



Participatory Approaches to a New Ethical and Legal Framework for ICT

PANELFIT

Project Agreement No: 788039

D3.1

**Issues and Gap Analysis on Data Commercialisation
in the Context of ICT Research and Innovation**

© Copyright 2020 – All Rights Reserved

Dissemination level

PU	Unrestricted PUBLIC Access – EU project	X
PP	Project Private, restricted to other programme participants (including the Commission Services) – EU project	
RE	RESTRICTED, Restricted to a group specified by the consortium (including the Commission Services) – EU project	
CO	Confidential, only for members of the consortium (including the Commission Services) – EU project	

Document Information

Grant Agreement n°	788039	
Project Title	Participatory Approaches to a New Ethical and Legal Framework for ICT	
Project Acronym	PANELFIT	
Project Coordinator	UPV/EHU	
Document Responsible Partner	GUF	frederic.tronnier@m-chair.de
Document Number	D3.1	
Document Title	D3.1: Issues and Gap Analysis on Data Commercialisation in the Context of ICT Research and Innovation	
Dissemination Level	PU	
Contractual Date of Delivery	30/09/2019	

Partners involved in the Document

N°	Participant organisation name (short name)	Acronym	Check if involved
1	Universidad del País Vasco/Euskal Herriko Unibertsitatea	UPV/EH U	X
2	Fonden Teknologiradet	DBT	
3	Vrije Universiteit Brussel	VUB	
4	Oesterreichische Akademie der Wissenschaften	OEAW	
5	Goethe Universität. Frankfurt am Main	GUF	X
7	European Citizen Science Association (ECSA)	ECSA	
8	European Network of Research Ethics Committees	EUREC	X
9	Consejo Superior de Investigaciones Científicas	CSIC	
10	Centro per la Cooperazione Internazionale/ Osservatorio Balcani Caucaso Transeuropa	CCI/ BCT	
12	EVERIS SPAIN, S.L.U.	EVERIS	X



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

13	Unabhängiges Landeszentrum für Datenschutz AöR	ULD	X
----	------------------------------------------------	-----	---

Circulation List

- European Commission
- PANELFIT Consortium



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Content

Executive Summary	6
1 Introduction to Data Commercialisation	9
2 Issues & Gap Analysis Devoted to Data Commercialisation	17
2.1 Data Commercialisation and Counter-Performance Practices	17
2.1.1 Context and Legal Background	17
2.1.2 Issue	21
2.1.3 Relevance & Impact on ICT Research and Innovation	21
2.1.4 Mitigation Measures	22
2.2 Collecting Consent for the Processing by yet Unidentified Recipients	24
2.2.1 Context and Legal Background	24
2.2.2 Issue	26
2.2.3 Relevance & Impact on ICT Research and Innovation	26
2.2.4 Mitigation Measures	27
2.3 Unclarities with Regards to shared Controllershship	28
2.3.1 Context and Legal Background	28
2.3.2 Issue 1: Processor or controller?	28
2.3.3 Relevance & Impact on ICT Research and Innovation	29
2.3.4 Mitigation Measures	30
2.3.5 Issue 2: Joint controllership	30
2.3.6 Relevance & Impact on ICT Research and Innovation	31
2.3.7 Mitigation Measures	31
2.3.8 Issue 3: Data subject and controller?	32
2.3.9 Relevance & Impact on ICT Research and Innovation	33
2.3.10 Mitigation Measures	34
2.4 Determination of the Value of Data	35
2.4.1 Context and Legal Background	35
2.4.2 Gap	36
2.4.3 Relevance & Impact on ICT Research and Innovation	36
2.4.4 Mitigation Measures	37
2.5 Management of Individual Privacy Preferences	39
2.5.1 Context and Legal Background	39
2.5.2 Gap	41
2.5.3 Relevance & Impact on ICT Research and Innovation	41



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.5.4 Mitigation Measures.....	42
3 Conclusion.....	43
Appendix.....	44



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Executive Summary

This document consists of the Issues & Gap Analysis on the current regulation related to data commercialisation in ICT research and innovation. It corresponds to “Task 3.1. To prepare an issues and gaps analysis on the regulation of commercialization of data produced in the context of ICT research and innovation ...” of the description of work in WP3 of the grant agreement. It is directed at the European Commission and will be further elaborated on in the Critical Analysis (D5.2).

In the context of the existing EU legal framework, ‘gap’ defines a missing regulation, while ‘issue’ relates to a current law that needs further clarification.

Starting point for the identification of issues and gaps was a workshop with four legal and four industry experts from Spain, Finland, England, the Netherlands, Germany, and France, which took place on 3 June 2019 in Bilbao (see appendix for the workshop agenda and the list of invited experts). The workshop, corresponding to Task 3.3. in the grant agreement for WP3, was structured into four sessions:

- 1) Ownership of Data
- 2) Usage of External Databases
- 3) Monetising Internal Databases
- 4) Good Commercialisation Governance

Each of the experts was asked to give a short presentation on one of the topics, followed by a discussion with all attendees (experts and present projects partners). Based on the results of the workshop, several attendants have also produced academic papers on the commercialisation of data, data ownership and big data that are currently awaiting review and are to be published in a special issue in the *European Review of Private Law*.

After the workshop, a literature review based on the identified issues and gaps was conducted. The results – the main issues and gaps found – are displayed in this deliverable. The objective of the analysis at hand is not to list all existing issues and gaps related to the topic, but rather to highlight the most pressing and most recently emerged issues and gaps in the legislation, as identified in the workshop through the help of the experts. In the following, these issues and gaps, their potential negative impact, as well as proposed mitigation measures are outlined shortly.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

- 1) **Issue - Data Commercialisation and Counter-Performance Practices:** It is unclear whether or not a form of trade that does not involve money transfers but rather the monetisation of the data, i.e. the process of converting personal data into currency, is lawful. This prevents not only the emergence of markets and commons of personal data, but also the development of new services, making an official position by legislators necessary.
- 2) **Issue - Collecting Consent for the Processing by yet Unidentified Recipients:** It is unclear whether, under the General Data Protection Regulation (GDPR), a primary controller can collect consent as a legal basis for a yet unidentified recipient, and if so, under what conditions. Without clarification by the European Data Protection Board (EDPB), research and innovation based on consent, for instance in health science or open access research, is restrained.
- 3) **Issue - Unclearities with regards to Shared Controllorship:** It is neither determined to what extent exactly a processor must be involved to become a (joint) controller nor what legal consequences will follow if the shared responsibilities and obligations are not suitably arranged among joint controllers. Furthermore, it is unclear what minimum responsibilities and obligations must be fulfilled if a cooperation is impossible. Until the issues are clarified through an authoritative interpretation of the GDPR, contracts and agreements may be utilised between (joint) controllers and processors to determine rights and responsibilities of all parties involved in order to mitigate legal uncertainties.
- 4) **Gap - Determination of the Value of Data:** There is no established pricing mechanism for data, which is necessary for a fair and transparent commercialisation of data. Determining the value of data is necessary in order to achieve a fair and transparent commercialisation of data and the development of regulated data markets. Further research on suitable pricing mechanism is required to overcome this gap.
- 5) **Gap - Management of individual privacy preferences:** Data subjects need to have a real choice about whether they want to share their data and to what extent. Due to the high number of services used, a system to manage individual privacy preferences is required. Realistically, the implementation of such needs to be legally obligatory in order to gain market acceptance and have a real impact. The development and implementation of such a system through research projects would counteract consent fatigue among individuals, benefiting both ICT researchers and data subjects



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

For all issues and gaps, the context and legal background are discussed first. Issues and gaps are then defined and their relevance and impact on ICT research and innovation (R&I) evaluated. Issues and gaps in the current regulation create uncertainty for researchers and organisations representing risks to their research or commercial activities. Lastly, measures to solve identified issues and fill existing gaps are stated. In order to overcome legal uncertainty, clarification of the existing legislation is necessary. Where applicable, additional measures for ICT researchers are illustrated.

The first draft of this document was evaluated by twenty additional experts who attended a common workshop held in Madrid between the 2nd and 4th of March, 2020. On the basis of the feedback provided, a renewed version of this document was created during March and April 2020 and again reviewed by two experts in a first round of extensive public consultation in May. This document represents the final version of D3.1 based on all feedback provided.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

1 Introduction to Data Commercialisation

According to the European Commission in 2019, “the value of the European Data Market is expected to reach 77.8 Billion Euro, with a growth rate of 97% in 2018, and at an average rate of 4.2% out to 2020¹”. In 2025, “... the Data Market will amount to more than 82 billion Euro in the EU27, against 60.3 billion Euro in 2018 (a 6.5% CAGR 2020-2025)...²”. The same estimate predicts that, if policy and legal framework conditions for the data economy are put in place in time, its value will increase to EUR 680 billion by 2025 for the EU28 (550 billion for the EU27), representing 4.2% (4.0%) of the overall EU GDP for a baseline scenario³.

Still, the term ‘data commercialisation’ is one that causes diverging reactions among different stakeholders in the environment of data protection and ICT research. While some people regard it as a reality that is indeed lawful - whether commercially and/or socially desirable or not -, others assess it to be unlawful and unacceptable for personal data in general. This could be explained by the fact that there does not exist one generally approved definition of the term. As the lawfulness of commercialising and processing data highly depends on its specification, it is crucial to define the context first. Hereby, one should differentiate between:

- a) The type of data, that is either personal or non-personal data⁴,
- b) The amount of data, that is either multiple data records in a database or individual data records
- c) The source of the data, that is either collected by the data controller, by a third party or publicly available data
- d) The recipient of the data, that is either another researcher/research institution or a commercial enterprise
- e) The form of commercialisation, that is the licensing or granting access of data

¹ The European Commission, IDC Italia and The Lisbon Council deliver annually a report on the European Data Market. Latest (28th of June, 2019) is available at:

http://datalandscape.eu/sites/default/files/report/D2.6_EDM_Second_Interim_Report_28.06.2019.pdf. p.67.

Disaggregated data can be found at The European Data Market Monitoring Tool:

<http://datalandscape.eu/european-data-market-monitoring-tool-2018>.

² Ibid. p.41

³ Ibid.

⁴ See European Commission. A European strategy for data, pp. 4-5. Available at:

https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

a) Personal data vs. non-personal data

According to 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”⁵.

Consequently, non-personal data refers to information that does not fulfil the criteria of Art. 4(1) GDPR. The European Commission views the free flow of non-personal data as a prerequisite of the data economy⁶ and the GDPR does not apply to non-personal data. The commercialisation of non-personal data is therefore not subject of this deliverable. Nonetheless, it must be taken into account that the EU aims to develop a European data market that encompasses both personal and non-personal data⁷. The focus here lies on the possibility of commercialising personal data.

b) Database vs. individual data records

A data record may consist of personal or non-personal data. A single data record that consists of personal data of one single data subject, is not a database, but the data set of a single data subject. For a single data record, for instance the telephone number of an individual, commercialisation seems unlikely, although not impossible, as the GDPR describes that personal data shall be collected for a specific and legitimate purpose (Art. 5(1)(b)) and the data should be adequate and relevant to achieve the purpose for which the data is going to be collected Art. 5(1)(c). Consequently, the commercialising of a single data record would rightly arouse suspicion from any data protection officer (DPO).

⁵ Art. 4(1) GDPR

⁶ European Commission. Free flow of non-personal data. Available at: <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>

⁷ See European Commission. A European strategy for data, pp. 4-5: “The aim is to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and business also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value...”. Available at: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

A database, on the other hand, can indeed be commercialised – even if it contains personal data provided that the requirements by the GDPR are met. A database is defined by the European Union Directive 96/9/EC on the legal protection of databases as “... a collection of independent works, data or other materials, which have been arranged in a systematic or methodical way, and have been made individually accessible by electronic or other means”.⁸

According to this Directive and the European IP Helpdesk⁹, the data or information must fulfil the following criteria to be regarded as database:

- The data or information must be capable of separation without losing their informative content;
- The data or information must be organised according to specific criteria, which means that only planned collections are covered;
- The data or information must be individually accessible – mere storage of data is not covered by the term database.

For a database, the sui generis database right applies¹⁰ to the holder, that is the creator, of the database. The sui generis right grants its holder the option to sell or license the database.¹¹

Recently, granting access to or licensing a database (see also subchapter e) that contains personal data to other organisations has become a profitable and frequent business model among large online corporations¹². Often companies monetise collected personal data from data subjects instead of charging the subject a fee for their service. Resulting legal issues will be discussed in chapter 2.1.

c) Source of data

Personal data can be obtained from different sources. It may be obtained from the data subject, whereby Art. 6 GDPR describes the legal grounds for processing that is, among others, the data subjects’ consent. It is important to state that consent must not only be obtained for collecting

⁸ See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. Whereas 17. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009>

⁹ European IP Helpdesk. Available at: <http://www.iprhelpdesk.eu/node/2014>

¹⁰ European IP Helpdesk. Available at: <https://www.iprhelpdesk.eu/taxonomy/term/166>

¹¹ See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

¹² Gomez, J., Pinnick, T. and A. Soltani (2009). KnowPrivacy. UC Berkeley, School of Information. Available at: http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf (visited on 04/04/2020).



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

the data, but also for commercialising the data to a third party and for the processing activities of this third party.

Personal data may also be obtained from third parties or could be publicly accessible. Art. 14 GDPR regulates how a data controller shall act if personal data was obtained from somewhere other than from the data subject itself. It states inter alia that the data subject needs to be informed whether the data was obtained from publicly accessible sources¹³ or another third party (Art. 14(2)(f) GDPR). Should the processing by the data controller further differ from the intended purpose for which the data was originally collected, the data controller is obliged to inform the data subject about this new purpose, as well as other points expressed in Art. 14(1) and Art. 14(2) before the processing. However, Art. 14(1-4) shall not apply if “the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Art. 89(1)(...)¹⁴”.

d) The recipient and the new purpose of the data

The preconditions for commercialising data also depend on the type of recipient and the recipient’s purposes with the data. Considering that the data is supposed to be commercialised, consent from the data subjects is needed as the main legal ground for processing. However, Art. 6 provides other legal grounds than consent, such as public interest or compliance with the law. However, these seem unlikely for commercialising activities.

If the data subjects have not explicitly given their consent, the commercialising of personal data is further regulated under Art. 6(4) GDPR. Here it states that the controller shall take into consideration the link between the original and the new purposes, the original context of collection, the nature of the personal data, and consequence and safeguard factors in order to assess whether the processing, here commercialisation, is lawful.

Therefore, the commercialisation of data from a research project to a commercial entity or to a researcher/research organisation needs to consider the factors described in Art. 6(4) GDPR.

¹³ Art. 14 GDPR. Available at: <https://gdpr.eu/article-14-personal-data-not-obtained-from-data-subject/>

¹⁴ Ibid.



Should these not apply, a new legal basis for processing, Art. 6(1), has to be obtained from the data subject for the new form of processing.

However, if data subjects consented to a processing of their data for research purposes beforehand, the commercialisation of data to other researchers or research organisations is thus more likely to be lawful than the sale to a for-profit organisation. Additionally, Art. 6.1(b) GDPR states that, in accordance with Art. 89(1) GDPR, research purposes are not to be considered incompatible with the initial purpose, if the identification of data subjects is no longer permitted during further processing. The new purpose of the data processing should nonetheless be stated to the data subject beforehand. Hereby, purpose limitation (limiting the purposes for which the data is going to be used) is advised. Nonetheless, while the commercialisation of data for research purposes might be more likely to be lawful than for non-research purposes, the mainstay should be the data subject and what potential disadvantages could arise through the data commercialisation for it.

e) Licensing and granting access to data

The concept of data ownership is a controversy being discussed in academia. It is not clear whether data can and should be owned in general and who the owner of personal data would be. This is not only a legal, but also a philosophical and ethical question that is yet to be answered. The GDPR touches this question only indirectly. Recital 7 GRPR states that “Natural persons should have control of their own personal data”¹⁵, which relates to a sort of ownership of data. Similarly, Recital 68 also mentions the control of the data subjects about their “own data”¹⁶. Rights such as the right of data portability can be seen as the first step towards data ownership of data subjects on their personal data¹⁷. Nonetheless we follow the current majority opinion that states that personal data cannot be owned. Therefore, personal data itself cannot be sold like physical goods. Even when data have been widely qualified as “the oil of 21st

¹⁵ Recital 7 GDPR. Available at: <https://www.privacy-regulation.eu/en/recital-7-GDPR.htm>

¹⁶ Recital 68 GDPR. Available at: <https://www.privacy-regulation.eu/en/r68.htm>

¹⁷ De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, 34(2), 193-203.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

century”¹⁸ in order to underline that data are a new source of wealth (just remember the economic data outlined above), the legal concept of goods is based on movable physical goods. Even if data work as assets, some of their characteristics make it difficult to apply the legal status of goods: data are non-rivalrous, non-depleting, regenerative, nearly limitless, easily transported, infinitely copyable and experiential. Instead the commercialisation of data is closer to the licensing of industrial property rights, whereby the licensor grants the licensee the right to access and use the data for a specific purpose that is to be stated in an agreement. This agreement includes the rights and obligations of both parties towards the data and the data subject. It is also necessary to determine whether this access right and right to use the data is exclusive, or rather constrained and non-exclusive. Similarly, one entity can grant another entity access to the data without collecting a payment for it.

Through the licensing of data, the obligations of the data controller may pass on to the licensor, who may become a data controller as well. Issues that might arise through this joint controllership are discussed in the Issues and Gap Analysis.

Overall, and specifically in the context of this document, the commercialisation of personal data may be defined as the processing of personal data as regulated under the GRPD, in form of licensing by granting third parties’ access to collected personal data for a monetary profit. While it is assumed that personal data possesses economic value that may be transferred between parties¹⁹, the specifics of the commercialisation of data however may differ, depending on the licensor, licensee and the purpose of the data, as was discussed above.

Ethical considerations

The commercialisation of data does not only create issues and gaps through unclear or missing regulation but needs also to be reviewed an ethical perspective. The European Commission states in a non-guiding document on *Ethics and Data Protection (2018)* for researchers that: “... the fact that your research is legally permissible does not

¹⁸ See Lohsse, S., Schulze, R., & Staudenmayer, D. (2017). Trading Data in the Digital Economy: Legal Concepts and Tools. *Trading Data in the Digital Economy: Legal Concepts and Tools*. Hart & Nomos, p. 15: “data is the blood in the veins of the digital economy”.

¹⁹ Definition based on the definition of commercialisation of consumer data by: Carmen Langhanke, Martin Schmidt-Kessel, ‘Consumer Data as Consideration’ [2016] EuCML 218, 219



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

necessarily mean that it will be deemed ethical²⁰. Ethical requirements for the commercialisation of data need also be met.

The GDPR already encompasses ethical aspects such as transparency and accountability between data subjects and controllers and processors²¹ and aims to foster the societal interest to protect data and ensure privacy, for instance in Art. 57(1)(b), stating that public authorities must “promote public awareness” on the aspects of data processing. Human dignity and personal autonomy are moral values, covered in constitutions and laws, that need to be respected through the protection of data²², also when data is being commercialised.

However, several ethical issues and questions arise when looking at the commercialisation of data, as defined in this document. Should it be possible to own personal data by the data subject? How can data indeed be ethically commercialised if the ownership of data is not defined? While data is commercialised in practise by data processors and controllers for a monetary benefit, the data subject itself is not benefiting from the commercialisation. The GDPR is protecting the data subject and giving him/her the possibility to deny other parties access and usage of his/her personal data. As will be shown in later chapters, the benefit from granting access and consenting to processing of personal data is marginal for the data subject. The monetary benefit for data subject is limited to access to services and products, ‘free of charge’, indirectly through their personal data. Although this is an ethical issue, the question if this transaction can be considered as a commercialisation of data, is also a legal issue and is discussed later in this document.

Unless an established pricing mechanism for personal data is developed, fair data markets that ensure an adequate remuneration of individuals relinquishing their personal data are unlikely to occur. As long as privacy is not transparently priced, individuals do not know the value of their personal data, do not know if they are getting a fair deal should they accept to monetise their data, and remain unaware of their market power. This demonstrates that legal and ethical issues

²⁰ Ethics and data protection. (2018). Available at: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

²¹ Hijmans, Hielke and Raab, Charles D., Ethical Dimensions of the GDPR (July 30, 2018). in: Mark Cole and Franziska Boehm (eds.), Commentary on the General Data Protection Regulation, Cheltenham: Edward Elgar (2018, Forthcoming) . Available at SSRN: <https://ssrn.com/abstract=3222677>

²² Hielke Hijmans, *The European Union as Guardian of Internet Privacy*, Law, Governance and Technology Series 31, 2016, at 2.8.2.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

are closely connected and that the commercialisation of data needs to be reviewed with both, ethical and legal issues in mind.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2 Issues & Gap Analysis Devoted to Data Commercialisation

2.1 Data Commercialisation and Counter-Performance Practices

2.1.1 Context and Legal Background

Both the commercialisation of data and the value of the EU data economy are experiencing strong growth that is predicted to continue in the future²³. In the data economy, an ecosystem consisting of as researchers, manufacturers and infrastructure providers, market players are extracting value from gathered data²⁴. Currently, a considerable number of service providers are opting for monetising personal information instead of charging a fee for using a content platform. This policy has become a very successful revenue model on the internet.²⁵ Once a large database is created, platform operators provide, rent, or sell it to their affiliates, business partners, and third parties²⁶. Nevertheless, it is unclear whether such practises are acceptable according to the EU regulatory framework.

There are good reasons that fuel such doubts. Surprisingly, neither the Directive on the legal protection of databases (Directive 96/9/EC) nor the General Data Protection Regulation (GDPR) (Regulation 2017/679) consider this topic. However, the Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services²⁷ states (whereas 24):

“Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot

²³ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions “Building a European Data Economy”. Brussels, 10.01.2017. COM (2017) 9 final. p. 2. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN>. These data on the evolution of EU data economy can be updated year-on-year at The European Data Market Monitoring Tool (<http://datalandscape.eu/european-data-market-monitoring-tool-2018>)

²⁴ Ibid.

²⁵ Schreiner, Michel & Hess, Thomas. (2015). Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-freemium Model to Media Companies. Conference: Proceedings of the 23rd European Conference on Information Systems, At Münster, Germany

²⁶ Gomez, J., Pinnick, T. and A. Soltani (2009). KnowPrivacy. UC Berkeley, School of Information. URL: http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf (visited on 04/04/2020).

²⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0770>



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

*be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to **contractual remedies**. This Directive should, therefore, apply to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or undertakes to provide, personal data. The personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service. Union law on the protection of personal data provides for an exhaustive list of legal grounds for the lawful processing of personal data. This Directive should apply to any contract where the consumer provides or undertakes to provide personal data to the trader. For example, this Directive should apply where the consumer opens a social media account and provides a name and email address that are used for purposes other than solely supplying the digital content or digital service, or other than complying with legal requirements. It should equally apply where the consumer gives consent for any material that constitutes personal data, such as photographs or posts that the consumer uploads, to be processed by the trader for marketing purposes. Member States should however remain free to determine whether the requirements for the formation, existence and validity of a contract under national law are fulfilled.”*

Somehow, this seems as accepting the idea of a data economy (that is, acceptance of data as wealth and data commercialisation as a reality). However, if this is the case, it should have been expressed in a stronger manner. As a matter of fact, this was the case at previous stages of this Directive. In particular, number 24 of the Directive 770/2019 should be confronted with the numbers 13 and 14 of the Proposal 634/2015 (the first proposal for current Directive 770/2019), where we can read the following on digital economy²⁸:

“(WH-13:.) In the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. Digital content is often supplied not in exchange for a price but against counter-performance other than money i.e. by giving access to personal data or other data (...)”

²⁸ See on this: Proposal 634/2015, p.16f. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015PC0634&from=EN>



“(WH-14:) As regards digital content supplied not in exchange for a price but against counter-performance other than money, this Directive should apply only to contracts where the supplier requests and the consumer actively provides data, such as name and e-mail address or photos, directly or indirectly to the supplier for example through individual registration or on the basis of a contract which allows access to consumers’ photos. This Directive should not apply to situations where the supplier collects data necessary for the digital content to function in conformity with the contract (...)”

Those considerations were withdrawn and changed into WH-24 in the final text of Directive 770/2019, probably due to the unfavourable opinion of the EDPS on the issue in the Opinion 4/2017²⁹, namely:

“(Executive Summary, p. 3:) The EDPS acknowledges the importance of the data-driven economy for the growth in the EU and its prominence in the digital environment as set out in the Digital Single Market strategy. We have argued consistently for the synergies and complementarity between consumer and data protection law. We therefore support the aim of the Commission’s proposal of December 2015 Directive on certain aspects concerning contracts for the supply of digital content to enhance the protection of consumers who are required to disclose data as a condition for the supply of ‘digital goods’. However, one aspect of the Proposal is problematic, since it will be applicable to situations where a price is paid for the digital content, but also the where digital content is supplied in exchange for a counter-performance other than money in the form of personal data or any other data. The EDPS warns against any new provision introducing the idea that people can pay with their data the same way as they do with money. Fundamental rights such as the right to the protection of personal data cannot be not be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity.

(...)

(2. The use of personal data as counter-performance)

14. The EDPS welcomes the intention of the legislator to make sure that the so-called “free services” are subject to same protection for the consumers when

²⁹ Opinion 4/2017, pp. 3 and 7. Available at: https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf.



they do not pay a price for a service or content. However, personal data cannot be compared to a price, or money. Personal information is related to a fundamental right and cannot be considered as a commodity. Elaborating on this assumption, the following sections present the reasons why the EDPS recommends avoiding the use of the notion of data as counter-performance in the Proposal and presents alternative options to replace the use of such a notion. (2.1. Personal data as counter-performance and the fundamental right to data protection)

15. The business models of “free services” have already been addressed by the EDPS in previous Opinions³⁰. For many digital services, companies foster the perception that they are provided for free, while in fact individuals are required to surrender valuable information. In effect, providers require the disclosure of personal information, often without the knowledge of the individual, as a condition for the supply of the service. The extent to which companies should be able to leverage and to monetise the personal datasets acquired has been subject of some debate.”

Similarly, Recital 18 of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), the so-called e-Privacy Regulation³¹, stated that “in the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements”. However, this Recital was again criticised by the European Data Protection Supervisor, in his Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)³², which states:

“The EDPS emphasises that personal data cannot be considered as ‘counter-performance’ for a requested service such as access to a website or an app. This is

³⁰ See Opinion 8/2016, on coherent enforcement of fundamental rights in the age of big data. Available at: https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.

³¹ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>

³² Opinion 6/2017, p.25. Available at: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

because consent is valid only if freely given and withdrawn without detriment to the individual concerned. As the EDPS recently explained in his Opinion 4/2017 on the Digital Content Proposal, the notion of ‘counter-performance’ creates additional obligations for the individual and is not consistent and compatible with the notion of consent under the GDPR. The notions of ‘paying with personal data’ and offering personal data as ‘counter-performance’ would indeed therefore undermine the current legal grounds for lawful processing as set out in Art. 6 of the GDPR. The EDPS, therefore, recommends deleting the quoted phrase from recital 18 and amending it as follows: ‘In the digital economy, services are often supplied with remuneration paid by a third party rather than by the recipient of the service’.”

However, this part of Recital 18 has remained the same in the last version of the Regulation (November 2019)³³. Thus, at the present moment it is unclear whether the EU policy is setting the limits to a market of data in an appropriate way. On the one hand, the sale of personal data, in form of an individual data record, in exchange for money, as such, seems incompatible with the GDPR. Therefore, it is uncertain whether or not it will be possible to continue with a form of trade that does not involve money transfers, but rather the monetisation of the data (that is, the process of converting personal data into currency). This would be achieved via the permission of counter-performance practices.

2.1.2 Issue

It is unclear in the EU legal framework whether the ban on data commercialisation extends to counter-performance practices, and if so, under what conditions. In other words, it is unclear whether monetisation of data will be considered as commercialisation of data and to what extent it will be forbidden in the EU.

2.1.3 Relevance & Impact on ICT Research and Innovation

In general, this lack of clarity represents a major impediment to the development of the digital market and the interchange of services in this context. A company could hardly plan its research strategy in the ICT sector if it cannot foresee whether personal data from customers can be

³³ <https://data.consilium.europa.eu/doc/document/ST-13808-2019-INIT/en/pdf>



processed and/or under which conditions. This prevents not only the emergence of markets and commons of personal data, but also the development of new services depending on the value added by their data collection processes ³⁴.

2.1.4 Mitigation Measures

The situation that we have described demands an urgent search “for solutions that serve to reconcile strong data protection with the interests of the data economy”³⁵. This is a complex goal, since the “GDPR has not primarily been drafted with the data economy in mind”³⁶. Nevertheless, it is difficult to imagine that the data economy will stop its path of growth in the future. Perhaps the best way to protect privacy would be facing data economy and data markets (both on personal and non-personal data) as a current reality, and regulate them. From the EU point of view this attitude has already begun not only in 2014³⁷ and 2017³⁸, but mainly in 2020 through the European strategy for data³⁹. Nonetheless, the issue demonstrated in this section need a major initiative able to provide a definitive solution on the question of the legality or not of counter-performance practises. An official, unique position on the possibility to offer

³⁴ As Wendehorst claimed, “the main problem with including personal data in the data economy is the requirement of separate justification and the fact that any invalidity or any withdrawal of consent where processing is based on consent, or any rightful objection where processing is based on legitimate interests, or any further developments that make the balance of interests under the legitimate interests justification tip, result in the unlawfulness of processing and a duty to erase. The result is excessive uncertainty for businesses and, in fact, the impossibility to make clear investment decisions” (Wendehorst, C.. How to reconcile data protection and the data economy. At Lohsse, S., Schulze, R.; Staudenmayer, D. (eds.). Trading Data in the Digital Economy: Legal Concepts and Tools. Münster Colloquia on EU Law and the Digital Economy III. Hart & Nomos. 2017. p. 354.)

³⁵ Wendehorst, C.. How to reconcile data protection and the data economy. At Lohsse, S., Schulze, R.; Staudenmayer, D. (eds.). Trading Data in the Digital Economy: Legal Concepts and Tools. Münster Colloquia on EU Law and the Digital Economy III. Hart & Nomos. 2017. pp. 353-354

³⁶ Ibid.

³⁷ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions “Towards a thriving data-driven economy”. Brussels. 02.07.2014. COM (2014) 442 final. Available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0442&from=EN>.

³⁸ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions “Building a European Data Economy”. Brussels, 10.01.2017. COM (2017) 9 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN>.

Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication Building a European data economy. Brussels. 10.01.2017. SWD (2017) 2 final. Available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN>.

³⁹ 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”. Brussels, 19.02.2020. COM (2020) 66 final. Available at: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

personal data to compensate access to some services must be produced, that can provide guidance for ICT researchers.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.2 Collecting Consent for the Processing by yet Unidentified Recipients

2.2.1 Context and Legal Background

Europe has recognised the importance of data for the growth of its internal market⁴⁰ and the competitiveness of its research and innovation⁴¹. Here, personal data plays an important role in many possible applications and sectors. Since it is not always possible to fully anonymise such data, any strategy to implement the processing for which the data was intended must be compliant with the General Data Protection Regulation (GDPR).

One of the requirements of the GDPR for the processing of personal data is the need for a valid legal basis (Art. 6). Consent (Art. 6(1)(a) GDPR) is one of the possible legal bases foreseen by the GDPR (in Art. 6(1)).

In the context of personal data, when conceiving market offerings, commons for sharing data for the common good, or open access to scientific research data, clarity of which legal bases are available is crucial. As illustrated in the sequel, whether consent is a valid option currently remains unclear. This uncertainty hinders the conception of initiatives within the European vision and ICT researchers in their daily business. It is therefore recommended here to clarify this issue.

The difficulty has its root in the combination of three elements:

- (i) Recital 42 GDPR states that in order for consent to be informed, the data subject has to know the identity of the controller at the time of giving consent⁴².
- (ii) In markets and commons, the parties who will receive and process the data (i.e., controllers according to the GDPR) are yet unknown at the point of time of data collection.
- (iii) Frequent subsequent requests to data subjects, asking for additional consent to the processing by new controllers (possibly in the form of *dynamic consent*⁴³), are likely

⁴⁰ European Commission, European data strategy, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (last visited 9/4/2020).

⁴¹ European Commission, European legislation on open data and the re-use of public sector information, <https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information> (last visited 9/4/2020).

⁴² Sentence 4 of Recital 42 GDPR reads: “For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.”

⁴³ See for example, Kristin Solum Steinsbekk et al., ‘Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem?’ (September 2013), 21(9) European journal of human genetics⁸⁹⁷.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

to lead to consent fatigue⁴⁴. In order to stop new requests, a data subject may then simply withdraw⁴⁵ all consent.

For these reasons, we consider consent only then a feasible legal basis, if it is possible to ask the data subject once at the time of data collection for consent to future processing by other controllers of specified categories, such as the similar industry or purpose of processing. The purposes of such future processing would evidently have to be specified⁴⁶. The use of *tiered consent*⁴⁷ could provide data subjects with several options here. For such consent to be feasible, instead of specifying every additional controller, it would have to be sufficient to specify only the categories of controllers. This would be comparable to the GDPR permitting to specify categories of recipients instead of individual recipients (see Art. 13(1)(e) GDPR).

A typical example that uses such a kind of consent is a health care institution who asks consent to using a pseudonymised version of the data for specified research purposes, not only of its inhouse research department, but also for external research departments. These could for example be specified as the category of formally accredited public medical research entities who are subject to a mandatory approval by an ethics commission prior to any data processing and are located in the EU. It is noteworthy that the here described form of consent is similar but distinct from *broad consent*⁴⁸, as extensively exposed in deliverable 2.1 produced by this project.

In summary, while the possibility of asking consent for the processing of yet unknown future controllers seems crucial for implementing markets and commons of personal data, Recital 42 GDPR seems to indicate that this is not permitted. This is not conclusive, however, since it is only a recital and other areas of the GDPR indeed grant comparable possibilities, including broad consent in scientific research (Recital 33 GDPR) and the specification of recipients as categories instead of individuals (Art 13(1)(e) GDPR).

⁴⁴ Ploug, T., & Holm, S. (2013). Informed Consent and Routinisation. *Journal of Medical Ethics*, 39(4), 214-218. <https://doi.org/10.1136/medethics-2012-101056>

⁴⁵ Note that according to the GDPR, the withdrawal of consent is possible at any point of time (see Art. 7(3)).

⁴⁶ Note that Art. 6(1)(a) GDPR, that defines consent as a legal basis, already states that consent must always be for specific purposes.

⁴⁷ See for instance Eline M. Bunnik et al., 'A tiered-layered-staged model for informed consent in personal genome testing' (21 November 2012), 21 *European journal of human genetics* 596.

⁴⁸ Mark Sheehan, 'Can broad consent be informed consent?' (November 2011), 4(3) *Public Health Ethics* 226; Graeme Laurie et al., 'A Review of evidence relating to harm resulting from uses of health and biomedical data' (30 June 2014), Nuffield Council on Bioethics.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

An authoritative clarification of this uncertainty is therefore necessary. It would either find that this form of consent is not permitted by the GDPR, or that it is but under specific conditions. Such conditions could for example include that the controller who collected the data must pass certain obligations (such as a restriction of possible purposes of processing) contractually to the recipients of data, in the same way that controllers do with processors. It could also require the implementation of adequate technical and organisational measures to guarantee that data subjects can exercise all their rights. Examples for such measures are dashboards that create transparency to data subjects about who processes their data for what purposes, or technical propagation mechanisms in support of withdrawal of consent or invocation of specific data subject rights⁴⁹.

2.2.2 Issue

It remains unclear whether the GDPR permits to ask consent for the processing of a yet unknown future recipient of the data. If permissible, such consent would provide a possible legal basis for the processing by a recipient. Clarification of this issue is necessary for a better understanding of the options of how to operationalise the vision of markets and commons of personal data and the open sharing of research data as foreseen in the European data strategy⁵⁰.

2.2.3 Relevance & Impact on ICT Research and Innovation

The issue raised is directly pertinent to the implementation of the European data strategy whenever personal data are involved. It is of particular importance in health science that currently has a strong reliance on consent⁵¹ but also in human sciences and research and innovation where open access to research data is a key strategy.

⁴⁹ Note that PANELFIT has already conducted research on possible such conditions. The current status is documented in an internal document titled “Transferrable Consent”.

⁵⁰ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (last visited 9/4/2020)

⁵¹ See: EDPS, A Preliminary Opinion on data protection and scientific research, above.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

The requested clarification provides important guidance on whether consent is a possible legal basis for the implementation of a wide range of initiatives in the context of the data strategy.

Without such guidance, there is a high risk that the following situations occur:

- Significant investments in implementations based on such consent are lost because it is later found to be legally invalid;
- Investments are made in less suited alternative legal bases that result in reduced efficiency and competitiveness since consent is considered excessively risky;
- Investments in data initiatives are cancelled or postponed due to a too high perceived business risk.

2.2.4 Mitigation Measures

This issue may be resolved and its related risks averted by an authoritative interpretation of the GDPR by the EDPB. The cost of such a clarification is very low, particularly compared to the positive impact on the free movement of personal data in the Union.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.3 Unclarities with Regards to shared Controllership

2.3.1 Context and Legal Background

The GDPR defines four different roles: Data subject, data controller, data processor, and joint controller. While clearly every natural person is a data subject⁵², the role of a data controller, data processor, or joint controller cannot be assigned as easily. According to Art. 4(7) GDPR a **data controller** is defined as “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”. Consequently, **joint controllers** are “two or more controllers jointly [determining] the purposes and means of processing”⁵³. In contrast to this, a **data processor** is “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”⁵⁴. Thus, the difference between controller and processor lays primarily in who is responsible for taking the decisions about what is happening with the personal data. The differentiation of these roles is essential as they come with different obligations. The opacity of the flow of data within research projects that may interact with other institutions, organisations, and services that are involved in processing the data hinder a clear distinction of roles in reality. Additionally, several issues have been identified that may be solved through clarifications in the legal framework.

2.3.2 Issue 1: Processor or controller?

It is unclear when exactly a processor becomes a controller. As most currently existing systems incorporate third-party services processing personal data (e.g. for analytics), it is not easy to determine who is a data controller and who is a data processor. Following the case of Google Spain⁵⁵ the European Court of Justice is executing a much wider interpretation of controllership as previously thought⁵⁶. In this case, Google was – other than before – classified as a data

⁵² Art. 4(1) GDPR

⁵³ Art. 26(1) GDPR

⁵⁴ Art. 26(1) GDPR

⁵⁵ C-131/12: Google Spain v AEPD and Mario Costeja Gonzalez

⁵⁶ Mahieu, R., van Hoboken, J., & Asghari, H. (2019). Responsibility for Data Protection in a Networked World – On the Question of the Controller, ‘Effective and Complete Protection’ and Its Application to Data Access Rights in Europe (SSRN Scholarly Paper No. ID 3256743). Retrieved from Social Science Research Network website: <https://papers.ssrn.com/abstract=3256743>



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

controller as the search engine operator determines the purposes of the search engine and is therefore responsible for processing that it carries out of personal data. It can be concluded that “any actor who has a purpose for a data processing operation, and can directly influence that processing, can be considered a data controller”⁵⁷. However, it is unclear under what circumstances are “... two or more controllers jointly [determining] the purposes and means of processing”⁵⁸. Past cases on this matter demonstrated that the scope of joint controllership is not easily determined.

2.3.3 Relevance & Impact on ICT Research and Innovation

The risk is that data controllers are not aware of being such – or simply neglect it. As explained above, this could also be the case if a data processor is not aware that they are also data controllers. As a consequence, a clear distribution of responsibility and liabilities between the joint controllers cannot be undertaken. If no strict prosecution of this will take place, the law will lose credibility and will be perceived as an optimum to strive for, rather than a real obligation.

In research this is a general problem for instance when students collect data for their research. Is the student a joint controller with the faculty or chair supervising the research (e.g., a thesis) or rather a processor? The latter is certainly preferable to ensure that all the obligations of the GDPR can be met. However, frequently students are not sufficiently advised in data protection measures and therefore often collect data on their own, indicating only their personal (possibly university) email address. From the perspective of the participants of the study, the student would consequently be regarded as the controller. This becomes particularly problematic with regards to data subject rights. For instance, participants could decide years later that they want to withdraw their consent to the usage of their material. If the student does not forward the request to the institution, or if the student has changed his or her email address, it cannot be fulfilled and the obligations of the GDPR are not met. Now, can the student be held liable as data controller?

For the concrete case of a researcher wanting to license access to his or her data, the foremost problem is to understand that third parties that obtain access to the data can be considered as

⁵⁷ *ibid.*, p. 85

⁵⁸ Art. 26 (1) GDPR



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

joint controllers, and that the responsibility for the data is shared during the process. However, as the Google Spain case⁵⁹ showed, the determination of whether the recipient is a joint controller or a processor is less than trivial. As this has a major impact on the obligations and expectations by the GDPR, it constitutes a difficult impediment for researchers who may want to share their data and/or use the opportunity to raise funds for their research.

2.3.4 Mitigation Measures

This issue may be resolved and its related risks averted by an authoritative interpretation of the GDPR. The cost of such a clarification is very low. The Opinion 1/2020, on the concepts of "controller" and "processor" by the Article 29 Data Protection working party, might simply be updated by the EDPB. Furthermore, awareness about the associated obligations must be raised among researchers who collect (or supervise the collection) and grant access to personal data. For researchers and organisations, contracts provide an opportunity to clarify the rights and obligations of every party in the processing of data.

2.3.5 Issue 2: Joint controllership

In the case of a joint controllership a series of questions arises: When is the responsibility handed over? Who is liable for upholding the accuracy? What happens if the data is transferred to another controller and anonymisation is broken? It is uncontested that the controllers do not need to allocate responsibility and obligations equally as long as all obligations are met⁶⁰.

However, what is unclear are the legal consequences of not suitably arranging responsibility and obligations among joint controllers and what minimum responsibilities and obligations must be fulfilled if a cooperation is impossible⁶¹. This means that GDPR does not express legal consequences of joint controllers failing to fulfil their obligations towards data subjects. This issue has high relevance as the exact data flows can be unclear to involved parties, particularly in the case of power asymmetries between them.

⁵⁹ C-131/12: Google Spain v AEPD and Mario Costeja Gonzalez

⁶⁰ Mahieu et al., 2019, p. 90

⁶¹ *ibid.*



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.3.6 Relevance & Impact on ICT Research and Innovation

For research this issue is for instance relevant in the previously mentioned case of students collecting personal data. If the compliance with the GDPR (i.e. data subjects rights) cannot be guaranteed, who is made responsible? What are the legal consequences for both parties, student and supervising institution?

In the context of commercialisation of data, the issue is particularly risky. If a researcher sells or licenses access to a database and an infringement is discovered in the original dataset, all partners will be held liable. Good faith will not protect the recipient of the data. Thus, how can a recipient of a database be sure that there has not been an infringement? And how can the researcher ensure a lawful processing of the data by the licensee? Consequently, by licensing a database, the licensor automatically takes a much higher risk upon him- or herself. This again impedes the possibility of licensing the data as researchers will hesitate to incur a legal dependency on further situations they cannot control. This is especially risky as, in principle, every joint controller is liable for the entire damage that a data subject suffers (Art. 82(4) GDPR), even if the joint controllers arranged appropriate division of responsibility among each other⁶².

2.3.7 Mitigation Measures

This issue may be resolved, and its related risks averted by an authoritative clarification of the GDPR. Hereby, it has to be clarified which exact rights and obligations exist in a joint controllership for every controller involved.

For researchers in ICT in the case of joint controllership, standard agreements and contracts provide a solution to overcome this issue without the help of clarification through improvements in the GDPR. These contracts are to state the duties and obligations of all individual controllers. The State Commissioner for Data Protection and Freedom of Information in Baden-Württemberg (LfDI), Germany for instance has provided a first sample

⁶² Van Alsenoy, B. (2016). Liability under EU data protection law: From directive 95/46 to the general data protection regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 7(3), 271.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

of such an agreement for joint controllers under special consideration of Art. 26(1) GDPR⁶³. Furthermore, another agreement relating to the fulfilment of the obligation to inform the data subjects in accordance with Art. 26(2) GDPR was also provided and is available online⁶⁴. Such an agreement should state the reasons and scope of the shared responsibility and should clearly define the responsibilities of the individual controllers in different stages of an activity that is to be carried out. Additionally, the agreement should state with which party data subjects may invoke their data protection rights, where they receive information from and from which controller they may assert their rights. This ensures transparency for the data subject.

2.3.8 Issue 3: Data subject and controller?

As detailed before, a data subject is any natural person, and Recital 18 of the GDPR clearly states that the regulation “does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity”. Thus, it seems clear: In the case of a data subject who owns a website to share pictures with his/her family living in another country, he/she is not considered as a data controller, but merely as a data subject. This holds even if he/she is collecting personal data for instance by collecting the IP-address of visitors, or applying analytics. However, the role of the data subject will change, if he/she incorporates for instance advertisement banners or affiliate links in his/her website. In this case he/she is not only pursuing a “purely personal or household activity”, but also a commercial objective.

Yet, the case of *Wirtschaftsakademie*⁶⁵ illustrates that the line to becoming a data controller is very thin. Here the *Wirtschaftsakademie Schleswig-Holstein*, a business academy, who was running a Facebook fan page, was considered of being a joint controller together with Facebook as “creating such a [fan] page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page” and enables the administrator of the fan page to request for “data which tell the fan page administrator where to make special offers and

⁶³ See LfDI Baden-Württemberg, 2019 for two templates of joint controllership agreements. Please note that the templates are provided only in German. Available at: <https://www.baden-wuerttemberg.datenschutz.de/mehr-licht-gemeinsame-verantwortlichkeit-sinnvoll-gestalten/>

⁶⁴ *ibid.*

⁶⁵ Case C-210/16: *Wirtschaftsakademie Schleswig-Holstein GmbH v Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

where to organise events, and more generally enable it to target best the information it offers”⁶⁶. As data subjects increasingly use the Internet not only to passively consume and obtain information, but to actively generate and produce content, the question on how quickly a data subject can become a data controller will gain importance.

2.3.9 Relevance & Impact on ICT Research and Innovation

The risk is that data subjects are not aware of being a data controller – or simply neglect it – and are thus not aware of their obligations and responsibilities. If no strict prosecution of infringements will take place, the law will lose credibility and will be perceived as an optimum to strive for, rather than a real obligation.

For research and innovation this issue gains importance when research includes new technologies such as Internet of things (IoT) devices. If the data of an IoT-device is collected, researchers must be aware that they will not only collect the data of the device owner, but possibly also from other people. For instance, a voice control assistant may not only be used by a single person – the owner – but by all people living in the same household or potential visitors of the device owner. Consequently, researchers are running the risk of not being aware that they will become joint controllers together with the device owner. This means not only that consent from other people than the device owner might be required, but also that the researcher will share obligations and responsibility with the device owner. Consequently, in the event that the device owner act against the will of the other IoT device users, the researchers will be held liable, too.

Clearly, it was not the intention of the GDPR to determine that private individuals, that for instance own IoT devices become data controllers themselves. Instead, the regulation likely did not foresee the increased usage of such devices, together with an increase of new technologies such as IoT or Artificial Intelligence (AI) that lead to such special cases. The uncertainty whether a data subject can and should become a data controller under the consideration of new technologies and use cases that may lead to such an outcome is therefore problematic.

⁶⁶ *ibid.*



2.3.10 Mitigation Measures

This issue may be resolved by an authoritative interpretation of the GDPR by the EDPB, declaring when exactly a data subject becomes a data controller. The cost of such a clarification is very low. With regards to researcher's unawareness of being joint controllers, educational advertising is required. Until then, standard agreements may be used to determine the obligations and responsibilities of data controllers. These contracts should also clarify the flow of data in the specific use case, enhancing transparency for both data controller and data subject.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.4 Determination of the Value of Data

2.4.1 Context and Legal Background

In the wake of big data, data markets, data commercialisation and the ensuing commodification of digital identities have become an emergent reality. Governing big data so as to realise its beneficial economic potential⁶⁷ while also empowering individuals⁶⁸ is a formidable legislative and regulative challenge policymakers face. Addressing this challenge presupposes the determination of value of data not only in qualitative (i.e. the different potential uses of data) but also in quantitative (i.e. monetary) terms in order to enable pricing mechanisms to support the governance architecture.

According to Art. 8(1) of the Charter of Fundamental Rights of the European Union and Art. 16(1) of the Treaty on the Functioning of the European Union, both of which are explicitly mentioned in Recital 1 of the GDPR, in the EU personal data protection constitutes a fundamental right. This approach to informational privacy accentuates the enormous qualitative value typically assigned to personal data. By contrast, extant legislation offers no guidance on how to determine the monetary value of data, although the recent Directive on certain aspects concerning contracts for the supply of digital content and digital services (2019/770) gingerly accepts that personal data can be used to pay for digital services⁶⁹ (see especially Art. 2(7) and Art. 3(1) as well as the chapter on ‘Data Commercialisation and Counter-Performance Practices’ above).

Researchers collect, process, store and share ever more data in order to move frontiers of knowledge and to develop new products and services. The role of big data in R&I is substantial and will increase further. Therefore, the R&I sector is directly affected by gaps and issues related to the value of data. Pricing and monetarisation of data, for instance, have an impact on the resources needed for data collection and the added value created by data analytics. The

⁶⁷ See e.g. World Economic Forum (2011): *Personal data: The emergence of a new asset class*. Davos. Available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (accessed 20 September 2019)

⁶⁸ See Malgieri, Gianclaudio and Custers, Bart (2018): Pricing Privacy – the right to know the value of your personal data. In: *Computer Law and Security Review*, 34, 289-303. Available at: <https://doi.org/10.1016/j.clsr.2017.08.006>

⁶⁹ Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770&from=EN>



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

absence of fair data markets disincentives researchers and innovators from small and medium size research institutions and enterprises in ICT because they often lack access to highly valuable datasets controlled by rather few big players. However, personal data are non-rival, cheap to produce, cheap to copy, cheap to transmit and highly diverse. Hence, data resemble free commons rather than typical commodities. All this hinders the application of traditional categories of patrimonial law.

Moreover, citizens are unaware of the real value of their personal data which hampers the growth of citizen science, increasingly considered an indispensable component to master the challenges of technological progress.

2.4.2 Gap

There is no established pricing mechanism for data.

Apart from data pricing, the consideration of data as a valuable asset is gaining strength, even from the point of view of the data subject. A proof of this is the fine to Facebook for misleading advertising by the Hungarian Competition Authority in 2019⁷⁰. Until August 2019, Facebook's main page said "Join. It's free and it will always be"; now it reads "Join. It's quick and easy". Facebook was fined for "misleading advertising", demonstrating that Facebook has never been free since data was given in exchange for the service that users receive. So, even if it is difficult to establish pricing mechanisms for data, the notion that personal data have economic value and, at least, when personal data is given in exchange for services those services should not be qualified as "free".

2.4.3 Relevance & Impact on ICT Research and Innovation

Regulating data markets risks hampering innovation based on the unrestricted flow of data, yet affords the opportunity to create a legal infrastructure that dissolves legal grey areas and permits fair data commercialisation. Adequately regulated markets for personal data "would need to rely on legal frameworks that establish alienability, rivalry, and excludability for personal data, and assign initial ownership to an entity such as the data subject⁷¹", which presupposes asset

⁷⁰ See <https://www.businessinsider.com/hungary-competition-authority-fines-facebook-4-million-2019-12?IR=T>.

⁷¹ Spiekermann, Sarah; Acquisti, Alessandro; Böhme, Rainer and Hui, Kai-Lung (2015): The challenges of personal data markets and privacy. In: *Electronic Markets*, 25, 161-167. p.162.163 Available at: <https://doi.org/10.1007/s12525-015-0191-0>



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

rights, institutions, sanctions and technology to interact coherently. Unless data is recognised as a unique asset class and duly regulated, research will suffer from uncertainty, which may slow innovation.

Furthermore, isolated pieces of data are relatively worthless in monetary terms, whereas datasets and dataset-based insights can have enormous value and facilitate new discoveries as well as the development of new products or services. Phrased differently, the value of data depends on the trajectory of their life-cycle and their position within the wider data ecosystem. Single pieces of data yield little innovative potential, but may be of use for advertising, whereas insights derived from large datasets often are key drivers of innovation.

However, whether or not data will eventually yield insights remains unknown during the data collection and aggregation phases so that accurately determining the value of data before their actual use is very difficult. This problem is particularly pronounced in R&I because the course of research is often hard to predict and outcomes difficult to anticipate. Hence, whether or not data will eventually become valuable often is unknown at the beginning of a project.

2.4.4 Mitigation Measures

There is considerable epistemic uncertainty about how to best devise pricing mechanisms for personal data, should it be decided that personal data can indeed be commercialised. In general, “[a]ttaching a monetary value to personal data requires some clarity on (1) how to express monetary value, (2) which object is actually being priced, and (3) and how to attach value to the object, i.e. the actual pricing system.”⁷² With regard to the expression of value, it seems recommendable to express value in Euros (or some other currency) per month and per person in order to account for the facts that personal data tend to change as time progresses and that reuse is very easy.⁷³ Important pricing factors are the completeness, accuracy and up-to-date status of datasets, the relative rarity and uniqueness of data, and their level of identifiability.⁷⁴ With regard to the pricing system, two possible approaches can be distinguished: market valuation methods and individual valuation methods. The former focus on financial results for data records, market prices for data, costs of data breaches and data prices in illegal markets.

⁷² Malgieri, G., & Custers, B. (2018). Pricing privacy—the right to know the value of your personal data. *Computer Law & Security Review*, 34(2), 289-303.

⁷³ Ibid., 295

⁷⁴ Ibid., 295-296



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

The latter focus on survey and experimental results and the willingness of users to pay for data protection⁷⁵, that is to prefer products and services that provide privacy sensitive options or are produced under principles of privacy by design and privacy by default. Both approaches remain incomplete as market valuation methods rely on indicators that are insufficiently precise while individual valuation methods are not incentive compatible.

In order to overcome this epistemic uncertainty more research investigating possible pricing mechanisms is clearly needed so as to better inform subsequent policymaking. However, especially balancing legitimate data protection concerns and business interests might be difficult and may lead to political conflict. Consequently, all policies aiming at erecting fair data markets should constantly be evaluated, with evaluation measures including a diverse range of stakeholders. Funding research on pricing mechanisms could be a promising venue to harness the knowledge and competency of researchers and would, moreover, increase the likelihood of finding research-friendly solutions. Specifying the exact value of data in advance will probably remain impossible, especially because the relative value of data within the data ecosystem will continue to change. It seems likely, for example, that data analysis will become more valuable, whereas data collection will become less valuable due to the continuously increasing supply of data and new ICTs that simplify data collection. Thus, the most probable and promising route would aim at developing adequate proxies and indicators that allow for an approximation of the data's value. Such proxies would also facilitate recognising the innovative potential of a research project at an early stage and support innovation management. Renewed legislation could provide examples and frameworks for measuring the value of data in order to compensate data subjects.

⁷⁵ Ibid., 296. The pricing systems are elaborated in detail in OECD (2013): Exploring the economics of personal data: A survey of methodologies for measuring monetary value. In: *OECD digital economy papers*. Paris: OECD. Available at: <https://doi.org/10.1787/5k486qtxldmq-en>



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

2.5 Management of Individual Privacy Preferences

2.5.1 Context and Legal Background

When processing of personal data is based on consent according to Art. 6(1)(a) GDPR, certain requirements set out in Art. 7 as well as Recitals 32, 42 and 43, need to be fulfilled. Among others, it is stated that the requirement of freely given consent is not satisfied “if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment” (Recital 42 GDPR). In practice, far too often, this requirement is not met. This is also a problem for data controllers, since the consent for data processing will always be precarious. For instance, requests for consent for setting cookies often use banners with the only option of being ‘accept’. Sometimes the cookies are even already set when loading the page – before requesting consent to do so⁷⁶. Similarly, companies oftentimes have a clear preference for the outcome and employ nudging to steer the users’ decision⁷⁷. For instance, organisations may threaten users with a loss of functionality if they do not consent to a privacy intrusive option or hide privacy-friendly options. At the same time, different users have widely diverging preferences on how much information they are willing to reveal and what degree of privacy protection they would like to have⁷⁸. Accommodating these different needs by offering diversified options is particularly relevant in the case of sensitive data for instance in a setting of medical research. Other requirements for consent are stated in Recital 32 GDPR, namely that it must be freely given, specific, and informed through an unambiguous indication of the data subject’s agreement. Yet, even if controllers satisfy these requirements, research has shown that data subjects have difficulties to assess terms and conditions and privacy policies. The presumably most common problem is that data subjects rarely read them. However, even if they are read, data subjects often lack the legal and technical expertise to correctly understand the implications

⁷⁶ GDPR Consent Examples. (2019). Retrieved September 16, 2019, from PrivacyPolicies.com Blog website: <https://www.privacypolicies.com/blog/gdpr-consent-examples/>

⁷⁷ Report: Deceived by design. (2018). Forbrukerrådet. Retrieved September 17, 2019, from <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/>

⁷⁸ Olavsrud, T. (2016). Carnegie Mellon University helps you control your privacy. Retrieved September 16, 2019, from CIO website: <https://www.cio.com/article/3117626/carnegie-mellon-university-helps-you-control-your-privacy.html>



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

of what is written⁷⁹. Furthermore, they are confronted with such an immense number of privacy decisions to take, that they often suffer from what is called ‘consent fatigue’⁸⁰.

Finally, requirements set in Recital 43 are not met either. According to the Recital, consent “is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance”. These requirements are frequently unfulfilled, which means that consent for data processing is not freely given. For example, when an online diary requires consent for cookies in order to allow a reader to consult the articles and content of the diary, or the more and more frequent “freemium versions”. The freemium versions of online diaries require the reader to register in order to read the whole diary or some specific articles. This, using words of Recital 43 GDPR, makes the performance of a service or delivery of a digital content (the article in the online diary) dependent on the consent for data processing and, hence, makes the consent to be not freely given.

There exist different approaches which attempt to overcome these difficulties. One of them, the Platform for privacy preferences project (P3P), was launched in 2002 by the World Wide Web Consortium⁸¹. P3P operates with machine-readable descriptions of data practices. If a site implements such a description, smart interfaces in browsers can help users in understanding the privacy practices and enable them to automate decisions about them⁸². This way, users do not have to read all the privacy policies and can instead delegate it to a P3P user agent that implements their privacy preferences. Unfortunately, many website operators have proved to be reluctant to embrace this new standard and as no legal requirement to implement P3P was introduced, P3P lacked market acceptance in the end⁸³ and the project was stopped in 2006⁸⁴. Since then, researchers have continued to try to implement similar solutions for end users to let them manage their privacy preferences. For instance, the Personalised Privacy Assistant

⁷⁹ Solove, D. J. (2012). Privacy Self-Management and the Consent Dilemma (SSRN Scholarly Paper No. ID 2171018). Retrieved from Social Science Research Network website: <https://papers.ssrn.com/abstract=2171018>

⁸⁰ *ibid.*

⁸¹ P3P: The Platform for Privacy Preferences, (2018). Retrieved September 17, 2019, from <https://www.w3.org/P3P/>

⁸² *ibid.*

⁸³ Olavsrud, 2016

⁸⁴ See www.w3.org. 2018.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Project⁸⁵ envisions intelligent agents that learn about the privacy preferences of their users to automatically apply them. Similar to the P3P, the project follows the approach to ask resource owners to provide their privacy practices in a machine-readable way on a voluntary basis. However, as the experiences with the P3P has shown, this can only be successful if a legal obligation for resource owners to implement a certain standard exists.

2.5.2 Gap

Data subjects need to have a real choice about whether they want to share their data and to what extent. Due to the high number of services used, a system to manage individual privacy preferences is required. Realistically, a standard for the provision of privacy practices in a machine-readable format, which is necessary for such a system, needs to be determined. Furthermore, in order to gain market acceptance and have a real impact it needs to be mandatory for resource owners to implement this standard.

2.5.3 Relevance & Impact on ICT Research and Innovation

The risk in this issue lays in staying inactive. Already now users suffer from consent fatigue and often agree to whatever is presented to them. The number of people reading the privacy practices is limited. Consequently, it cannot be expected that users will or can realistically protect them by themselves. At the same time, service providers have little incentive to implement privacy-friendly settings. Consequently, governmental intervention is advisable. Although the GDPR already introduced the principle of privacy by design and default, this is not enough. For instance, a study by the Norwegian Consumer Protection Agency⁸⁶ showed that Facebook and Google use compelling wordings for certain privacy protecting choices and make users go through a significantly longer process if they choose more privacy-friendly settings. At some points, they even threaten with a loss of functionality or the deletion of the user account if the privacy intrusive option is not chosen.

For research and innovation, the introduction of a system for the management of individual privacy preferences, would bring different advantages. Firstly, researchers could focus on the critical privacy aspects of their study and ask participants about these. As participants would

⁸⁵ Personalized Privacy Assistant Project. (n.d.). Retrieved September 24, 2019, from <https://privacyassistant.org/>

⁸⁶ Forbrukerrådet, 2018



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

not have to go through all obvious choices (according to their preferences), researchers could present the critical aspects more thoroughly. In doing so, they could make sure that participants really understand the impact of their choices and reduce the risk of belated complaints. This is particularly relevant in the context of a future sharing or even commercialisation of the data. As this is a very critical aspect in research, data subjects are likely in having varying opinions about it. The opportunity to further explain the details and/or the necessity of these practices – without the data subjects being overwhelmed by a waste amount of other (rather uncritical) explanations – would enhance the chances that participants actually do agree.

Naturally, for participants the risk of missing the important points is reduced likewise. Furthermore, such a system reduces the time that is needed for one participant to go through the study. As time is a critical factor not only for the willingness for participating in research, but also for the researchers themselves, this can be beneficial for research in two ways.

2.5.4 Mitigation Measures

The P3P demonstrates a first attempt to solve this problem by providing a platform to standardise privacy preferences. However, the P3P has shown that the advantages of this self-disclosure for the organisation, such as a reliable prediction of how a website will be presented to the user, are not sufficient for such a tool to succeed. Organisations did not adopt this standard as it comes with obvious disadvantages for them. Similarly, several projects and tools exist that help individuals protect their privacy but are not widely known and used by individuals. Through the GDPR, individuals have already become more aware about privacy as they see cookie policies and consent pop-ups. Now, to counteract consent fatigue, measures need to be taken that ensure that individuals are able to manage their privacy preferences in general, not for every website, tool, platform or other service individually.

The Mitigation Measure of choice is therefore to introduce an incentive system for resource owners to provide their privacy practice in a machine-readable format and for Browsers, IoT and other platforms to provide an interface for users. For this a suitable standard is required that organisations need to comply with. Therefore, a new legislation needs to be passed. Although, the costs in doing this seem high, the expected impact for data subjects and their rights is tremendous.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

3 Conclusion

The aim of this document was to highlight recent and important issues and gaps in the current legislation with regards to the commercialisation of data. The issues and gaps were identified through an expert workshop and later refined through several rounds of feedback. The legal background and relevance of the issues and gaps for ICT research have been discussed. To solve the identified problems, mitigation measures have been proposed.

The first issue identified relates to the question whether counter-performance practises, the monetisation of data in exchange for services, is lawful. This prevents not only the emergence of markets and commons of personal data, but also the development of new services, making an official position by legislators necessary.

The second issue demonstrated that it is unclear whether a primary controller can collect consent for a yet unidentified recipient. Without clarification by the EDPB, research and innovation based on consent, for instance in health science or open access research, is restrained.

Multiple unclarities with regards to shared controllership have been discussed. It has to be determined when and under what conditions a processor becomes a (joint) controller, how rights and responsibilities are shared in a joint controllership and whether data subjects can and should become data controllers. Until the issues are clarified through an authoritative interpretation of the GDPR, contracts and agreements may be utilised between (joint) controllers and processors to determine rights and responsibilities.

The lack of an established pricing mechanism for data was established as a gap in the current regulation. Determining the value of data is necessary in order to achieve a fair and transparent commercialisation of data and the development of regulated data markets. Research on suitable pricing mechanism is required to overcome this gap.

Lastly, the lack of a standard for the provision of privacy practices, possibly in a machine-readable format, is necessary to develop systems that give individuals the opportunity to effectively manage privacy preferences. The development and implementation of such a standard through research projects would counteract consent fatigue and would benefit data subjects and ICT researchers alike.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Appendix

1. Workshop Concept
2. List of experts



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Participatory Approaches to a New Ethical and Legal Framework for ICT

Workshop on Data Commercialization

3 June 2019, University of the Basque Country, Bilbao

A workshop of WP3 “Commercialization of Data” organized by Goethe University Frankfurt

Session 1: Ownership of Data

When a data subject participates in a survey or experiment this poses the question to whom the obtained data belongs. The same questions arise when personal data is used as input for new ICT products and services. Does there exist something like “ownership” of data? In this session alternative concepts will be explored and the obligations of data processors discussed.

Session 2: Usage of External Databases

Purchasing external databases may come with a series of questions both in scientific and commercial application scenarios. Is it at all legal? What regulation is applicable? Can I be held liable if data subjects had not given their consent? These and similar questions will be examined in the second session.

Session 3: Monetising Internal Databases

If the effort of creating a new database is taken, one may ask whether and how the collected data can be monetized? What rights do the data subjects have in these regards? How can they be compensated? In this session issues about selling databases will be explored.

Session 4: Good Commercialization Governance

A good governance for the commercialization of data in research and innovation is strictly necessary. But what exactly is good governance? Can regulation, ethics committees or community representations enhance the governance? What is needed for good governance? These questions will be discussed in session 4.



Participants

Richard Sawhney, *Dawex - Global data marketplace*

Vice president and data exchange advisor of Dawex, a Global Data Marketplace. Dawex is a leading data exchange technology company and the operator of the largest global data marketplace. With Dawex technology organisations orchestrate data circulation by sourcing, monetising and exchanging data directly without intermediary, securely, efficiently and in full compliance with regulations leveraging the blockchain technology to ensure the integrity of licensing contracts.

Francisco de Luna, *CNIO - Spanish national biobank network*

Has worked in one of the most important biobanks in Spain for a long time and will be able to tell us about the way in which biobanks gain funding by providing samples, data or similar to third parties. Has a PhD in biochemistry and molecular biology from the Universidad Autónoma de Madrid.

Rebekka Weiß, *Bitkom - Germany's digital association*


Is the Head of Trust & Security at Bitkom e.V and has a Master of Laws in Intellectual Property and the Digital Economy (LL.M.) of the University of Glasgow. Interested in privacy, consumer protection, competition law, Trust Services and IT Security, Data Economics, and legal and economic questions on the digital economy.

Jaana Sinipuro, *Sitra - Finnish Innovation Fund*

Is an experienced ICT professional who works as Project Director responsible for the IHAN® – Human-driven data economy focus area and also sees to the final stages of the Digital Health HUB projects. She is an accountancy professional and has worked in consulting, sales and sales support in an international company in the software industry and has more than 17 years' experience in analytics, big data and business intelligence.

Jose Castillo Parrilla, *University of Granada*





Spanish postdoc who wrote for his PhD an in-depth analysis of the legal, fiscal and criminal challenges of building this Digital Single Market in Europe, within the milestones of the European Union's Digital Agenda for Europe 2020 programme.

Mateja Durovik, *King's College London*

Is a Lecturer in Contract and Commercial Law, having joined the Dickson Poon School of Law in July 2017. Worked for the Legal Service of the European Commission, as well as a consultant for the European Commission, BEUC (European Consumer Organisation) and the United Nations.

Gemma Minero, *Universidad Autonoma de Madrid*

Her research is focused on IP rights and new technologies, in particular, software, databases and technological measures. Prof. Dr. D. Rodrigo Bercovitz Rodríguez-Cano was the director of her thesis, on IP protection of databases. She has published works on personal data protection, protection of consumers and protection of disability.

Bart van der Sloot, *Tilburg University*

Specializes in the field of Privacy and Big Data. He publishes regularly on the liability of internet intermediaries, data protection and internet regulation. He works as a senior researcher at the Tilburg Institute for Law, Technology, and Society, Tilburg University, and is the General Editor of the European Data Protection Law Review, the coordinator of the Amsterdam Platform for Privacy Research and the scientific director of the Privacy and Identity Lab.

