2020), p.13.
60 (Malgieri, 2016), p.10.
61 (Malgieri, 2016)
62 (Scassa, 2020)
63 (Fia, 2020), published online 22 September 2020.
64 (Benkler, 2014)
65 (Swinnen, 2020), p.146.
66 (Janeček, 2018), p.4.
67 (van Erp, 2017)

characteristics of the creation, it will be protected under different regimes: copyright (literary and artistic works), trademarks (distinctive sign), patent (inventions), design,…

Copyright protects the original expression of an idea. The definition of data is still debated, and the legislative initiatives developed at 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 protect *'the mere fact that someone has somehow contributed to the creation of digital data but this would have nothing to do with the original purpose of IP law'*.[68] 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.

4.5.2 Legal regimes related to Intellectual Property

Trade Secret Directive

The trade secret Directive[69], does not create an erga omnes right, but provides some useful protective elements for the data-driven economy.[70] According to the trade secret definition[71], 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.[72]

Database Directive

The Database Directive[73] 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 the collection of data.[74] Nevertheless, after some years into force, some argue that this specific IP right is already outdated.[75] 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.[76]

68 (Swinnen, 2020), p.151-152.

69 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.

70 (Drexl *et al.*, 2017), p.6.

71 Art. 2(1) Trade Secret Directive*:'trade secret means information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret'*.

72 (Drexl *et al.*, 2017), p.7.

73 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.

74 (Scassa, 2020), p.7.; (Malgieri, 2016), p.3

75 (Swinnen, 2020), p.153.

76 (Drexl *et al.*, 2017), p.4.

4.5.3 European Data Protection Framework

One may think that natural individuals own their personal data thanks to European data protection framework and especially thanks to the GDPR. Indeed, the GDPR was designed to give individuals a degree of control over their personal data.[77] 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. They constitute at their best a 'quasi ownership regime'.[78]

Thirdly, **providing an exact definition of data is complex**. Even if we have a definition of personal data[79], the line between personal and non-personal data is hard to trace, due to technological innovation.[80] Here again, we see some shadow zones and discussion about which type of data would be exactly covered by this data ownership regime.[81] The retention of intrinsic personal data could constitute a violation of the right to privacy (Art. 8 ECHR and Art. 7 ECFR).[82] But once personal data are anonymised, could they fall in the ownership regime? Locating the foci of data ownership will be challenging due to the dynamic characteristics of data: non-rival, easily reusable, easily sharable, and extremely volatile.[83]

Fourthly, these theories of data ownership raise some **risks and practical difficulties linked to the unclarity of the debate.**
Case-law helps interpret legislation and legal concepts but is dependent on the cases brought to its attention. However, in a rapidly evolving data economy, the legal uncertainties related to data ownership cases submitted to court are business cases, which will only expand a certain angle of the data ownership question.[84] Public interest in access and use of the data risks to be overlooked.

The ownership question often raises conflicting fundamental rights questions. 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.[85]
Furthermore, access and use of data are increasingly perceived as a crucial enabler for transparency, innovation, knowledge, accountability, expression and privacy compliant.[86] Therefore, developing and establishing a legal regime for data ownership is sensitive and may not be the path chosen by the policymakers for the years to come.

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

77 (Scassa, 2020), p.7.

78 (Scassa, 2020), p.13.; (Malgieri, 2016), p.6.

79 Art. 4(1) GDPR : 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

80 (Janeček, 2018), p.

81 (Swinnen, 2020), p.156 Authors often use interchangeably the following terms : data, digital data, data carriers, data files. Even if such terms refer to different realities.

82 (Janeček, 2018), p.14

83 (Scassa, 2020)

84 (Scassa, 2019)

85 (Scassa, 2020), p. 15.

86 (Scassa, 2020), p.3.

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.[87] 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.[88]

4.6 Moving forward from the economic approach

Due to the existing asymmetries between entities processing personal data and customers providing such data, policymakers across the globe have started developing legislative initiatives to empower citizens and give them access to *'the wealth'* created by Big Data. [89]

Concrete examples of such an approach are provided in the GDPR. For example, the data portability principle, embedded in Rec. 68 and Art. 20 GDPR[90], allows data subjects to take advantages by commercial offer and services of companies other than the one that has processed their data. 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.[91]

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. In particular, the methodology used in a traditional DPIA for assessing the impact on certain processing activities on the fundamental right of privacy and data protection does not seem to address all potential impact such activities might have on fundamental rights, collective societal issues and individual ethical values. Therefore, an approach that takes into account possible consequences beyond the ones related to security and data quality might help to overcome the potential negative impact on a variety of different

87 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Comittee 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-data-19feb2020_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

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

89 (Custers and Uršič, 2016)

90 Art.20 GDPR: *'The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to 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: the processing is based on consent pursuant to point (a) of Art. 6(1) or point (a) of Art. 9(2) or on a contract pursuant to point (b) of Art. 6(1); and the processing is carried out by automated means. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. 1The exercise of the right referred to in paragraph 1 of this Art. shall be without prejudice to Art. 17. 2That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others'.*

91 (Custers and Uršič, 2016)

fundamental rights issues that might also involve businesses (right to run a business).[92] Indeed, according to Mantelero, the methodology foreseen in the GDPR Art. 35 *'focus on the potential adverse effects of data use has not been an explicit element of data protection laws. Many of their provisions adopt a procedural approach that leaves in the shadows the safeguarded interests, which are encapsulated in the broad and general notion of data protection'* for instance, the ethical principle of non-discrimination. Massive data collection and indiscriminate processing of data might determine potential prejudice leading to discriminatory practices both for businesses and consumers. As a result, a comprehensive DVIA, looking at the normative, ethical and societal dimension through an analysis of fundamental rights and freedom might be useful to enhance trust and develop economic models for data-usage activities.

To develop a DVIA, entities involved in the processing activities have to determine which are the values at stake. First of all, they need to define whether the analysis will focus on universal or sector-specific values. In the **Safe-DEED** context, the use-cases developed within the project target different users (consumers vs companies), and different datasets (personal vs non-personal). At the same time, horizontal ethical and normative values are recognisable in both use-cases. Specifically, ethical principles of dignity or societal values of solidarity, inclusion and exclusion are clearly embraced by both data-markets that can be developed by **Forthnet** and **Infineon**. At the same time, legal provisions rising by EU competition law and specifically those on data usage need to be observed in each use-case.[93]

There is a variety of impact assessments developed in different domains (i.e. environmental impact assessment). Before evaluating the benefits of carrying out a DVIA, it is necessary to clarify which are the factors that should be used to measure the outcomes of a certain activity. In our case, societal, ethical and normative factors will help us assess the effects certain processing activities might have to develop adequate safeguards and mitigation measures. The development of a DVIA considering normative, ethical and societal factors might be crucial to demonstrate the goodwill of the entities involved in the data exploitation activities. As a result, a DVIA might provide costumers and individuals with more necessary general information about implications certain activities or process might have on their fundamental rights, helping them to assess the value of their data.

Notwithstanding data subjects' rights and values, it is necessary that such an assessment should also consider the rights and economic prerogatives of those conducting the business. Consequently, a certain level of disclosure regarding their business activities (i.e. algorithms used to value data) needs to be ensured to protect their activity as ensured by European Charter of Human rights and multiple legislative initiatives (i.e. Trade Secrets Directive[94]).[95]

92 (Mantelero, 2018)

93 (Mantelero, 2018)

94 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

95 (Mantelero, 2018)

4.7 Remaining open questions

An analysis of the literature on data quality assessment (one of the contributors to data value) and DVIA reveals that only a handful of these is directly preoccupied with the economic aspects derived from data quality.[96] The rest of them focus either on providing an accurate audit of data quality (DQ), or to effectively employ technical methods to detect and improve DQ.

Despite attempts to move the discussion in the commercial realm – especially through the promotion of data markets – our ever-growing online presence and the reliance of data companies on personal data, means that this domain continues to be a source of debates that go beyond economics.

Legal perspectives related to data ownership are prevalent due to the heterogeneous definitions of personal data in jurisdictions across the world. Considering personal data as part of our identities – *'digital selves'*[97] – raises great ethical questions about the dangers of buying and selling identities.[98] From a technical perspective, these could be solved by applying solutions inspired by digital rights management (DRM), promoting the use of privacy enhancing technologies (PETs), or to leverage 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? Solove et al.[99] believe that the data practices currently promoted by Western societies (aggregation, identification, secondary use) '*completely undermine and breach the notion of privacy'*.[100] Other researchers wonder about 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 *'trade of behavioural futures'*,[101] as Shoshana Zuboff characterises the prediction products developed with such data.[102] She proposes three actions:

1. 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".[103] 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 legislation.[104]

96 Batini, C., Cappiello, C., Francalanci, C., and Maurino, A. (2009). Methodologies for Data Quality Assessment and Improvement. ACM Computing Surveys 41, 3 (July 2009).

97 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

98 Ibid.

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

100 Ibid.

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

102 Ibid.

103 Mason, R. (2014). HMRC to sell taxpayers' financial data. The Guardian. Retrieved October 28, 2020 from https://www.theguardian.com/politics/2014/apr/18/hmrc-to-sell-taxpayers-data, accessed 09/11/2020

104 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/116th-congress/senate-bill/1951/text

2. 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.
3. Give a chance to alternatives. Creating the opportunity for competitive solutions to the currently established actors and supporting their activity if they play by the good rules.

Within **Safe-DEED**, we are focusing our activity on the enhancement of secure and reliable PETs and the creation of self-regulatory instruments to provide data market peers with secure and economically attractive solutions. Within **Safe-DEED**, we believe the foreseen approach would be easily deployable, enabling the creation of competitive solutions for businesses and individuals.

5 Safe-DEED Data Protection Value Impact Assessment

In this section, following the structure of DPIA,[105] we analyse the economic, legal, social and ethical elements that should be taken into account by any entity interested in developing a data-market. Such an approach will permit a comprehensive analysis of all crucial elements that are necessary to be identified and will evaluate the various values at stake.

Safe-DEED project is currently working on enabling technologies for the creation of decentralised data-market platforms. Therefore, notwithstanding general considerations on the data-market context, a tailored analysis for every data market created using tools developed in the **Safe-DEED** context should be performed. Such an assessment should consider the specific context where it is developed, the actors involved, the type of platform such entities want to create and consequently, data and rights and values at stake.

5.1 Context

5.1.1 Economic Consideration

Data is nowadays considered an independent and extremely valuable production factor. In particular, we have seen that such an asset has led to the creation of a brand new ecosystem, where data are exchanged and lead to the creation of other data: data-markets. The European Commission (EC) defines a data market as *'a 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'*.[106]

105 Art. 35(7) GDPR: *'the assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.'*

106 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions 'Building a European Data Economy' COM/2017/9 final, available at < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN>, accessed 27/10/2020.

The exploitation of capabilities of such data markets in different domains (financial, manufacture, health,…) is expected to boost the EU data economy. According to the EC, the exploitation of economic possibilities linked to data will lead to an increase of 530% in the global data volume and will generate within the EU an 829 billion euro value, creating a data supply chain of 10.3 million data professionals.[107]

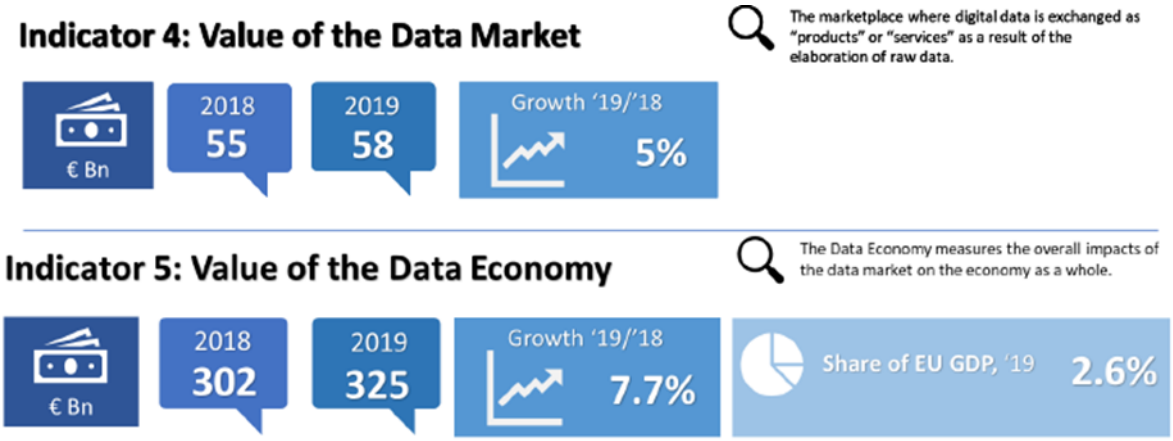

Figure 4: Details regarding EC projections on the EU Data Market Value

To achieve such an ambitious economic goal, crucial aspects need to be addressed. In particular, the new European Data Strategy[108] highlights the necessity to develop a social and economic data governance model enabling a fair and competitive economy.[109] Consequently, in the last years, EU policymakers have started working on developing different legislative initiatives to cover what is right now a patchwork of different legislations. Currently different regulatory approaches come together and legal scholars have started an ongoing discussion on crucial aspects of data markets.

The development of a framework for the data market economy is one crucial pillar of the EU. Digital Single Market, which aims to enhance internet access quality both for businesses and consumers, increase the exchange of goods and services online and as a consequence, boost the EU economy. As pointed out by Zech, these measures aim to *'build-up of a data economy, […] increase competitiveness through interoperability and standardisation and create an inclusive digital society'*.[110]

107 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

108 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

109 Gabriella Cattaneo, Giorgio Micheletti, Mike Glennon, Carla La Croce (IDC) and Chrysoula Mitta, European Commission, The European Data Market monitoring tool, Key facts & Figures, First Policy Conclusions, Data Landscape and Qualified Stories, D2.9 Final Study Report, Directorate-General for Communications Networks, Content and Technology, June 2020, available https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68015, accessed 27/10/2020

110 (Zech, 2016)

5.1.2 Legislative Considerations

The main difficulties for the EU legislator in developing a comprehensive strategy for tackling main regulatory challenges arising from the setup of a data market economy concern the significant implication such field has with national contractual law. As highlighted in the previous section (6.3), data -as intangible goods- are regulated, directly or indirectly by contractual law, which is a field where the national government has exclusive competencies. As a result, liability and other crucial legal issues linked to the data market are not harmonised at EU level. Besides, the EU and national legislators have demonstrated to be frequently reluctant to regulate B2B relationships. Indeed, the only legislative initiatives developed at EU level in such a context, is the Platform to Business regulation. Nonetheless, this regulation only provides transparency and out-of-court solutions for those situations where one of the entities results to have bargaining power on the other, recreating a sort of B2C (business to consumers) relationship.[111]

Data as a '*machine-readable encoded information*'[112] is now a crucial economic asset. Especially when aggregated and processed in the form of big data like in **Safe-DEED**, they can generate significant revenues for the entities involved in the processing value chain. Such a chain can be divided into three macro-groups where multiple actors interact at a different level. We differentiate between the (I) data collection stage, where we distinguish between user-generated data (i.e. online purchase) and business-generated-data, (II)the data processing stage (aggregation of data for extracting economic value), and (III) the result stage, where processed data are used to deliver services or goods. In such a transaction context, main discussion concerns whom has ownership over such data and how such ownership can be turned into legal protection. Unfortunately, as said before, property law, contractual law and liability law represent main pillars of civil law, and consequently, its regulation is massively influenced by the national legislation. In addition, the discussion on data ownership described in section six is far from being concluded. 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, we will focus our normative analysis on these latter aspects, integrating and complementing with a valuation on societal norms and individual ethical values.

5.1.3 Normative and Ethical Considerations

A crucial aspect that should be tackled when it comes to the legal challenges related to the exchange of data and the right to use data concerns the economic evaluation of such data. As pointed out by Zech,[113] 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. 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. 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

111 (Kerber, 2016)

112 H Zech, Information als Schutzgegenstand (Mohr Siebeck 2012), 32.

113 (Zech, 2016)

fundamental rights of the data subject, and ethical principles linked to such data.[114] The European Data Protection Supervisor Authority (EDPS) Ethical Advisory group confirmed such an assumption in its recommendation which clarified that 'Personhood, with his or her moral values and social and cultural characteristics, cannot be taken apart from his or her personal data'.[115]

In such a context, it is useful to point out a crucial legislative initiative, the Directive on the legal protection of databases.[116] Even if such a legislative initiative does not address whole legal issues arising from massive processing and exploitation of data sets, it addresses the legal protection generated by a database. Interestingly, the protection here is not linked on a human right creation like classical copyright, but rather, on the economic effort for setting up such a database. Considering this, we can fairly assume that the same level of protection ensured for an investment to set up and run a database can be translated in the data market context.[117]

Considering such an assumption, it should be stressed that the data market and the activities linked to such a data-driven economic tool embed different activities and frameworks. According to the actors involved and the activities performed different levels of legal protection are enshrined at national and EU level.

Consequently, the current legal scenario in the data market context can be divided into two complementary groups. On the one hand, national civil law and EU legislation on platform, database, trade secrets, competition law address commercial needs of businesses and commercial entities in exchanging and transferring the right to use data. On the other hand, consumer protection law and privacy and data protection law address legal, ethical and societal issues to those actors whose right might be restricted and hampered.

To summarise, data markets challenges are linked to the tension between EU and national legislation and between economic efficiency of those entities relying on data as an economic asset and individual legitimate interest to retain personal information.

The research activity carried out in the **Safe-DEED** context aims to create a technological and legal bridge between businesses and citizens. Developing measures that are not going to hamper individual personal expectations to protect their private life and information and the fundamental rights of

114 Right to access (Art.15 GDPR), Right to rectification (Art. 16 GDPR), The right to erasure of data (Art. 17 GDPR), the right to the restriction of the processing (Art.18 GDPR), right to data portability (Art. 20 GDPR). In Germany the federal court has confirmed such an assumption, stating that 'the individual has no absolute, unrestricted control over its data; because it develops its personality within the social community where information, even if it is personal, is a part of social reality which cannot be exclusively assigned to the person concerned alone.' BGHZ 181, 328 ¼ NJW 2009, 2888, 'www.spickmich.de'.

115 Ethics Advisory Group 2018 Report, Towards a digital ethics. p.13

116 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 077/22, 27 March 1996.

117 (Zech, 2016)

companies to conduct a business, such activity will ensure all actors the protection of the Charter of Fundamental Right of the EU.[118]

5.2 Fundamental Rights and Values

Due to the rapid evolution of technology, there is a need for a broader view of the impact of data processing activities ongoing in the data markets. Assessment models centered on human rights have been acclaimed.[119] They would keep the traditional characteristics of data protection but would go beyond the focus on data quality and security, integrating fundamental rights, collective social and ethical values.

The data protection value assessment would focus on the rights and values affected in each sector rather than the technology used. Such an approach would be based on the experience developed by the GDPR DPIA and should further enhance the integration of fundamental rights and values in the risk evaluation methodology. As a result, a data protection value assessment would address the demands for a uniform regulatory model as well as for a human-centred use of technology.[120] Public Opinion and studies have underlined the *'importance of the social and ethical implications of data processing in the context of data-intensive applications'*.[121]

The DPIA described in the GDPR only provides limited explicit references to fundamental rights and freedoms; therefore, no thorough analysis is uniformly conducted at this stage.[122] However, there is a pressing need to broaden the assessment as potential negative outcomes for data uses are no longer confined to privacy-related risks but encompass a broader range of fundamental rights and values which will be briefly exposed below.

For more substantial information on legal frameworks and ethical issues, we refer you to **Safe-DEED** deliverable 3.1.

5.2.1 Normative, Ethical and Social Values

5.2.1.1 Legal Values

Concerning the study of fundamental rights, we have several fundamental rights protection schemes that share common grounds. For our analysis, we focused on the United Nations Universal Declaration of

118 Art. 16: 'The freedom to conduct a business in accordance with Union law and national laws and practices is recognised.', Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407

119 (Mantelero, 2018), p.757; (Stahl and Wright, 2018)

120 European Commission Communication from the Commission to the European Parliament, the Council, the European Economic and Social Comittee and the Committee of the Regions, Shaping Europe's digital future, COM/2020/67 final, https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

121 (Mantelero, 2018)

122 Art. 35 (1 GDPR: 'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks'.

Human Rights,[123] the European Convention of Human Rights[124] and the Charter of Fundamental Rights of the European Union.[125] The data protection value assessment aims to contain a universal approach without underestimating the local dimension of each case, taking into account those elements that might interfere and hamper fundamental rights stemming from the above-mentioned texts.[126][127]

However, this fundamental rights focus contains some **limitations**. Fundamental rights, being a normative concept, are framed by their legal description and the case-law which has contributed to their interpretation and evolution. The assessment may be stuck in an inflexible legal construct which does not reflect the specificity of the data processing at stake. Fundamental rights and freedoms were built around traditional notions, and they may not fit the new challenges raised by the data economy and data markets.

Furthermore, some data applications, while not being desirable for society, might be legally allowed. An assessment focusing only on fundamental rights would pass by the societal and ethical issues.[128] The massive use of targeting using biometric data based on informed consent would be an illustration of this shortcoming. Therefore, social and ethical values will be necessary to provide a better, balanced and broader assessment. Most fundamental rights and freedoms are framed in individualistic terms even if there are also rights directly or indirectly addressed to groups or collective.[129]

5.2.1.2 Ethical and social values

The ethical and social values are balancing and influencing the assessment of fundamental rights at stake, they will be key for interpreting the rights in their local, temporal or sectoral context. Therefore the values are assessed through the lens of fundamental rights; they serve as interpreters.[130] They permit to enshrine the assessment in a broader contextual picture and address collective concerns from the design stage. Such assessment triggers public debate and should involve all interested stakeholders to have the broader ethical picture possible and to better shape the technology of tomorrow.[131] Technology has considerably shaped today's world, however, we see that technology ethics is still in its infancy.[132]

The European Union primary law explicitly provides that the 'EU is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between

123 United Nations Universal Declaration of Human Rights, 10 December 1948, https://www.un.org/en/universal-declaration-human-rights/

124 European Convention on Human Rights, 4 November 1950, https://www.echr.coe.int/documents/convention_eng.pdf

125 Charter of Fundamental Rights of the European Union, 18 December 2000 and legally biding since the entry into force of the Lisbon Treaty. •Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407, available https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT, last access 03/11/2020

126 (Mantelero, 2018), p. 765.

127 Specific attention has been paid to the right to life, the right to non-discrimination, the right to privacy and data protection, the right to the integrity of the person, the right to education, the right to be equal before the law, the freedom of movement, the freedom of thought, the freedom of expression, and the freedom of assembly.

128 (Mantelero, 2018), p.765.

129 (Mantelero, 2018), p.764.

130 (Mantelero, 2018), p.758-759.

131 (Wright, 2011), p.201.

132 (Wright, 2011), p.203.

women and men prevail'.[133] Other ethical principles that could be used are autonomy (right to liberty), beneficence[134], non-maleficence[135], responsibility, trust, safety, accessibility, value by design, sustainability (economic and social), fairness. Further specific ethical values are applicable for data environment: data minimisation, data quality, purpose specification, use limitation, confidentiality, security, transparency, access to data, anonymity, privacy under different aspects (of personal communications, of the person and personal behaviour).

To illustrate the added value of ethics and social values, algorithms fed by data can create discrimination for a targeted group in an insidious way, which considerably limits the collective perception of this collective issue. The data protection value assessment will permit to lift the veil on these potentials less visible impacts.

The traditional values will be challenged by innovation and need to be assessed in a dynamic framework. This new big data ecosystem generates unprecedented challenges for society and digital opportunities, risks, benefits, and harms will need to be addressed.[136] EDPS underlined how the convergence between law and ethics would allow putting human beings, as well as their experience and dignity at the centre of data deliberation.[137]

5.2.1.3 Economic Values

Data protection value assessment will foster users' informed consent and ensure extensive compliance with the information duty. An informed and freely given consent ensures the perennially of a data processing activity and by extension of a certain business model.

Furthermore, a principle-based model is better designed to deal with the rapid change of technology and will permit to have accurate data protection value assessment.[138] Respecting the flexibility necessary to innovation and technology will only promote a better reconciliation between legal, societal, ethical interest and the economic opportunity of data markets.

5.3 Risks

Assessing risk is crucial to measure the broad value of data and represents, in fact, a critical factor for the DPIA. However, DPIA's risk process does not adequately identify the ethical and social risks for fundamental freedoms and values.[139] The current GDPR approach does not set the potential interests and risks affected on the front of the stage; it focuses on procedural aspects of data protection. Data protection authorities focus their argumentation on procedural criteria such as transparency, data minimisation, storage limitation. Still, these are in the end an indirect expression of the interest

133 Art. 2 of the Treaty on European Union, Preamble of the Charter of Fundamental Rights of the European Union

134 Morality requires that individuals not only restrain from harmin others but actively contribute to their welfare through beneficial actions. (source: Beauchamp, T. L., & Childress, J. F. (2001). Principles of biomedical ethics (5th ed.). New York: Oxford University Press, p.165).

135 The principle asserts an obligation not to inflict harm on others, it requires intentionally refraining from actions that cause harm. (source: Beauchamp, T. L., & Childress, J. F. (2001). Principles of biomedical ethics (5th ed.). New York: Oxford University Press, p.113-115).

136 (EDPS Ethics Advisory Group, 2018), p.16.

137 (EDPS Ethics Advisory Group, 2018)

138 (Mantelero, 2018), p.767.

139 (Cnil, 2018) https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

safeguarded.[140] This value-oriented approach will permit to analyse further the potential adverse risks linked to the above presented fundamental rights and values.

The European Commission favours the integration of the precautionary principle in a structured risk assessment approach in several fields.[141] '*The precautionary principle*[142] *is relevant only in the event of a potential risk, even if this risk cannot be fully demonstrated or quantified or its effects determined because of the insufficiency or inclusive nature of the scientific data'*.[143] The evaluation must identify the costs and benefits of the action or lack of action, and the decision should be compliant with a level of risk that is acceptable to the society on which the risks is imposed.[144] Transparency is also a key feature of the risk assessment; it requires to take all stakeholders on board to detect the risks and their management options.[145]

Conducting such a risk assessment should determine if the foreseen measures are necessary and proportional to the chosen level of protection. Besides, the analysis should assess whether or not such procedures are non-discriminatory in their application, consistent with similar measures already taken, based on an examination of the potential benefits and costs of action or lack of action (fundamental rights and ethical evaluation). Last, the data value assessment should also be able to evaluate whether, in the light of new scientific data, it is possible to produce the scientific evidence necessary for a more comprehensive risk assessment.[146] The last criteria echo one of the essential requirements of GDPR and what we started discussing in this deliverable: the accountability principle. GDPR emphasised it and identifying the responsibilities of each partner involved in the technology development corresponds to the quality of the risk assessment analysis.[147]

Risks are, by definition, indefinite and can occur in various forms. Thus, it would be pointless to list all potential risks that might occur in any data-driven process as they will be highly dependent on the data characteristics and project context. For instance, one of the major risks linked to the nature of technological development is the uncertainty or unanticipated use that could be done of a certain technology, for instance far away from the initially designed use.[148]

5.3.1 Normative, Ethical and Social Risks

The ethical risks of the intensive use of data include a scored society, a convergence between machines and humans, the loss of responsibility through a chain of multiple and distributed responsibility, and –

140 (Porcedda and Adinolfi, 2017)

141 European Commission, Communication on the precautionary principle, COM (2000)1, Brussels, 2 Feb 2000.

142 The precautionary principle was mainly used in environmental law : Art. 191 TFEU, UN Rio Conference of 1992, however, throughout the years this principle has been used in other fields thanks to case-law and multiple policy initiatives. The precautionary principle provides that when there are reasonable grounds for concern that potential hazards may affect the environment or human, animal or plant health, a risks assessment must be conducted which will determine the actions to undertake.

143 European Commission, Communication on the precautionary principle, COM/2000/1 final, Brussels, 2 Feb 2000., p.13.

144 European Commission, Communication on the precautionary principle, COM/2000/1 final, Brussels, 2 Feb 2000., p.15.

145 (Wright, 2011), p.220.

146 European Commission, Communication on the precautionary principle, COM/2000/1 final, Brussels, 2 Feb 2000., p.17-21.

147 (Wright, 2011), p.221.

148 (Sollie, 2007), p.295.

with regard to justice - the risk of a pre-emptive justice. As correctly explained by Mantelero the traditional concern about government surveillance and technology *'has been joined by new concerns regarding the economic exploitation of personal information (risk of unfair or unauthorised uses of personal information and, nowadays, by the increasing number of decision-making processes based on information (risk of discrimination, large-scale social surveillance, and bias in predictive analyses'*.[149]

5.3.2 Economic Risks

Assessing and identifying the risk at the design phase also reduces the failure and commercial flop chances.[150] Taking on board stakeholders enables to identify the flaws before deploying a specific technology correctly. Liability could be limited, and traps could be anticipated and prevented.[151] With a better data valuation model, innovation could better take into account the potential socio-economic impact of new technologies developed.

5.4 Mitigation Measures

5.4.1 Safe-DEED approach: The use of Multi-Party-Computation

According to Safe-DEED partners, the use of multi-party computation (MPC) for exchanging information between data market peers represents 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 activities of data-markets.

As also stressed in Sade-DEED deliverable D2.2 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'*.[152] From a business perspective, the benefit in adopting MPC concerns the possibility such cryptographic protocols give entities to gain insight from data shared and ensures at the same time assurance about the secrecy of the data. MPC ensure data own by a certain business entity will remain secure since no other party would be able to get access to such data. In fact, adoption of such cryptographic protocol allows to gain and provide insights without exchange of data.[153]

From a technical and economic perspective, characteristics and outcomes concerning the adoption of MPC are extensively explained in Safe-DEED deliverable D2.2 and D4.3. In this deliverable we analyse crucial legal and ethical aspects link to MPC. In the upcoming paragraphs crucial aspects arising from the use of MPC and other specific cryptographic protocols are analysed, namely, the legal notions of accessibility and identifiability. Such an investigation should in fact be considered necessary to verify whether or not such measures are compatible with existing EU privacy and data protection framework.

The approach carried out within the **Safe-DEED** context, due to its scalability, can ensure multiple valuable outcomes for businesses and data subjects, creating an overall benefit for society. Proactiveness in providing data subjects with effective safeguards regarding the processing of their data represents -in

149 (Mantelero, 2018), p.761.

150 (Palm and Hansson, 2006), p.547.

151 (Wright, 2011)

152 Mark de Reuver, Wirawan Agahari, Ricardo Dolci, Gert Breitfuss, Michael Fruewirth, Safe-DEED deliverable D2.2 Business models for use cases and generic business models, Safe-DEED Project Grant Agreement Number: 825225

153 Ibid.

the consortium's opinion- a necessary activity to create a bridge between compelling needs (business vs individuals). Such a demonstrable proactive approach towards citizens will contribute to enhancing consumer trust, which should result in an economic opportunity for companies adopting **Safe-DEED**'s protocols.

5.4.2 Safe-DEED approach in practice: COVID-19 use case

In the development of a heat-map for tackling the COVID-pandemic, a DVIA has been carried out to validate the approach described in this deliverable (D3.4). While technical aspects have been described in detail in the WP5 deliverables (D5.8 and D5.9), here (in this deliverable) we have merely described the main considerations that have been taken into account for assessing the impact of such a data-driven technological solution. [154]

Data-driven measures are providing fundamental supports to public authorities in their fight against COVID-19. In such a context, the necessity to carry out a DVIA is necessary considering the implications such solutions have on fundamental rights of those citizens affected, directly (i.e. patients) or indirectly (i.e. citizens living in an area that might result affected by the virus.

The impact foreseen solution will have on the fundamental right of citizens requires an assessment focused on the compliance of the foreseen technological solutions with the relevant fundamental rights, since ensuring compliance of such rights implies also an assessment on social and ethical values.

In the **Safe-DEED** consortium, we believed that a proactive approach by those entities involved in the (implementation) process would represent a precondition to enhance citizens' trust, necessary for an efficient implementation of a protocol to fight COVID-19 pandemic.

5.4.2.1 Context

In the first section of this paragraph (7) we have stressed the necessity to tailor a DPVIA to the context, the actors, their activities, and to the technology used. In our use-case, the protocol developed by TU. Graz and KNOW-Center with the support of KUL has been developed the protocol and showed it officials. So far, there was not a request by anyone to actually deploy the protocol [155] to implement measures considered necessary to tackle the COVID-19 crisis. The protocol foresaw an exchange of encrypted personal data between the Austrian Health Authority on behalf of the Austrian government, and Austrian electronic communication services provider. The exchange of information will be used to develop an interactive 'heat-map' showing area with a significant presence of COVID-19 patients. Specifically, data sets processed by the two entities include data identifying patients affected by COVID-19 virus (i.e. name, surname, telephone number) and patients' mobile location data. The outcomes of the process of such data would give the possibility to the Austrian Health Authority to provide the government with useful information (tailored confinement).

The initial analysis carried out concerned the existence of the principle of effectiveness and proportionality. Each state, while implementing measures that have an impact on fundamental rights, should avoid unjustified compression of the fundamental rights of its citizens.[156] To do so, an assessment

154 (Bruni *et al.*, no date)

155 The Health National Authority is the public entity responsible to enforce policy measures coming from the EU and national government touching upon the health sector.

156 EDPB, 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' (2020)

on the invasiveness of the technological foreseen solutions should aim at balancing through safeguards and mitigation measures, any risk that might be originated by the implementation of the forecasted solutions in similar contexts is recommended.

5.4.2.2 Fundamental Rights

The protocol developed by TU. Graz relies on the exchange of personal data between two distinct entities. Notwithstanding the possibility actors involved and activities carried out might fall into multiple legislative initiatives, the legal analysis focused on the EU privacy and data protection framework and jurisprudence. Therefore, the DVIA on the processing activities carried out by both entities should, first of all, assess the nature of data involved in their activities.

From a legislative perspective two initiatives have been be taken into account: the General Data Protection Regulation (GDPR)[157] and ePrivacy Directive,[158] a lex specialis that exclusively Deals With '*The Processing Of Personal Data In Connection With The Provision Of Publicly Available electronic communication services in public communications networks in the community'.*[159] The GDPR applies to the whole processing of personal, defining principles and key notions such as personal data and processing. On the other hand, the ePrivacy Directive focuses on the specific type of data, generated and exchange through a specific medium, namely, *public communications networks.*

Art. 4 GDPR defines personal data as *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.*[160]

Data processed by the Health Authority and the electronic communication providers fall in the scope of application of the EU privacy and data protection framework. Additional analysis is required for the mobile data hold by the electronic service provider. Due to their characteristic mobile data, these fall within the ePrivacy Directive definition for traffic and location data. According to Art. 2(b) ePrivacy Directive traffic data are *'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;'*. For location data instead, we refer to *'any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.*[161] Due to the sensitivity of such information art. 6 ePrivacy Directive prescribes a specific procedure for such data. Specifically, if the consent of the user was not obtained, such data need to be processed for a specific processing purpose and should be erased or

<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf> accessed 19 October 2020.

157 Regulation (EU) 2016/679 of The European Parliament And Of The Council 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)

158 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), OJ L 201, 31.7.2002, p. 37

159 Ibid.

160 Art.4(1) GDPR

161 Art.2(c) ePrivacy Directive

anonymised straight after such purpose has been achieved. In addition, if stored, access to location and traffic data is only allowed if authorised by the data subject.[162] Notwithstanding such obligations, Art. 15 ePrivacy Directive foresees an exception when *'such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or unauthorised use of the electronic communication system'*.[163] Art. 15 foresees *de facto* a balanced evaluation between the individual and societal interests at stake. On the one hand, Art. 15 foresees an overall protection of data subjects rights and values . On the other hand, same article ensure without the that societal public interests are ensured. Concretely, the assessment carried out by the EU legislator in such context is not restricted to legal considerations but also embraces other evaluations such as the societal and ethical ones. The impossibility in using location or traffic data might determine a detrimental effect on society (spread of the virus). At the same time, such lack of action of public authorities might also configure an infringement to the ethical principle of non-maleficence that prescribes a positive obligation of non inflict harm to others.

Taking into account our analysis' angle, specific attention should be paid to art. 23 GDPR. As stressed by the EDPB in its guidelines, the GDPR forecasts situations where the fundamental right of data protection might be limited if it is necessary to balance compelling fundamental rights. According to art. 23 such restriction can take place *'when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard'*. In our case, these concern the fundamental and absolute right to life, art. 2 of the Charter of Fundamental Rights of the European Union mirroring art. 2 of the European Convention of Human Rights of the Council of Europe.

5.4.2.3 Risks

After having described and analysed critical characteristics of the contexts and actors involved in the use case, through the DVIA has also been verified a concrete list of risks to fundamental rights that might be generated by the specific technology used for gaining value from involved personal data. To achieve such result through a case-by-case approach,[164] it should be, first of all, verified whether it is possible to identify (directly or indirectly) patients using the information available online. As a matter of fact, from a legal perspective, the main risk in the given use case is the possibility that unauthorised third parties can have access to data subjects data (health data, but also mobile data).

The identifiability of data subjects, taking into account the nature of data at stake (health data of patients affected by COVID-19), determines the involvement of different legal but also ethical and societal considerations. The assessment on the cryptographic protocols foreseen for the creation of the COVID-19 heat map aim at verifying whether data sets held by the two involved entities are accessible and consequently identifiable by entities other than the one legitimately processing the data. The analysis on the identifiability is necessary to determine first of all which legal framework applies to the given use case In the EU privacy and data protection context, an assessment on specific cryptographic measures

162 Art.5(3): confidentiality principle

163 Art.15 ePrivacy Directive

164 (EDPB, 2020)

is prodromal to also assess compatibility of such measures, such as differential privacy and MPC with relevant EU data protection framework.

As stressed by Rec. 26 *'the principles of data protection should not apply to anonymous information, namely, information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'*.[165]

Unfortunately, neither the GDPR nor the ePrivacy Directive defines the characteristics of anonymised data. Lack of clear definition of anonymized data has created legal uncertainty and confusion between anonymisation and pseudonymisation.[166] We can, therefore, legally assume that when individuals can be identified by any other party than the data controller, the process involving such data falls into the scope of application of the EU Privacy and Data Protection Framework, imposing specific requirements to those carrying out such activities.[167]

Key elements to assess identifiability have been provided by WP29 [168] and the jurisprudence of the European Court of Justice (CJEU). In a landmark case (Breyer case),[169] the Luxembourg judges had to assess whether or not a dynamic IP address can be considered as personal data. In its decision, the CJEU has clarified which crucial aspects each entity should pay attention to when assessing the identifiability of data subjects. Even if the case was based on the Directive 95/46,[170] now replaced by the GDPR, the same conclusion can be translated to the current framework. According to the CJEU, the identifiability process of personal data by 'any other person' should be related to *'all the information enabling the identification of the data subject must be in the hands of one person'*.[171] The CJEU stressed that the identification of a data subject should be evaluated taking into account *'all the means likely reasonably to be used either by the controller or by any other person to identify the said person'*. [172] To assess the

165 Rec.26 GDPR

166 Art.4(5) GDPR *'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'*.

167 (Bruni *et al.*, no date)

168 Art. 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216' (2014) <http://ec.europa.eu/justice/data-protection/index_en.htm> accessed 22 October 2020.

169 CJEU, *Patrick Breyer v Bundesrepublik Deutschland* [2016] European Court of Justice Case C-582/14, ECLI:EU:C:2016:779 [42]

170 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

OJ L 281, 23.11.1995, p. 31–50

171 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

OJ L 281, 23.11.1995, p. 31–50, paragraph 43

172 *' Just as recital 26 refers not to any means which may be used by the controller (in this case, the provider of services on the Internet), but only to those that it is likely 'reasonably' to use, the legislature must also be understood as referring to 'third parties' who, also in a reasonable manner, may be approached by a controller seeking to obtain additional data for the purpose of identification This will not occur when contact with those third parties is, in fact, very costly in human and economic terms, or practically impossible or prohibited by law. Otherwise, as noted earlier, it would be virtually impossible to discriminate between the various means, since it would always be possible to imagine the hypothetical contingency of a third party who, no matter how inaccessible to the provider of services on the Internet, could — now or in the future — have additional relevant data to assist*

identifiability of a person, the CJEU confirms the Advocate General's approach requiring to check *'if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.'*[173]

5.4.2.4 Mitigation Measures: Use of Cryptography Protocols

To preserve societal and individual values (i.e. autonomy), compliance with given normative framework (i.e. Privacy and Data Protection) and the development of a set of measures having beneficial effect on society (i.e. public health), the technological solutions implemented by the TU. Graz and endorsed by KUL foresees the adoption of specific cryptographic measures. Cryptographic measures such as differential privacy, homomorphic encryption, but also multi-party computation, which has not been used in this specific use case, ensure an adequate balance of norms and values at stake. The use of such privacy-preserving technologies (PETs) has been evaluated as an optimum to reduce risks and provide individuals with concrete safeguards. In particular, measures implemented by the TU. Graz team ensure, on the one hand, the compliance with privacy and data protection by involved entities (Austrian Authority and electronic communication provider), and - on the other hand - the development of efficient measures to tackle the spread of the COVID-19 virus. Concretely, selected cryptographic measures have been used to anonymise data sets in possession of the two entities during the whole data value chain (acquisition stage, data analysis, data storage and data usage).[174]

5.4.2.4.1 The usage of cryptographic measures in the EU Privacy and Data Protection Context

To verify the legal compliance of the cryptographic techniques with the EU Privacy and Data Protection framework we should assess whether the foreseen encryption measures can reduce the risk linked to the identification of data subjects whose data are processed to create the COVID-19 heat map. Concretely, the assessment carried out aimed to verify that developed cryptographic measures made identification of data subject no longer possible, transforming personal data into anonymised data.

According to the WP29 Opinion,[175] and CJEU jurisprudence,[176] crucial aspects should be taken into account when assessing the identifiability of a given dataset concern time necessary to de-anonymise the data sets in terms of hours and workforce, technical means, together with other contextual elements.[177]

The process to encrypt and make inaccessible to those not in possession of the encryption, fall in the scope of application of the GDPR as a processing[178] of personal data. Consequently, involved entities applying such cryptographic measures should be considered as data controllers for the data sets they

*in the identification of a user'.*Opinion Of Advocate General Campos Sánchez-Bordona, Case C-582/14 Patrick Breyer V Bundesrepublik Deutschland, 12 May 2016 (1), ECLI:EU:C:2016:339, paragraph 68.

173 CJEU, *Patrick Breyer v Bundesrepublik Deutschland* [46]

174 (Bruni *et al.*, no date)

175 Art. 29 Data Protection Working Party (n 13).

176 CJEU, Patrick Breyer v Bundesrepublik Deutschland [46]

177 (Bruni *et al.*, no date)

178 Art. 4(2) GDPR: *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;'*

own and process and need, therefore, to comply with EU privacy and data protection principles and requirements.[179] Contrary, the impossibility to have access and consequently identify personal data by entities other than the one legally entitled to process such data determines for such entities no additional legal obligations. In this case, respect for non-discrimination, non-maleficence and autonomy principles is a necessary precondition for technological solutions that aim to have a beneficial effect on society.[180]

In conclusion, the processing activity involving the exchange of personal data of both electronic communication operator and health authority should be considered per se in compliance with the GDPR provisions.[181] At the same time, the use of cryptographic measures that allows data to be visible only to the data controller in possession of such data ensures an additional level of protection for the individuals.

As a result, the foreseen data-driven solutions ensure compliance by both entities about the personal datasets they have. Contrary, the exchange of data between entities does not foresee any implication for fundamental rights at stake.[182]

6 Conclusion

The cryptographic measures deployed for the exchange of data both from the Health Authority and the electronic communication service providers have been tested by TU. Graz; also taking into account normative, ethical and societal values. The same activities and technologies are performed and developed by members of the **Safe-DEED** consortium that have chosen MPC as a cryptographic measure.

The use of MPC or differential privacy as cryptographic measures will, first of all, guarantee a substantial reduction of risks linked to the processing of personal data as requested by the GDPR. To achieve such purpose, compliance of such cryptographic measures with the EU framework will be ensured following the measurable criteria listed by the Court. Multi-party computation and other cryptographic measures should ensure the impossibility 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, regardless of the exchange of personal data occurring between the two or more entities, the used cryptographic procedures applied to such data make the risk of identification insignificant. Doing so, the adoption of multi-party computation or differential privacy will also, reduce and balance those fundamental rights hampered by the implementation of COVID-19's heat map.

To conclude, the use of multi-party computation and other specific cryptographic measures 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.

179 Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' [2016] Journal of Intellectual Property, Information Technology and Electronic Commerce Law 15, 166; Finck and Pallas (n 23) 17–18.

180 (Bruni *et al.*, no date)

181 Ibid (17)

182 (Bruni *et al.*, no date)

Similarly, due to its technical characteristics multi-party computation, the cryptographic protocol adopted within the **Safe-DEED** project allows for the exchange of data that cannot be visible to others apart from the entity that owns such data.

References

Legislation

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/E.C. (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

Directive (EU) 95/46/E.C. 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.

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.

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.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 077/22, 27 March 1996.

United Nations Universal Declaration of Human Rights, 10 December 1948, https://www.un.org/en/universal-declaration-human-rights/

Convention for the Protection of Human Rights and Fundamental Freedoms, Coucil of Europe, ETS No.005

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407

Directive 2002/58/E.C. 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), OJ L 201, 31.7.2002, p. 37

Jurisprudence

CJEU, Patrick Breyer v Bundesrepublik Deutschland [2016] European Court of Justice Case C-582/14, ECLI:EU:C:2016:779 [42]

Other documents

EU Bodies and Agencies

Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216' (2014)

Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purpose of Regulation 2016/679 (2017).

EDPB, 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' (2020)

Ethics Advisory Group Report, Towards a digital ethics, (2018).

OECD

OECD, 'Exploring the Economics of Personal Data' (2013) 220 OECD Digital Economy Papers 40 <http://dx.doi.org/10.1787/5k486qtxldmq-en>.

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

European Commission

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.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions 'Building a European Data Economy', COM/2017/9 final.

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.

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.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, COM/2020/67 final.

European Commission, Communication on the precautionary principle, COM/2000/1, final.

European Commission, Data Governance and data policies at the European Commission, July 2020.

Academia

Acquisti A., Taylor C. and Wagman L., 'The Economics of Privacy' (2016) 54 Journal of Economic Literature 442. See also Taylor, C. and L. Wagman (2014). Consumer privacy in oligopolistic markets: Winners, losers, and welfare. International Journal of Industrial Organization 34, 80-84.

Batini, C., Cappiello, C., Francalanci, C., and Maurino, A. (2009). Methodologies for Data Quality Assessment and Improvement. ACM Computing Surveys 41, 3 (July 2009).

Beauchamp, T. L., & Childress, J. F. (2001). Principles of biomedical ethics (5th ed.). New York: Oxford University Press.

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

Bruni A. and Helminger L. and Kales D. and Rechberger C. and Walch R. , Privately Connecting Mobility to Infectious Diseases via Applied Cryptography, Cryptology ePrint Archive: Report 2020/522

Cattaneo G., Micheletti G., Glennon M., La Croce C., (IDC) and Mitta C., European Commission, The European Data Market monitoring tool, Key facts & Figures, First Policy Conclusions, Data Landscape and Qualified Stories, D2.9 Final Study Report, Directorate-General for Communications Networks, Content and Technology, June 2020.

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.

Demetzou K., 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of 'High Risk' in the General Data Protection Regulation' (2019) 35 Computer Law and Security Review 105342.

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.

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.

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

Kerber W., 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection' [2016] SSRN Electronic Journal.

Mantelero A., 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law and Security Review 754

Angwin J. Online tracking ramps up e popularity of user-tailored advertising fuels data gathering on browsing habits. Wall Str J June 18 2012:B1.

S Spiekermann and others, 'Towards a Value Theory for Personal Data' <www.palgrave.com/journals> accessed 7 October 2020.

Palm E. and Hansson S.O., 'The Case for Ethical Technology Assessment (ETA)' (2006) 73 Technological Forecasting and Social Change 543.

Porcedda MG., and Adinolfi A., 'Use of the Charter of Fundamental Rights by National Data Protection Authorities and the EDPS' (2017).

Scassa T., 'Data Ownership' [2020] Centre for International Governance Innovation 1

Short, JE, and Todd, S. What's Your Data Worth? MIT Sloan Management Review. Retrieved October 24, 2019 from https://sloanreview.mit.edu/article/whats-your-data-worth/

Slotin, J. (2018): What Do We Know About the Value of Data? Global Partnership for Sustainable Development Data. Retrieved from http://www.data4sdgs.org/sites/default/files/services_files/Value%20of%20Data%20Report_Final_compressed_0.pdf

Sollie P., 'Ethics, Technology Development and Uncertainty: An Outline for Any Future Ethics of Technology' (2007) 5 Journal of Information, Communication and Ethics in Society 293.

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

Spiekermann S., and Korunovska J., 'Towards a Value Theory for Personal Data' (2017) 32 Journal of Information Technology 62.

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.

Spindler G. and Schmechel P., 'Personal Data and Encryption in the European General Data Protection Regulation' [2016] Journal of Intellectual Property, Information Technology and Electronic Commerce Law 15, 166; Finck and Pallas (n 23) 17–18.

Stahl B.C. and Wright D., 'Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation' (2018) 16 IEEE Security and Privacy 26.

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

Wright D. and de Hert P., Privacy Impact Assessment (Springer Netherlands 2012).

Wright D., 'A Framework for the Ethical Impact Assessment of Information Technology' (2011) 13 Ethics and Information Technology 199.

Yordanov A., 'Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation' (2017) 3 European Data Protection Law Review 486.

Zech H., 'A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data' (2016) 11 Journal of Intellectual Property Law and Practice 460.

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

Others

Centre for Information Policy Leadership, 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR', CIPL GDPR Interpretation and Implementation Project, 21 December 2016, 13.

CNIL, 'PIA, Knowledge Bases' (2018). https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

Mason, R. (2014). HMRC to sell taxpayers' financial data. The Guardian. Retrieved October 28, 2020 from https://www.theguardian.com/politics/2014/apr/18/hmrc-to-sell-taxpayers-data

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/116th-congress/senate-bill/1951/text