Department of Economics and Finance

Course of Economics and Finance with major in Economics

Chair of Experimental and Behavioral Economics

Consumers' Willingness to Share Personal Health Data within the EU

SUPERVISOR

Prof. Di Cagno, Daniela Teresa

CO - SUPERVISOR

Prof. Campioni, Eloisa

CANDIDATE

Virginia Poliseno

762281

ACADEMIC YEAR 2023/2024

Abstract

One of the latest goals of the European Union is to create a single market for data as part of its plan to transform the EU into a data-driven society. This goal is being pursued through the creation of several data spaces in the main economic sectors and public domains. One of the priority areas under this framework is the health sector. For this reason, in 2022, the European Commission presented a proposal for the European Health Data Space. This framework encourages the development of a cohesive European health system. In order to achieve this, it is fundamental that individuals trust national and European institutions and that they are willing to share their personal health data with these recipients. In that context, this thesis aims at better understanding people's willingness to share their personal health information with different recipients. In order to fully understand this, the work first addresses the legislative landscape of the main health data legislation. Then, it examines the main experiments and surveys related to the topic, while highlighting both the benefits of sharing data and the concerns that people may have. Finally, in the last chapter, it presents the results of a survey that has been conducted with the aim of better understanding people's propensity to share personal health data. The survey obtained 197 valid answers, and it was found that the majority of the participants were willing to share their personal health data with healthcare providers. However, the number of participants willing to share such information with other recipients (i.e. researchers, friends, and the government) decreased. This could present a problem for the correct implementation of the EHDS since one of its key elements is the creation of national Health Data Access Bodies to manage data sharing.

List of Abbreviations

AI	Artificial Intelligence
DPO	Data Protection Officer
EHDS	European Health Data Space
ECHR	European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation
HDABs	Health Data Access Bodies
HR	Human Rights
ICTs	Information & Communication Technologies
MS	Member States
NGO	Non-Governmental Organization
STDs	Sexually transmitted diseases
US	United States
VIPs	Very Important Peoples

Index

INTRODUCTION 5

CHAPTER I: LEGISLATIVE OVERVIEW AND MORE 8

European Convention on Human Rights 8

Data Protection Convention 10

European Data Protection Directive 11

General Data Protection Regulation 12

European Health Data Space 18

CHAPTER II: IN REALITY… 23

Benefits of sharing 23

Concerns about sharing 25

Factors influencing people's willingness to share: previous research and experiments 28

CHAPTER III: A SURVEY AND AN EXPERIMENT 33

Trust Game 33

Public Good Game 36

Survey: results and future research 37

An experiment 45

CONCLUSION 48

BIBLIOGRAPHY 53

APPENDIX 59

Introduction

In the last few decades, there have been numerous technological developments. This phenomenon has led to an increase in the number of people having access to the internet, and, as a consequence, to the digitalization of societies.

In order to keep up with these rapid developments, the European Union has decided to undertake a digital transformation. The foundations of this transition date back to the 1990s. In fact, the EU recognized early on that Information and Communication Technologies (ICTs) would play a fundamental role in economic and societal development. For this reason, it started implementing policies to promote ICTs since the beginning.

Over the decades, the EU has designed many legislation to promote and improve technological advancement across the region.

Fast forward to today, the European Union aims to create a "genuine single market for data" as part of its plan to transform the EU into a data-driven society. This objective is being achieved through the European Data Strategy, which is a framework aimed at making the European Union a global leader in the digital age. As highlighted by the European Parliament, "*the EU wants to strengthen its digital sovereignty and set standards, rather than follow standards set by others*".

Furthermore, the European Data Strategy is based on three main pillars:

- The implementation of data-sharing services and technologies to enable the gathering, processing, and exchange of data among several organizations.
- Include data governance frameworks that provide the rights to access and process data in a transparent and equitable manner that is compliant with applicable EU legislation.
- Enhance data accessibility, quality, and interoperability within and between sectors as well as in domain-specific contexts.

As a consequence, to achieve a single market for data, the EU wants to create several data spaces in the main economic sectors and public domains. The objective is to increase and facilitate data sharing in important social, scientific, and economic areas (Quinn et al., 2024).

It is also important to note that one of the priority areas under the European Data Strategy is the health sector. Indeed, in 2022, the European Commission presented a proposal for the European Health Data Space (EHDS). This framework addresses the complexity of existing EU regulations on health data sharing, and it promotes digital health services across the region. Furthermore, it encourages the development of a cohesive European health system that would ensure a rapid answer to any future threats, would support medical research and innovation, and it would ensure better and cross-border healthcare for patients.

To better understand this new European Union framework, it is essential to first examine the historical context of data protection legislation in the region. Europe, and particularly the European Union, has a long-lasting history of data protection. The main legislative acts are the European Convention on Human Rights, the Data Protection Convention, the European Data Protection Directive, and the General Data Protection Regulation (GDPR).

The aim of these legislation is to regulate and facilitate the safe and efficient sharing of personal data within the EU. Among the aforementioned, the most significant is the GDPR. This regulation became applicable in 2018, and its only scope is personal data. It is a comprehensive regulation that governs the use, storage, and sharing of personal data within the EU.

Additionally, for a correct implementation of the EHDS framework, it is essential to understand people's willingness to share personal health information. It is, indeed, crucial to have insight into what data individuals are inclined to share and with whom.

The purpose of this thesis is precisely this. It aims to better understand people's propensity to share personal health data within the European Union. Specifically, it tries to determine whether individuals are more willing to share with certain recipients rather than others and whether they feel more comfortable sharing some categories of data over others. This analysis is done through a six-section survey. This survey has been shared via WhatsApp groups and Instagram stories, and it obtained 197 valid answers, which are analyzed in chapter 3 of the thesis.

Furthermore, to better comprehend the results of this survey, the thesis also provides background information on the sharing of personal health data. The first chapter analyses the main European legislation on the matter, which were previously mentioned. Then, in chapter 2, the main experiments related to the topic are analyzed. Additionally, chapter 2 highlights both the benefits of sharing data and the concerns that people may have. Finally, in the last chapter, alongside the aforementioned survey, the thesis first sets the context by exploring the concept of trust through two widely known games: the Trust Game and the Public Good Games. After that, it discusses an experiment that will be carried out in the upcoming months by Professor Di Cagno, Daniela, Professor Savona, Maria, and PhD candidate Lisovaia, Anastasiia.

Chapter I: Legislative overview and more

In order to protect individuals' privacy and their data, many measures have been put in place so far. This is particularly true when it comes to Europe and more specifically the European Union (EU). Indeed, there exists a long-standing history of data protection legislation in this region. For this reason, this first chapter will focus on the main legislative acts concerning data protection in the EU. More precisely, an emphasis will be placed on the acts that discuss health data protection, as they are the most relevant to the topic of this thesis.

European Convention on Human Rights

For a bit of history, the concept of data protection first appeared in Article 12 of the Universal Declaration of Human Rights in 1948. At first, it represented only a rather weak version of the idea. Therefore, in the following years, the Council of Europe decided to further deepen this concept in Article 8 of the European Convention on Human Rights (Hustinx P, 2014).

The convention was signed in Rome on the 4th of November 1950 by 12 Member States (MS) of the Council of Europe, and it entered into force on the 3rd of September 1953 (Council of Europe, n.d.a). As of today, it currently applies to all 46 MS of the Council, and it is enforced by The European Court of HR which is located in Strasbourg, France.

Going more into the details, the Convention does not only represent an important step in the field of data protection, but it also represents a groundbreaking development in the legislative world. In fact, it is the first treaty in the field of Human Rights to establish a dedicated supranational body to ensure that the signatory states fulfill their obligations[1]. According to the Convention, the treaty allows any individual, group of individuals, company, or Non-Governmental Organization (NGO) to appeal to the European Court of Human Rights (ECHR) if they think their rights have been violated. However, this can be done only after having exhausted all domestic remedies. As a result, this means that

[1] The very first treaty to establish a supranational organ was the Treaty of Versailles, which in 1919 founded the International Labour Organization.

decisions taken by national courts could be challenged by a supranational court. Thanks to this Convention, human rights had de facto gained precedence over national legislation and practice (Council of Europe, n.d.a). This means that if there were to be a conflict between a national law and the principles enshrined in the convention, the latter would take priority, reinforcing the importance and universality of human rights.

As already stated, when discussing data protection, the most important Article is the number 8, which reads as follows:

"*(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

As can be seen, the aim of this Article was to protect individuals from violations of their privacy by the government. In addition, as the second paragraph of the Article states, intervention from the government is only permitted by law and should be carried out with justification (Council of Europe, n.d.b).

Furthermore, the European Court of Human Rights has explained the scope and consequences of this protection in several different judgments. In these judgments, the court has taken into consideration three different aspects. The first one is whether there was an interference with the right to respect for private life. Secondly, whether this interference had an adequate, for example clear, accessible, foreseeable, legal basis. Lastly, it checks whether the interference was necessary and proportionate to the legitimate interests at stake. Moreover, the Court has also ruled that Article 8 could give rise to positive obligations for the MS. This means that they could be held liable for a breach of privacy committed by a private party. However, the cases regarding this matter are still limited. Therefore, ensuring the protection of personal data in horizontal relations is not a general obligation for MS (Hustinx P, 2014).

Data Protection Convention

Considering the many new developments in the use of information technology that took place in the early 1970s, the Council of Europe concluded that Article 8 of the European Convention on Human Rights had different shortcomings. This has led to the adoption of the Data Protection Convention, also commonly known as Convention 108. The Data Protection Convention was adopted in 1981 and was signed not only by the 47 MS of the Council of Europe but also by several countries outside the European border.

In the territory of the signature countries, the aim of this convention was to secure respect for every individual's rights and fundamental freedoms, and that, independently of their nationality or residence (Hustinx P, 2014).

Many years later, more precisely in 2018, the Protocol of Amendment to the Convention for the Protection of Personal Data was adopted. The aim of these amendments was to modernize the Convention, so it could tackle the new challenges of today's society (de Terwangne C, 2021). This update even granted it a new name, Convention 108+. However, despite these new amendments, the aim of the convention has not changed. Indeed, as stated in the Preamble of the amended version of the convention, the States recognize that "*it is necessary to promote at the global level the fundamental values of respect for privacy and protection of personal data, thereby contributing to the free flow of information between people*". According to the Convention, the notion of "personal data" includes "*any information relating to an identified or identifiable individual*". As it can be understood, such a notion covers any and all types of information (de Terwangne C, 2021).

Moreover, as one can see from the preamble just mentioned, the idea of Convention 108+ is to offer data protection to every individual, independent of their nationality or residence. For this reason, when defining the scope of application of the convention, it is referred to the concept of "jurisdiction" rather than "territory". Furthermore, the convention is applicable to all data processing activities, and it covers all fields of activity in which data processing is carried out. That means both in the public and the private sectors. An important exception of the Convention is that it "*does not apply to data processing carried out by a natural person in the course of purely personal or house-hold activities*" (de Terwangne C, 2021).

Finally, the Convention's most relevant part to the topic of this thesis can be found in Article 6. In this Article, the Convention identifies a list of special categories of personal data to which a higher level of protection is applied. These categories are justified by the risk of illegitimate discrimination linked to such data, and the serious risk of harm if this data is abused. More precisely, in the last point of the Article, the Convention mentions the processing of personal data that reveals information related to one's health as a special category. The process of such data is allowed only where and when there are appropriate safeguards that are incorporated in laws that complement the Convention (de Terwangne C, 2021). In this case and according to Article 60 of the Convention, information related to health includes "*information concerning the past, present, and future, physical or mental health of an individual, and which may refer to a person who is sick or healthy*". Furthermore, it is mentioned, in Article 59, that the processing of images intended to reveal health information, among other things, is considered as processing of sensitive data. However, this is not the case if such images are processed by a video surveillance system solely for security reasons in a shopping area for example (de Terwangne C, 2021).

European Data Protection Directive

Although the Council of Europe was successful in setting out the main elements of the legal framework when it comes to data protection rights, it was less successful when it came to ensuring sufficient consistency across its MS. Not only did some members implement the Convention late, but also the implementation of the Convention led to different outcomes among the Member States. As a result of this, there have been some cases of restrictions on data flows to other MS, which concerned the European Commission. As a consequence of this, at the end of 1990, it decided to submit a proposal for a Directive. The aim was to harmonize national laws regarding data protection in the private sector and most parts of the public sector too. The goal of the Directive was to protect the fundamental rights and freedoms of individuals, especially the ones linked to the processing of personal data, while still ensuring the free flow of personal data between MS (Hustinx P, 2014).

The scope of the Directive is laid out in Article 3, which states that it applies to all processing of personal data wholly or partially by automatic means, and to the processing by other means in or

intended for a filling system. The second point of this Article mentions two exceptions to the Directive. The first one is if the processing happens throughout the course of an activity that falls outside the scope of Community Law and in any event where processing concerns public security, defense, State security, and activities of the State in areas of criminal law. The second exception is the processing "by a natural person in the course of a purely personal or household activity", as already mentioned in Convention 108+ (Hustinx P, 2014).

In addition, the European Data Protection Directive, like the Convention 108+, elaborates on the processing of special categories of data which is the most relevant part to this work. Indeed, the Directive mentions a list of these special categories, and, although there are fewer categories than in Convention 108+, health is still mentioned as one of them, making it relevant for this thesis. More precisely, according to Article 8 of the Directive, MS should prohibit the processing of personal data concerning health, among other things. However, it is to be noted that there are some exceptions to this prohibition. More particularly, paragraph 3 of the Article mentions some exceptions linked to the health sector. In that, it reads that this prohibition shall not apply when the processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or management of health-care services. Moreover, it also mentions that this prohibition does not apply when the person processing the data is a health professional who, under national law or rules, is obligated to professional secrecy (Hustinx P, 2014).

General Data Protection Regulation

Despite the much greater consistency between MS brought by the European Data Protection Directive, there were still some differences between them. In fact, there was still no full harmony between the countries. This was especially due to the fact that Directives set goals and standards and that then, need to be achieved by the MS through national laws. Therefore, with the aim of ensuring an even greater uniformization of the EU legal framework on data protection the European Union decided to make a change. Indeed, it decided to make it evolve from a Directive to a Regulation (de Terwangne C, 2021). Therefore, in 2016, the EU passed Regulation (EU) 2016/679, also known as the General Data Protection Regulation, which then became applicable two years later in 2018, taking the place of Directive 95/46/EC.

As of right now, the GDPR presents the centerpiece of EU data privacy law. The only scope of the regulation is personal data, which is intended as data that can directly or indirectly allow the identification of a natural person (Mildebrath H, 2023). In addition, there are two other important definitions when discussing the GDPR. Firstly, when "data subject", it is intended as "*the natural persons whose personal data are processed*". Secondly, when mentioned "controllers", it is intended as "*the natural or legal persons, public authorities, or other bodies which alone or jointly with others, determine the purposes and means of the processing of person data*" (Tzanou M, 2021).

When comparing the GDPR to its predecessor, Directive 95/46/EC, it can be noticed that not many changes were brought to the articles regarding the objectives and the scope. Indeed, the regulation applies to companies[2] and organizations regardless of the techniques used to collect or process data and independently from where it takes place. In fact, the regulation is not limited to the processing of personal data that is performed with automated means. The GDPR also includes things such as collecting, recording, organizing, and consulting data (Mildebrath H, 2023). Furthermore, the GDPR also applies to those companies that, although processing outside of the EU, are processing personal data of data subjects within the EU (Mulder & Tudorica, 2019). For this reason, Article 44 of the GDPR states that data cannot be transferred to a third country unless the conditions of Chapter V are met. Furthermore, according to Article 45 of the GDPR, transfer to a third country can take place if there is an adequacy decision[3], like the EU – US Privacy Shield. If there is no "adequacy decision", then the transfer can still take place once the data subject has explicitly consented to the transfer (Mulder & Tudorica, 2019). Therefore, it can be understood that the goal of the GDPR is to offer a similar level of protection to EU citizens independently from where their data is being processed.

Under Article 6 of the GDPR, personal data can be processed only if at least one of six legal grounds is met. In addition, it is to be noted that these grounds are consistent with those that are outlined in Directive 95/46/EC. To cite them, the six legal grounds are:

- If the data subject has given consent to the processing for one or more specific purposes.

[2] The regulation is not sector specific, although there exist some other sector specific laws.

[3] An adequacy decision is a ruling by the European Commission that a non-EU country ensures a level of data protection comparable to the EU's. This allows personal data to be transferred to that country without needing additional safeguards.

- If it is necessary for the submission of a contract to which the data subject is part.
- If it is necessary for compliance with a legal obligation.
- If it is necessary to protect the vital interests of the data subject or another natural person.
- If it is necessary for the performance of something carried out in the public interest.
- If it is necessary for the purposes of the legitimate interests brought forward from the controller or by a third party, unless such processing conflicts with the interests or fundamental rights and freedoms of the data subject that requires protection of personal data, especially if the data subject is a child.

Furthermore, as in the case of Convention 108+, the GDPR also mentions some special categories of data that enjoy special status and an increased level of protection. One of these categories is health data. Such categories cannot be processed, and in fact, the GDPR prohibits their processing. The reason for that is that the processing of such data might pose risks to the rights and freedoms of natural persons. In addition, the GDPR also recognizes that if such data are processed "on a large scale" it would present an even higher risk to the rights and freedoms of natural persons (Tzanou M, 2021).

According to the GDPR "data concerning health" means "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*". This includes information related to the past, current, and future physical or mental health status of the data subject. This definition, pretty similar to the one given by Convention 108+, is pretty broad, but we can notice that personal data is considered to be health data as soon as "it reveals information about a person's health" (Mulder & Tudorica, 2019).

Furthermore, the GDPR's preambles provide some examples of what is considered 'health data': information on a disease, a disability, and also a disease risk. For example, information about someone's obesity or tobacco information is all part of disease risk information. The preamble also mentions that the source of such information does not matter. This means that it is not limited to medical devices, so it also applies to data processed by applications or wearable devices (Mulder & Tudorica, 2019).

The GDPR also mentions some rights and prohibitions around health data. In addition, it mentions some exemptions to the non-processing rule. Throughout the following paragraphs, we will be taking a look at all three topics.

The regulation prohibits automated decision-making when it comes to these special categories of data. This means that data subjects have the right to not undergo fully automated decisions that analyze or predict aspects concerning their health (Tzanou M, 2021). This is due to the fact that what constitutes health-related information could depend on the context: a "*piece of information might not possess the intrinsic nature of health data but, analysed by algorithms, it might reveal the health status of a person*". For example, a supermarket shopping list might reveal information about someone's dietary habits and as a consequence of this their health status (Tzanou M, 2021).

Furthermore, the regulation also imposes additional responsibilities on controllers that process health data. In fact, according to Article 13, they must keep records of processing activities even if the organization employs fewer than 250 people. Furthermore, Article 37 states that if the main activity of the organization is to process health data on a large scale, it must designate a Data Protection Officer (DPO).

As stated, the GDPR presents some exemptions to the prohibition on the processing of health data. These exemptions are listed in Article 9, paragraph 2, and are different from the ones mentioned in Article 6 that were seen before.

Firstly, the processing is allowed if the data subject has given their explicit consent. In this case, the GDPR allows MS and the EU to remove the consent exception under certain circumstances.

Secondly, processing is allowed when it is necessary in order to fulfill obligations and exercise specific rights of the controller or of the data subject in relation to the field of employment, social security, and social protection law.

Thirdly, it is allowed if the data subject is physically or legally incapable of giving their consent and the data is necessary to protect their vital interests. An example of this is when the data subject is unconscious due to an accident and the hospital needs to know the person's medical history.

It is important to know that it is also allowed if the data has been manifestly made public by the data subject. This exemption is a reason for discussion because, while the GDPR would seem to state that the data published on social media, apps, and devices is information that is manifestly made public, and so it can be processed, some individuals would argue that the posting of health data on social media or apps is not enough to allow the processing of such data by another controller (Tzanou M, 2021).

When the processing is necessary for reasons of "substantial public interest", it is important to underline that processing in the "public interest" is not enough, in fact, such interest needs to be substantial. What constitutes as "substantial public interest" is not defined by the GDPR, but it does specify that such processing of data must be proportionate to the aim pursued, it shall still respect the "essence" of the right and provide specific and suitable safeguards for the data subjects.

Furthermore, processing is also allowed when it is necessary for reasons of "public interest in the area of public health" and for achieving purposes in scientific or historical research purposes or statistical purposes. As in the case of "substantial public interest", the processing must be proportionate, always carried out on the basis of EU and MS law while still safeguarding the fundamental rights and interests of the data subjects. It is important to underline that one of the exemptions is not enough for the processing of data to take place. In fact, there must also be "suitable safeguards" to protect the data (Mulder & Tudorica, 2019).

In addition to the exemption based on "public interest in the area of public health" that is stated in Article 9 and that has just been mentioned, the GDPR also allows the processing of sensitive data for reasons of public interest when it comes to public health in Article 54. In this regard, the regulation underlines the fact that the processing of health data for reasons of public interest should not result in personal data being processed by third parties for reasons different from public interest. Furthermore, the GDPR also allows for public health exemption to the right to erasure (right to be forgotten). This means that if personal data needs to be retained for public health reasons, then the controller is not obliged to erase the information even if the data subject exercises their right to erasure. According to the GDPR, public health means "*all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, an universal access to, health care as well as health care expenditure and financing and the causes of mortality*" (Tzanou M, 2021).

As we have seen, the first exemption mentioned in Article 9 is if there is "explicit consent" from the data subject. According to the GDPR, consent means "*a clear affirmative act establishing at least the freely given, informed indication that the data subject agrees to the processing of his or her personal data*" (Article 4.11). Neither the GDPR nor the Convention 108+ determine how consent must be given. This means that data subjects can give their consent both through a written or oral statement. However, both legislative pieces state that the request for consent[4] has to be clear, concise, not unnecessarily disruptive and it needs to be presented in a clearly distinguishable form. For example, it cannot be buried within a contract or another written document (Mulder & Tudorica, 2019).

Furthermore, according to Article 7 of the GDPR, the controller must be able to demonstrate that the data subject has given consent to the processing of the data, and, additionally, it must allow the data subject to withdraw their consent at any given moment in a manner that is neither more complicated nor easier than initially providing it. For the consent to be "freely given" it is important that the data subject has a free choice and can refuse or withdraw the consent. For the consent "to be informed" the data subject must be aware of the identity of the controller and the intention behind the processing. A written request for consent must be written in clear and plain language. Another key characteristic that requests for consent must have is transparency. A data subject has the right to know who processes the data, what is the purpose of the processing, and the risks, rules, safeguards, and rights (Mulder & Tudorica, 2019).

A frequent problem is that, if written in the request for consent, personal data can be shared with third parties. Usually, in the request, it is only mentioned several categories of recipients, which are not named specifically. This means that personal data can be shared with a variety of unknown parties. Furthermore, these third parties could share the data with other third parties, and so on. In this case, the responsibility to protect the data remains with the original controllers, however, it is not hard to see that this comes with a number of challenges and problems (Mulder & Tudorica, 2019).

The data subjects also present other rights, we will now see some of the most important ones. The GDPR mentions the data subject's right to information and access to their personal health data (Tzanou M, 2021). Furthermore, according to Article 34 of the GDPR, data subjects need to be

[4] A request for consent is a formal or informal notice in which one party asks another party for permission or approval to perform a specific action or to move forward with a particular choice

informed, without undue delay, if there is a data breach. According to the GDPR, a personal data breach is "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*". This right is very important since the health sector is one of the most affected sectors when it comes to personal data breaches. In fact, in the first quarter of 2018, 1.13 million patient records were breached via 110 data breaches. The majority of these breaches were caused by snooping on family members, neighbors, and VIPs and by hacking incidents. Most of these health data records are then used or sold for commercial purposes. Such breaches are clearly inside the medical context, but it can be assumed that breaches regarding health data generated by modern technologies, like apps and wearable devices, can also be used for malicious purposes. Unfortunately, there are no numbers available regarding data breaches within companies, this is probably due to the fact that companies do not always publish their major breaches for reputational reasons. In fact, according to the GDPR companies need to communicate the data breach to the data subject only in case of a high risk to rights and freedoms (Mulder & Tudorica, 2019).

European Health Data Space

Unfortunately, after the implementation of the GDPR, several problems started to arise. Indeed, the GDPR was interpreted and implemented in different ways throughout the MS, and this created problems for the improvement of cross-border health care in the EU. It resulted in a fragmented landscape across the European Union, which raised legal uncertainties in the territory. This has made the entrance into the markets of other MS quite difficult for digital health product manufacturers and health service providers. They would face barriers and additional costs when trying to enter another MS. Furthermore, structural problems prevented people from fully benefiting from the use of electronic health data. In fact, it is not always easy for patients to interpret national law and, as a consequence of this, exercise their rights. Additionally, such structural problems also made it hard for researchers to access the necessary data to create better healthcare products and services. As a result of this, patients were not able to benefit from innovative treatments. Lastly, the COVID-19 pandemic highlighted the limitations of the existing EU health data system. It showed the urgent need for better health data sharing and collaboration across MS. The lack of a common framework posed key barriers to scientific research on the virus and has limited the cooperation among the MS. Health authorities needed accurate up-to-date information about the infection rates, vaccine distribution, supplies, and

more. However, the absence of a centralized platform to exchange such information made it difficult to properly coordinate efforts (Quinn et al., 2024). It was clear that the efforts to cultivate a cross-border health service were not generating the results that were hoped for, or any development for that matter.

Therefore, on May 3rd, 2022, as a result of these problems and as an attempt to solve such issues, the European Commission presented a proposal for the European Health Data Space. The proposal was then adopted by the European Parliament in April 2024. As a result of this, the Council of the Europe Union will now have to formally adopt the new regulation and publish it in the Official Journal of the EU this upcoming autumn. From there the EHDS will gradually become applicable in different stages, with a full implementation expected for 2028 (European Commission, 2024).

The aim of the EHDS is to address the complexity of current EU rules on health data sharing and promote health digital services throughout the European Union. In order to achieve this, the ecosystem created by the EHDS is composed of rules, common standards, practices, infrastructures, and a governance framework for two data purposes. The first purpose is to empower individuals through increased digital access to, and control of, their electronic personal health data (i.e., primary use of data), both at a domestic and cross-border level. The second goal is to provide a reliable, dependable, and effective framework for the secondary use of health data, which is the use of data for research, innovation, policy-making, and regulatory activities (European Union, 2022; European Commission, n.d.).

As of today, not only is the EHDS one of the main pillars of the European Health Union[5], but it is also "*the first common EU data space in a specific area to emerge from the European Strategy for Data*". This framework was created with the aim of establishing a single European data space, that is a unified market where data can move freely between industries and nations within the EU while still maintaining privacy and security for individuals and companies. The aim of this "single market for data" is to make the EU a "Data-driven society". In order to achieve this, the EU aims to create a

[5] It is an initiative brought out by the European Commission in response to the COVID-19 epidemic. The European Health Union seeks to strengthen the resilience of Europe's health systems overall, better safeguard the health of EU residents, and prepare member states to combat future pandemics. In order to guarantee that health systems are strong, well-coordinated, and equipped to handle both ordinary medical demands and emergencies, it places a strong emphasis on cooperation and solidarity among member states.

number of data spaces in the main economic sectors and public domains. Therefore, under this perspective, the EHDS fosters a "*genuine single market for electronic health record systems, relevant medical devices and high-risk artificial intelligence (AI) systems*" (Quinn et al., 2024).

For the correct implementation of this new health data framework, the EHDS mentions two key data intermediary platforms, MyHealth@EU and HealthData@EU, and the creation of national entities, the Health Data Access Bodies (HDABs). These are all linked to one of the two data usages that were previously mentioned, primary use of data and secondary use of data.

The first use (EHDS1) is associated with personal data access, it is used to support and provide direct individual healthcare delivery to data subjects. In fact, it consists of the collection, storage, and processing of health data to guarantee that healthcare providers can deliver appropriate and effective care to patients. Health professionals have access to the medical history, diagnostic information, treatment plans, and lab tests of patients. They also have access to online prescriptions, the progress of the patient, and more. In order to achieve this the EHDS also strengthens the initiative 'MyHealth@EU'. This initiative aims at facilitating the cross-border exchange of health data among Member States. In fact, it allows healthcare providers and individuals to access and share health information no matter where they are located in the EU. However, it is important to note that all these exchanges must be compliant with the GDPR. The EHDS was not the first European legislation act to adopt the patients' right to cross-border healthcare. In fact, it was already adopted in the European Directive 2011/24/EU, which guarantees the continuity of care for European citizens across borders through the use of electronic prescriptions and the summary of the patient's medical records. Unfortunately, to this day, only nine countries have shown some kind of capability of cross-border health services, four actively exchange electronic prescription data and eight can exchange summaries about patients' data. As a consequence, the EHDS made participation in the MyHealth@EU initiative mandatory for all EU countries.

The second use (EHDS2) is regulated by Chapter IV of the EHDS. In this chapter, one can find the purposes for which data may be used as well as lists of prohibited uses. As previously mentioned, secondary usage of data is defined as "*the use of individual-level health data, or aggregate datasets, for the purpose of supporting research, innovation, policy making, regulatory activities and other uses*" (Marcus et al., 2022). Therefore, this use of data goes beyond the direct care of individual patients. Indeed, it entails the analysis and processing of health data in order to support a broad range

of initiatives that bring societal benefits. An example of such benefits could be the usage of such data to track the spread of a disease, such as COVID-19, and identify potential risks and find a potential cure or/and vaccine. The EHDS applies to both health data that has been collected for the intended secondary use and also to re-used data, that is information that has been previously collected in the context of primary use (Slokenberga S, 2022). It is important to highlight that, in recital 41, the EHDS makes a distinction between scientific research, on the one hand, and development and innovation on the other hand. It is to be noted that this division is something that was not carried out in the General Data Protection Regulation.

The categories of health data that should be made available for secondary use cover a wide range of data and can be found in Article 33 of the EHDS. For example, electronic health records, human genetic, genomic, electronic health data from biobanks and dedicated databases, and person-generated electronic health data, that is data collected from wellness applications or devices are all part of data that should be made available for secondary usage (Slokenberga S, 2022).

Furthermore, the EHDS mentions some main roles, for example, data holder, data user, and data access body, and some main administrative tools like data permit, data access application, and data request.

To begin with, a data holder is a "*natural or legal person holding the right or obligation to make available certain data according to the rules set out in Chapter IV of the EHDS*" (Slokenberga S, 2022).

Then, a data user is a "*natural or legal person who gains lawful access to personal or non-personal electronic health data for secondary use as prescribed in Chapter IV of the EHDS*". This notion captures both public and private actors, non-profit entities, and individual researchers. Furthermore, a data user is required to demonstrate that all conditions are satisfied, including the legal justification for accessing personal data. They also need to ensure that the intended use does not violate any of the banned uses specified in Article 35 of the EHDS (Slokenberga S, 2022).

The third main role is the national health entity previously mentioned, the National Data Access Bodies. They are entities that operate at the national level within each Member State. Their main aims are to manage access to health data for secondary usage and ensure that such access complies with both national and EU regulations. They are granted wide discretion in order to gather electronic health data from various sources to then allow third parties to process such data for a variety of purposes, which are mentioned in Article 34 (Quinn et al., 2024). However, it is important to mention that consent to process health data for secondary usage is not required. This has raised numerous concerns

regarding potential privacy harm to individuals, but the EHDS presents opt-out options. In addition to such options, there are two primary protective pillars. The first is the broad discretion granted to the HDABs in authorizing a data access permit, along with a set of principles outlining when such a permit should and should not be granted. Secondly, data access permits can only be granted if the intended processing is compliant with the GDPR. This includes the existence of a valid legal basis and respect for data processing principles, like data minimization and storage limitation (Quinn et al., 2024).

In addition, the three administrative tools mentioned above (i.e., data permit, data access application, and data request) are important in order to obtain the health data needed.

In fact, a data request is the first formal step in the data request. It is made by an individual or organization seeking access to specific health information for secondary use. This request usually outlines the intended purpose, scope, and nature of the data needed.

After the data request, an individual or organization will have to submit the data access application, which is a more formal and detailed submission. This application must contain a lot of information that justifies the request, as for example a detailed explanation of the intended use of the data, a description of the safeguards that will be put in place to prevent any other use of the data, the format, and data source.

Lastly, the data permit is the formal authorization issued by a National Data Access Body. It allows individuals or organizations to access and use electronic health data for secondary purposes. As mentioned before, National Data Access Bodies are granted a broad discretion when it comes to granting a data permit.

Finally, as previously mentioned, the EHDS also created the HealthData@EU in order to ensure the correct implementation of the secondary usage of data. This initiative has the goal of fostering secure and efficient use and exchange of health data across MS. HealthData@EU not only facilitates access to large health datasets but also allows the analysis of health trends and the impact of healthcare across the European Union. Furthermore, this initiative is subject to strict data protection standards under the EHDS. It places significant emphasis on transparency about how the data is used. This is done with the goal of ensuring that citizens remain in control of their health data.

Chapter II: In reality…

As previously seen, one of the aims of the EU, in the last few years, has been to establish a single European data space, that is a single market for data in the main economic sectors and public domains. As part of these sectors, we find the health sector which is the one of main interest in this thesis. As it could be understood so far, through the GDPR and the EHDS, the EU aims to transform the current fragmented national health systems into a cohesive digital European system. Through these legislation, the EU has set the basis and the framework for this system but in order for it to become a reality, people must be willing to share their personal health data. Throughout the years people have expressed their concerns regarding the sharing of such information, and that, while overlooking the many benefits this could actually bring them.

In this chapter, we will analyze exactly this, the benefits, and the concerns around health data sharing. We will also consider various research and experiments on the willingness of people to share personal health information. Indeed, this step will be fundamental as the analysis of these experiments can help to understand how to better improve the implementation of the health digital system.

Benefits of sharing

The advantages arising from the sharing of personal health data are many both for patients and organizations, but also for Member States.

One of the biggest benefits of health data sharing, for individuals, is the fact that they would receive more personalized treatments. In fact, thanks to the EHDS, healthcare professionals would have access to the patient's detailed and accurate clinical, genetic, and pharmaceutical history. This means the healthcare professionals would be able to see all lab test results (i.e., x-rays, blood work), allergies, reactions to medication, genetic predisposition to certain diseases, and more. As a result, this would allow them to make informed decisions about what treatment to carry out for the patient. For example, a person with a genetic predisposition to a certain disease may receive a more tailored preventive treatment. While, if a patient has a reaction to a certain medication, the doctors might prescribe another more effective one, therefore reducing the risk of side effects. Furthermore, the decisions

taken by the healthcare staff would be more accurate and informed since there would be no missing data in the patient's health history, reducing the possibility of a medical error due to misinformation.

Another benefit for individuals is the fact that one's health data could be easily accessible to healthcare professionals in case of emergency. In such cases, a timely and appropriate response could make the difference between life and death. In these critical situations, the healthcare staff could immediately access the patient's medical history and know about any allergies or reactions to medications and pre-existing conditions. This would not only reduce the patient's risk but also shorten the decision-making time, as medical staff would avoid performing repetitive diagnostic tests.

As just stated, the sharing of a patient's health data can also help avoid carrying out the same tests multiple times. This often occurs when patients change doctors or go to multiple health facilities without having all the previous health information available. Such tests, like X-rays, CT scans, and laboratory tests, are very expensive to run, so reducing their duplication can also significantly reduce costs for everyone. Therefore, not only does it save money, which in turn could be utilized for improvements and/or research, but it also frees up staff and equipment, which could be reallocated to guarantee accessibility of care for more patients.

Furthermore, the use and re-use of digital health data could drastically change the medical research field. It could deliver substantial public health benefits, ranging from disease risk prevention to the discovery of new therapies (Nwebonyi et al., 2022).

It would provide larger and more representative datasets for researchers. This would improve the quality and reliability of their studies, potentially leading to medical breakthroughs. This is especially true for studies on rare diseases that involve a very limited number of patients.

Moreover, it would help identify the most cost-effective therapies. In fact, by collecting long-term health data it would be possible to monitor the effects of treatments over the years, assessing both the immediate effectiveness and long-term impact.

Additionally, data sharing would allow the EU to conduct epidemiological research and carry out prevention programs. In fact, as seen in the previous chapter, the lack of a common framework and of a centralized platform to exchange health information posed significant limitations on the COVID-19 response and research. The cross-border sharing of health data would allow the EU to better

identify risk factors, and study the spread of diseases and the effectiveness of vaccinations. This would guarantee a rapid answer to any future threats.

Therefore, it can be seen that all these benefits are possible thanks to the continuity of the health data between one country and another. This continuity is granted by European legislation and is a relatively new concept. In fact, the fragmentation of health policies and systems between MS has been one of the historical problems of the EU. Although new regulations like the GDPR and the EHDS ensure data cohesion, making these benefits possible, it remains essential for individuals to be willing to share their personal health data to fully realize these advantages.

Concerns about sharing

As seen in the previous paragraph, health data sharing comes with many different opportunities, but it also comes with several privacy and security issues. Some examples include but are not limited to, unauthorized access, secondary usage, breach of personal information, and consumers' reduced personal information control rights (Dimodugno et al., 2021).

These issues are important to take into consideration when discussing the sharing of health data because people's concerns about that matter can affect their decisions.

In fact, how much information, which one, and to whom one shares health data varies depending on several factors. For example, some data are considered more sensitive than others, i.e. consumers are more likely to share demographic information over financial or health data. Other factors are the use of such information, that is if it will be used by a particular industry sector, and the political context, i.e., if privacy is considered a right, and the laws that are put in place (Pelteret & Ophoff, 2016).

As seen, the concept of privacy is a very broad one that is influenced by various factors. For this reason, Acquisti (2004) states that the value of privacy can be discussed only once the context has

been specified[6]. However, there might be several different complexities that are hidden inside concepts that are too difficult to understand even for those individuals that really want to protect their data and privacy. In fact, Pelteret & Ophoff (2016) correctly point out that individuals will encounter incomplete information, bounded rationality, and psychological distortions, which are concepts that will be explored and explained more in detail in the following paragraphs.

First, individuals might face incomplete or asymmetric information when making decisions. An example of this is the fact that they do not know to which third parties the data is being shared with. As seen in the previous chapter, many requests for consent only mention categories of recipients, they do not mention any specific company or institution name. Furthermore, these parties could share the health data with other third parties without the individual knowing.

Then, people might also be affected by bounded rationality and psychological distortions. This means that they are not fully able to process all the information they receive, they might be unable to properly calculate and compare payoffs. These payoffs may only be determined through experiences and which probability values may be entirely subjective or affected by biases (i.e. optimism bias, framing effect, anchoring, individuals are usually loss averse, etc.) (Pelteret & Ophoff, 2016).

Passing now to another concern, it is to be known that the secondary use of information has given rise to big data[7]. Such data can be used in a variety of positive ways, that is optimizing operations and improving the performance and safety of products and services. This phenomenon also presents some issues that have raised some concerns among individuals. In fact, big data can include both personal and non-personal data that are combined together through sophisticated techniques. This creates a new type of data that might not be labeled as personal data and thus avoids regulation. In addition, with enough data organization, this new data could also generate group profiling that could then be used to discriminate against individuals (Pelteret & Ophoff, 2016). For example, it could lead to stereotyping by associating certain health risks or diseases with a specific demographic group, even when data only shows a correlation and not a causation.

[6] Context here is defined as "stimuli and phenomena that surround and thus exist in the environment external to the individual, most often at a different level of analysis" (Mowday & Sutton, 1993)

[7] According to the Cambridge Dictionary, big data are "*very large sets of data that are produced by people using the internet, and that can only be stored, understood, and used with the help of special tools and methods*".

Mason (1986) summarizes these concerns and problems in a framework called PAPA, which stands for privacy, accuracy, property, and accessibility.

Privacy will concern questions on who has access to this data, and how it is collected, stored, and shared: "*What information should one be required to divulge about oneself to others*?"

Accuracy relates to errors in data and misinformation which have severe implications for individuals and organizations: "*Who is responsible for the authenticity, fidelity, and accuracy of information*?"

Property focuses on the intellectual property rights and ownership of information: "*Who owns information*?"

Lastly, accessibility relates to the issues of who has the right and the ability to access such information and under what circumstances: "*What information does someone have a right to obtain*?" (Pelteret & Ophoff, 2016).

Similarly, Smith, Milberg, and Burke (1996) listed four areas of concern and found that consumers are usually concerned about all four categories rather than just one. The four categories are; i) improper access to personal information; ii) unauthorized secondary use of personal information; iii) errors in personal information; and iv) collection of personal information (Pelteret & Ophoff, 2016).

However, as seen in the first chapter, all these concerns are covered by EU legislation.

Indeed, privacy is the central component of main EU legislation, like the GDPR and the EHDS. These legislation focus on individuals' rights to privacy and set strict guidelines for the processing, storage, and transfer of health information. Additionally, they require explicit consent for the processing of such sensitive data and provide individuals with the right to access, correct, and delete their data.

Through the EHDS initiative, the EU wants to strengthen these rights as it aims to create a common framework that facilitates the secure sharing and accessibility of health data while still ensuring privacy and security.

Furthermore, Article 5.1.d requires that personal data must be accurate and kept to date while inaccurate data must be erased without delay. This is fundamental in the health sector as inaccuracies can lead to wrong diagnoses which could lead in turn to more serious problems.

Therefore, while there are still some concerns among individuals when it comes to sharing health data, it can be seen that the EU is trying to create a strong and secure legislative framework for the sharing of health data.

Factors influencing people's willingness to share: previous research and experiments

Discussion about a European digital health system started getting momentum in the early 2000s, but the formalization of such efforts started only in the 2010s. Therefore, since it is a relatively new topic, there are not many research and experiments that study people's willingness to share personal health data and the factors that influence such decisions. In addition, the majority of the studies conducted are surveys that focus on one specific MS.

A first interesting study has been conducted by Dimodugno et al. (2021), who state in their paper: "*the purpose of this quantitative correlation study is to measure the effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information in the context of big data analysis*".

In order to fully understand what influences people's willingness to share personal health information, a focus will be placed on the results of these surveys and experiments. By doing so, it could be possible to understand what could be done to strengthen the European digital health system.

As seen in the previous subchapter, there are many concerns around the sharing of health data, and these concerns affect people's willingness to share it. Indeed, studies showed that increased privacy concerns usually diminish the willingness to share of individuals.

There are different factors that can influence people's perception of privacy concerns. Dimodugno et al. (2021) have seen that increased perceived privacy control reduces privacy concerns. This result is also aligned with previous studies that showed that when perceived privacy control decreases, privacy

concerns usually increase. Moreover, studies have shown that people tend to value, to different extents, the level of involvement they have in the decision-making process about health data sharing, access, use, and reuse (Dimodugno et al., 2021; Nwebonyi et al., 2022).

Analyzing the results of other studies, Courbier et al. (2019) found that patients and their relatives "would like to keep control of" the data they shared, and the majority of them would not delegate "the decision about whom their data will be shared with to an ethics committee".

Another study showed that the participants would like to be re-contacted to decide on the reuse of their health data and these persons perceived the lack of opportunity to re-consent as a threat to personal autonomy.

Additionally, Nwebonyi et al. (2022) found that around 80%-87% of participants affected by rare diseases placed a high value on opportunities for involvement in decisions about sharing, accessing, using, and reusing their health data. This number is significantly higher than other participants not affected by rare diseases, among whom less than 50% considered it important to decide these matters.

In that same study, Nwebonyi et al. (2022) also found that participants who give high importance to trust in research institutions when deciding whether or not to share information, to whom, and what, are significantly more likely to value involvement in the decision-making process of data sharing.

Therefore, as it can be understood, it is essential to guarantee people's participation in managing the privacy of their own health data, if they want to. Indeed, this would increase their willingness to share data and strengthen the new digital health system.

Furthermore, many studies show that health data sensitivity raises important privacy concerns that affect consumers' intention to share personal information (Cherif et al., 2021). It is important to underline that not all personal health data is seen as equally sensitive (Bosanac & Stefanovic, 2022). As a consequence of that, people might be more willing to share information that is considered "less sensitive". To illustrate what could be considered as such, a study conducted by Bosanac & Stefanovic (2022) showed that mental health and STDs are considered the most sensitive health data, followed by family history and hereditary diseases. On the other hand, blood pressure, height, allergies, and cigarette consumption were regarded as the least sensitive.

Another factor influencing privacy concerns is trust. Indeed, as trust decreases, concerns increase. Both of these variables are significantly important when talking about the sharing of health

information. As a matter of fact, studies have shown that two main predictors of people's behavior in accepting technology in health services and disclosing private information are trust and privacy concerns (Dimodugno et al., 2021).

In that way, there are some factors that have been identified as contributors to a positive trust relationship between citizens companies, and organizations. For example, on the one hand, the belief that companies and organizations will keep data private and secure in their private databases, and not share it with third parties is one of these factors. This trust is further strengthened by the faith that these entities will only use the minimum amount of data necessary, always acting in the consumer's best interest. On the other hand, Moon (2017) also identified some factors that are associated with negative trust relations. For instance, one that has been identified is the fear of discrimination and lack of trust by ethnically diverse populations when an internet mechanism is used. Moreover, another factor is the absence of confidence in healthcare workers, the healthcare system, and the government. Studies have shown that trust in healthcare providers is fundamental in building a digital health system as it reduces privacy concerns and increases the intention to share (Vodicka et al., 2013; Gajanayake et al., 2014; Dinev et al., 2016; Cherif et al., 2021). To that extent, an interesting finding was made by Bosanac & Stefanovic (2022) in their survey. Indeed, they found that respondents who were health professionals had less trust in doctors' confidentiality compared to non-health professional respondents.

Trust is a fundamental characteristic needed in the digital health infrastructure (Moon L.A, 2017). On the one hand, consumers need to give permission for their data to be accessed and shared and, on the other hand, providers, researchers, and organizations are responsible for the safe and secure storage, use, and exchange of such data. Therefore, it is fundamental to strengthen trust relations with consumers, and as a result, strengthen their willingness to share personal data.

A way to do so could be to write clear privacy policies. Such policies should be placed in a "conspicuous" place on the website, it should also contain the principles of collection, control, and usage of personal data. In addition, what really matters to consumers is the execution of these privacy policies (Dimodugno et al., 2021). This would allow the patients to have a clearer understanding of how their data is used, to whom it is shared, and for what reason. As a result, having knowledge of these facts would not only increase people's level of trust, but it would also increase their sense of perceived privacy control.

Furthermore, increased perceived privacy risk increases privacy concerns. This is backed by previous studies, in particular a study that used the privacy calculus[8] to analyze several survey responses and found that perceived privacy risk is positively related to social privacy concerns (Dimodugno et al., 2021).

In light of this, it is important to underline that several studies using the privacy calculus effects have shown that perceived benefits outweigh the perceived risks, and this reduces individuals' privacy concerns and positively affects their intention to share personal health data (Cherif et al., 2021).

In a systematic review, Shen et al. (2019) found that personal health concerns might lead individuals to change their privacy behaviors in order to benefit from a better health system. This is a recurring result among studies on the topic. In fact, a study by Menon et al. (2002, 2006) showed that the perception patients have of health risks affects the way they perceive and share health information. For example, chronically ill patients worry far less about privacy than healthy patients. Studies have also found that people are more inclined to share personal health data if they perceive such information to be useful for public health research, non-sensitive, and if they trust the anonymity of research (Bosanac & Stefanovic, 2022).

Therefore, perceived benefits, both individual and of the society, outweigh perceived risks and reduce privacy concerns. Highlighting the benefits that come with implementing a digital health system, which are usually overlooked by patients, could help people overcome their privacy concerns, and this could increase the sharing of personal health information.

A study by Nwebonyi et al. (2022) and another by Bosanac & Stefanovic (2022) have shown that participants with lower levels of education give significantly less importance to involvement in decision-making about the purposes for which their data can be used. In addition, a higher digital literacy was found to be related to a higher confidence in online data protection. Therefore, promoting computer skills and digital literacy could be a way to improve the implementation of the digital health system.

Finally, it is important to note that other factors such as age, gender, profession, and nationality could also influence the decision-making process of data sharing and trust levels in the digital health system.

[8] According to Dienlin (2023), "*The privacy calculus states that before disclosing personal information online, people engage in a rudimentary tradeoff by comparing expected benefits with anticipated costs. If benefits exceed costs, people are more likely to self-disclose.*"

It could be interesting to further develop such topics in the future (Cherif et al., 2021; Bosanac & Stefanovic, 2022).

Chapter III: A survey and an experiment

As discussed so far, for an efficient and correct implementation of the EHDS it is important to understand people's propensity to share their personal health data and to whom they are willing to share it. Furthermore, it is also essential to identify which categories of data people are more inclined to share.

Gaining insight into these things can help strengthen the relationship between individuals and recipients, particularly the government, who represents a key figure in the EHDS. Indeed, the National Access Bodies Agencies proposed by the EHDS are government owned.

This chapter aims at further exploring these topics in order to gain a deeper knowledge. It does so through a six-section survey. First, it does so by exploring the concept of the trust game and the public good game in order to set the context on the concept of trust which is essential when talking about sharing of information. After that, it goes through a six-sections survey that has been conducted to learn more about people's knowledge on the subject but also their potential propensity to share some of their data to diverse recipients. Furthermore, the chapter also suggests several potential ideas for future research. To conclude, it is discussed a future experiment that will be carried out by Professor Di Cagno, Daniela, Professor Savona, Maria, and PhD candidate Lisovaia, Anastasiia.

Trust Game

Trust is an essential part of everyone's economic life. In fact, everyone, implicitly or explicitly, trusts institutions, employers, companies, and citizens. For example, without trust, nobody would accept money that is intrinsically valueless in exchange for goods or services (Alós-Ferrer & Farolfi, 2019).

According to Alós-Ferrer & Farolfi (2019), trust "*is revealed when an agent performs an initial sacrifice, that is, an action which, depending on the reaction of another agent, might be detrimental to the first agent's own interests*". This means that, by doing so, you are putting yourself in the hands

of someone else. This trust is repaid if the reaction of the second agent offsets and compensates the sacrifice of the first agent, in this case, the second agent is revealed to be trustworthy.

Considering how important trust is in social contexts, economists have developed various games to study participants' willingness to trust others and reciprocate such trust. The most famous is the Trust Game, created by Berg, Dickhaut, & McCabe in 1995.

In this game, we have two agents. The first one is called the trustor, and they are given a monetary endowment X. The trustor then needs to choose which fraction p of X, zero being also an option, to send to the second agent, who is called the trustee. Once the trustor has made their decision, the transfer $p \cdot X$ is gone and there is nothing they can do to ensure a return of any kind. Before the transfer arrives to the trustee, it is magnified by a factor $K > 1$, i.e. doubled or tripled. The trustee is then free to keep the whole amount of the received transfer, without repercussion, or they can send a fraction q back to the trustor, honoring the trustor's initial sacrifice (Alós-Ferrer & Farolfi, 2019).

It is important to underline that, originally Berg, Dickhaut, & McCabe (1995) called this game the Investment Game, and the name Trust Game was used for an earlier and simpler game by Kreps in 1990.

In the game by Kreps, the trustor has a binary choice; that is to trust the trustee or not. If no trust is shown, then payoffs will be $0 for both. However, if the trustor decides to trust, the trustee will be presented with a binary choice to either honor it or abuse the given trust. If the trust is honored, then there will be an equal payoff of $10 for both players, while if the trust is abused, then there will be a payoff of $15 for the trustee and a negative payoff of -$5 for the trustor.

While the two trust games proposed by Kreps (1990) and by Berg, Dickhaut, & McCabe (1995) are different, they share four crucial characteristics that were summarized by Coleman (1990). First, the decision of the trustor to trust is voluntary. Second, there is a time lag between the decision taken by the trustor and the trustee. Third, the possibility of the trustee misusing or honoring the trust shown by the trustor occurs if and only if the trustor does actually show trust. Lastly, in the case that the trustee decides to misuse the demonstrated trust, the trustor will be left worse off than if no trust had been given, so the trustor becomes vulnerable by exercising trust. Furthermore, Alós-Ferrer & Farolfi (2019) also added a fifth element: if one is to consider economic efficiency, trust should be optimal,

at least in the sense of maximizing the sum of payoffs. In addition, such efficiency further requires that trust is repaid.

In these games, the theory would suggest that agents, who are rational and selfish, do poorly: "*a selfish trustee will never send any money back, and anticipating this a selfish trustor will never make any transfer*". However, these experiments showed that actual human beings are far more trusting and more trustworthy than selfishness would imply (Alós-Ferrer & Farolfi, 2019).

To further sustain this observation, let us consider Berg, Dickhaut, & McCabe's study, in which two different treatments were run. The first one, "no-history", gave the participants instructions on how the game worked, but no additional information was given. However, in the second treatment, "social history", the participants were given a report summarizing the decisions of the previous 32 pairs of subjects in the no-history treatment.

According to Bergs, Dickhaut, & McCabe (1995), the unique Nash equilibrium prediction was for participants in room A, hence the trustor, to send no money. This was proven wrong right away in the first treatment (i.e., the no-history one), in which 30 out of 32 trustors sent money to the other subjects, hence the trustees, and 11 of these 30 decisions resulted in a payback greater than the amount sent. Therefore, the subjects of room A, the trustors, were willing to risk an amount of money to place their trust in the expectation that there would be reciprocity, and the subjects in room B, the trustees, would keep this trust (Berg et al., 1995). However, the remaining subjects of room B that did not reciprocate the trust may have been acting out of self-interest or they may have not understood that the subjects in room A were trying to build trust and so reciprocation was not an issue for them.

The aim of the social history treatment was to see whether subjects in room A, the trustors, would still trust and send money to the trustees despite knowing that 2/3 of the subjects in the no-history case did not reciprocate. Knowledge of such information could lead to a loss of trust from the trustors, resulting in lower amounts of money sent. However, such a prediction was proven wrong. Indeed, only 3 of 28 subjects sent zero, and $5 and $10 were now sent 50% of the time, which presents a slight increase from before (but this result was not statistically significant). Furthermore, moving from the no-history to the social history treatment, there was a change in average return that went from a negative $0.50 in the no-history case, up to a positive 1.10 in the social history case. The average amount sent only increased by 20 cents, so most of this change was accounted for by an increase in the average payback.

Therefore, the Trust Game is an experiment to better understand people's willingness to trust and reciprocate this trust. As it can be seen, it has been proven that humans are more trustworthy and far more trusting than the theory says.

Public Good Game

Another fundamental aspect of economic life is the concept of public goods. These are commodities or services that are non-excludable and nondepletable (Ingham S, n.d.). In other words, they are goods that every member of society can use without reducing their availability to all other members. Examples include public streets and national defense; the state cannot give access to these services and commodities to only certain citizens while excluding others. Typically, these goods are provided by the government, and they are paid for through taxation.

Since public goods are non-excludable, meaning that they are available to all people regardless of whether they contribute to such goods, this creates what is known as the free rider problem. Some individuals, called 'free riders', benefit from these goods without contributing to them (Fernando J, 2024). So, these people 'free ride' on the efforts of others. However, if too many individuals free ride, the public good will not be provided anymore and nobody will benefit from it.

To better understand human behavior and to examine the conflict between personal gain and the collective benefit that individuals often face, economists developed the Public Good Game. This game was first formulated by Mancur Olson in 1965 in his book "The Logic of Collective Action". It was later expanded by researchers such as Dawes (1970s), Ledyard (1980s), and Isaac and Walker (1980s).

In this game, participants receive a monetary endowment, and they then need to decide how much to keep for themselves and how much to contribute to a common pool. The sum of all these contributions is then multiplied by a factor b and the resulting amount is divided equally among the participants,

irrespective of their contribution. The Nash equilibrium of the game is to contribute nothing, as individual returns are maximized by not contributing anything regardless of what others do. However, the collective optimal outcome is obtained from everybody contributing as much as possible. Moreover, collective returns are maximized if everybody contributes their full endowment to the common pool (Perada et al., 2019; Otten et al., 2022).

Studies have shown that during the first few rounds of the game, participants are more likely to contribute a significant portion of their endowment to the common pool. Hence, participants show high levels of cooperation. However, as the game progresses, contributions decrease. Researchers found that this happens because individuals observe that others might free-ride ride and so they adjust their behavior accordingly. With time, the participants realize that they can benefit from the common pool without giving up their share of endowments. As a consequence, this leads them to reduce their contributions. In the long run, this results in an under-provisioned common pool.

In addition, studies also found that punishing these free riders increases cooperation. This, however, can be counterproductive if the punishments are too high as it can reduce the common pool.

Finally, it was also found that communication among participants increases cooperation and contribution to the common pool. Indeed, when the participants can talk among themselves, they discuss strategies and agreements, and this encourages cooperation.

Knowing all this and considering the EU's new EHDS initiative, the Public Good Game is particularly relevant to the sharing of personal health data. The framework created by the EU to share such information represents indeed a public good. As it is a service provided by the government of each MS and by the EU, it can be used by any citizen regardless of their contribution to the service, hence regardless of whether they share personal information. Therefore, it is important to study how to increase people's contribution to the common pool, which in this case is the EHDS, and avoid free riding.

Survey: results and future research

To better understand people's willingness to share personal health information, we have developed a survey, entirely in English, composed of 6 different sections. In this subchapter, we will briefly go over the structure of the survey and analyze the results obtained. It is also to be known that the full version of the survey can be found in the appendix of the work.

To conduct this survey and collect answers, it has been sent out on various WhatsApp groups and posted on Instagram. By doing so, we managed to get a total of 287 answers. Out of these, 84 were incomplete answers and 6 were non-EU participants, who were not considered for the analysis of the results. Out of the remaining answers, 123 were participants from Italy, 39 were from Belgium, 20 from Germany, and 15 participants were from other EU member states countries (more particularly 4 Czech, 4 French, 3 Dutch, 1 Polish, and 1 Ukrainian). This grand total of saved answers amounts to 197. The results obtained by the survey were first analyzed separately in four different categories, grouped by nationalities (Italian, Belgian, German, and other EU). However, this study showed no significant difference between the answers of the four aforementioned categories. As a result of this, it was decided to study the answers all together with no distinction of nationality.

However, it is important to underline that the lack of variation between nationality groups might be due to the low availability of data. It would, in fact, be interesting to run the same survey in different MS. This would ensure a larger dataset of answers for each country. Furthermore, a cross-border analysis could be carried out to identify potential cultural differences between populations. This could also be very helpful in the implementation of the EHDS as it would help to understand societal perceptions of sharing health data and provide guidance on how to strengthen the EU system.

Lastly, the participants' ages ranged from 19 years to 66 years old. However, most of the population was between 19 and 27. In fact, only 13 participants were over the age of 40. The answers of these individuals were included in the general analysis, except for when it will be specifically stated otherwise.

Indeed, it would be interesting to study the differences between younger generations and older ones. On the one hand, it is recognized that younger people are, generally, more familiar with technology and digital platforms, so they might find the EHDS easier to use than older generations. Therefore, this could lead to higher adoption rates among young people. On the other hand, the younger generation could also be more aware of privacy risks, hence they might be more cautious when sharing their data.

Passing now to the survey in itself, the participants were first presented with an introductory text, which explained the aim of the survey, why it was conducted and by whom.

The first section aims at understanding whether someone is inclined to share their personal information. This is relevant since willingness to share personal data can be considered as an inherent characteristic of oneself. Some people, for example, are naturally more extroverted and open than others. This might make them more comfortable sharing personal data. Additionally, peoples' level of trust can significantly influence their propensity to share personal data. Someone who is naturally trusting might assume others have good intentions, leading them to share information more easily. Societal norms also play a crucial role in the decision-making process. People from certain cultures and/or backgrounds might feel more comfortable sharing more data than others.

The idea behind this is that the more inclined someone is to share personal information, the more likely they should be to also share their health data.

In order to understand people's inclination to disclose personal data, the survey presented five questions. The participants were asked if they would share their i) email address, ii) phone number, iii) location data, iv) financial information, and v) health information.

From Table 1, we can notice that in all cases, except for financial information, the participants would be willing to share their information but with some limitations. In the case of financial information, the majority of the participants, 78% of them to be precise, were not willing to share such information. This is in line with the studies aforementioned, which found that people consider financial information to be very sensitive data. Furthermore, one can notice that 41% of the population is not willing to share health data, and 55% of them are willing to share such information with some limitations. Finally, when talking about sharing with limitations, 127 participants (out of the 175 that answered "Yes, but with limitations") would base their sharing on who will be receiving the information and on the quantity of data that is being shared.

	email address	phone number	location data	financial info	health info
Yes, but with limations	69,04 %	67,01 %	52,79 %	21,83 %	54,82 %
Yes, no matter with who	13,71 %	1,02 %	0,51 %	0,51 %	4,06 %
No	17,26 %	31,98 %	46,70 %	77,66 %	41,12 %

Table 1: percentage of answers to “Would you share your…?”

This presents a hopeful scenario for the sharing of personal health data. To better understand this topic, participants were then asked more detailed questions in the third section of the survey. In this part, the subjects were presented with a matrix with four columns and five rows. On the one hand, each column represented someone they could potentially share the health data with. More specifically, “healthcare providers (i.e., doctors, nurses, etc.)”, “government agencies (i.e., public health authorities, etc.)”, “researchers”, and lastly “friends”. On the other hand, each row represented a category of health data they would be sharing. The categories considered were the following:

- Biometric data (i.e., health, weight, blood pressure, heart rate)
- Medical history (i.e., chronic conditions, allergies, prescription medications, past surgeries, or treatments)
- Clinical data (i.e., diagnoses, laboratory results)
- Lifestyle and behavioral data (i.e., dietary habits, exercise habits, sleep schedule)
- Mental health data (i.e., diagnoses, treatments, and medications)

From Table 2, it can be noticed that participants show a high willingness to share their data with healthcare providers. The category of data that people are more inclined to share with medical staff was biometric information, in fact, 96% of the participants answered that they would share such data. The other categories also presented high percentages of positive answers. Indeed, 95% of the participants are willing to share their medical history with healthcare providers, 93% of them are willing to share their clinical data, and lastly, 86% are willing to share their lifestyle and behavioral data and their mental health data.

However, willingness significantly decreased across the other three categories of recipients, hence researchers, friends, and lastly government.

For what concerns the category “researchers”, 59% of the participants are willing to share their biometric data with them. Following that, 58% of them are willing to share their lifestyle information, and then the percentages decrease to 55% for medical history, 53% for clinical data, and lastly 49% for mental health data.

Passing now to the category “friends”, these numbers further decline.

This category “friends” was included to see if people are more inclined to share information with their friends rather than other recipients. This could be due to feelings of trust and familiarity; people have close personal bonds that have been developed over the years and this usually increases trust. Furthermore, conversations with friends are more fluid and one can easily adjust the amount and type of information given. However, the data collected proves this to be untrue. In fact, only 47% of the participants are willing to share their biometric data with friends. While 42% of the participants are unsure (i.e., answering “maybe”) about disclosing their medical history to their friends, and the same percentage is willing to share such information with them. When it comes to clinical data and mental health, the number of unsure participants increases, surpassing the ones who are willing to share such information. Indeed, 41% of participants are unsure whether they want to disclose their clinical data to friends, and 36% would disclose such information to them. For mental health data, 47% of the participants are unsure about sharing such information with friends, and 32% would share it with them. However, an outlier in this analysis is lifestyle data. To be more precise, 60% of the participants are willing to share this type of information with friends, this is a higher number than for researchers and for the government. This could be due to the fact that lifestyle data is perceived as less serious, and it can be more easily discussed in everyday settings.

Lastly, the data shows that participants are the most reluctant to share personal health data with the government. Three out of five categories of data show a higher percentage of participants who are unwilling to share their information with this recipient. Specifically, 36% of participants are unwilling to share their clinical data, 41% are unwilling to share their lifestyle information and 45% are unwilling to share their mental health data. While opinions on sharing personal medical history are almost equally divided; 35% are willing, 35% are unsure, and 31% are unwilling. The only category of data that most participants are willing to share is biometric data. Although the number remains relatively low, being at only 38%.

Considering that one of the key elements of the new EHDS initiative is the creation of national bodies to manage health data governance, these results provide an interesting point for reflection. Under the EHDS, citizens will have to share their data with these government-controlled bodies, which will then act as gatekeepers.

The results of the survey showed that participants are less willing to share personal health information with the government. This could present a problem for the implementation of the EHDS. In fact, if people are unwilling to share their personal health information, it will be hard to create a digitalized and cohesive European health system.

Furthermore, one of the participants reached out to me with some questions about the work. They then talked about their experience with sharing personal health data.

This participant suffers from a chronic illness and their doctor strongly advised them to avoid disclosing this information if possible. For example, the doctor told them that it is better not to share this kind of data with employers during job search because the employer may see it as a potential "risk of absence", due to crises or treatment, and therefore exclude them from the selection process. Another example that the participant mentioned is that if the government knew about their chronic illness, they would probably have a harder time, than a non-chronically ill person, to obtain public funding for a project. This is because it would present a higher risk for the government as the founder of the project is more likely to have serious health problems. Lastly, the participant also stated that they had to pay an additional premium when borrowing money to acquire a property as there is usually a medical questionnaire for mortgage loans. Therefore, a national and European entity and dataset that would know that they have a chronic illness would scare them. However, it is to be noted that they would not mind giving their health data directly to researchers in the hopes of helping the advancement of medicine.

As it can be seen, the concerns of this participant are aligned with those discussed by other studies and more precisely in the second chapter of this work. Therefore, to transform the EHDS into reality, it is necessary to ensure that these government agencies are transparent and non-discriminatory in their work, and that data is protected and not misused or shared with any unauthorized party.

Finally, it would be interesting to carry out further studies on this subject, to better comprehend the level of trust citizens have in their government and their willingness to share information with state institutions. These studies could also help understand how to increase trust and propensity to share.

Medical staff:	biometric data	medical history	clinical data	lifestyle data	mental health
Yes	96,45 %	95,43 %	92,89 %	85,79 %	85,79 %
Maybe	2,54 %	3,05 %	4,06 %	9,14 %	10,15 %
No	1,02 %	1,52 %	3,05 %	5,08 %	4,06 %

Researchers:	biometric data	medical history	clinical data	lifestyle data	mental health
Yes	58,88 %	54,82 %	52,79 %	57,87 %	48,73 %
Maybe	31,98 %	34,52 %	33,50 %	29,95 %	32,99 %
No	9,14 %	10,66 %	13,71 %	12,18 %	18,27 %

Friends:	biometric data	medical history	clinical data	lifestyle data	mental health
Yes	46,70 %	42,13 %	34,52 %	60,41 %	31,98 %
Maybe	37,06 %	42,13 %	40,61 %	28,93 %	46,70 %
No	16,24 %	15,74 %	24,87 %	10,66 %	21,32 %

Government:	biometric data	medical history	clinical data	lifestyle data	mental health
Yes	38,07 %	34,52 %	30,96 %	30,46 %	19,29 %
Maybe	35,53 %	35,03 %	32,99 %	28,93 %	36,04 %
No	26,40 %	30,46 %	36,04 %	40,61 %	44,67 %

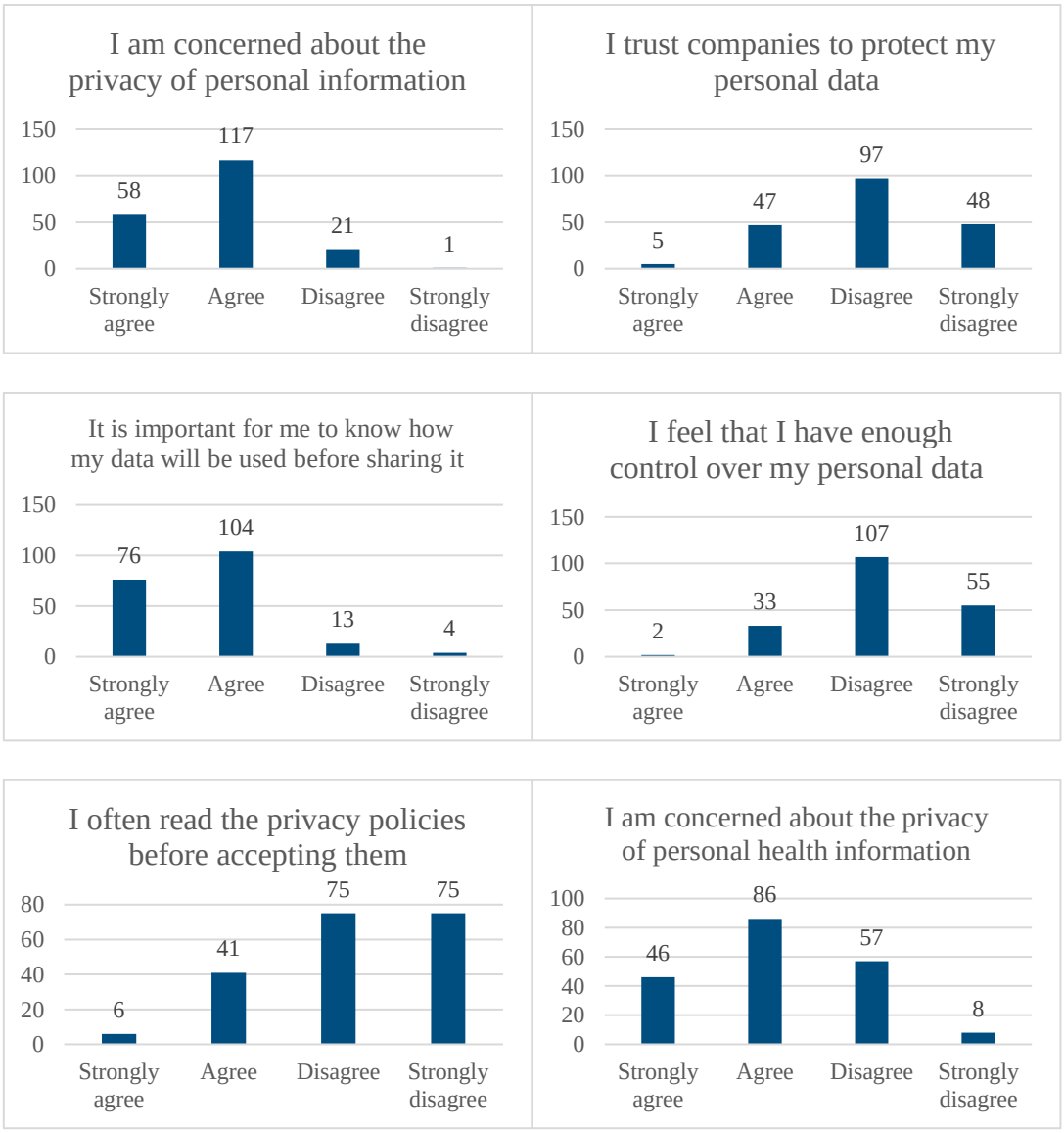
Table 2: Willingness to share data with various recipients

Continuing on the survey, the last two sections aimed at better understanding people's attitudes towards data privacy and their knowledge of the main European data protection legislation.

In the fifth section, participants were presented with six different statements, and they were asked to assess their level of agreement with each one on a Likert scale consisting of four alternatives: i) Strongly Agree; ii) Agree; iii) Disagree; and iv) Strongly Disagree.

The results show that most of the participants, 175 out of 197, are concerned about the privacy of their personal data. Surprisingly, this number decreases when asked about their concern for the privacy of personal health information. Only 132 out of 197 agreed (or strongly agreed) with the statement, indicating concern for the issue.

In line with these privacy concerns, the results also show that the majority of the participants (145 out of 197) do not trust companies to protect their personal data. Furthermore, most participants (165 out of 197) feel like they do not have enough control over their personal data, and an even higher number of participants (180) would like to know how their information is being used. Despite these concerns, 150 participants admitted that they often do not read privacy policies before accepting them. This discrepancy could be due to time constraints, or to the length and complexity of the privacy policies.



Graph 1: Answers to the fifth section

Lastly, the final section was designed to provide an overview of people's knowledge of the main European legislation on the sharing of data. Specifically, it aimed at analyzing whether individuals are aware of the GDPR and their rights under this regulation. The expectation for this section is that not many people will be familiar with the GDPR and their rights. Additionally, it is expected that even fewer people will know about the EHDS, as it is relatively new.

The survey has proven these expectations to be correct. In fact, out of the 197 participants, only a bit less than 50% knew about the existence of the GDPR. Indeed, 95 participants knew about the regulation, 90 admitted not to know about it and the remaining 12 people maybe knew about it. However, only 16% of the participants knew about their rights under the GDPR.

Furthermore, one can observe a slight discrepancy between the answers of the participants who are over 40 years old and the answers of the participants younger than 40 years old. In fact, 62% (9 out

of 13 people) of the over-40 population answered that they knew what the GDPR is, while, on the other hand, 47% (87 out of 184) of the population under 40 knew what it was. However, it is important to underline that this result is not significant due to the limited availability of data, but it could be an interesting starting point for future research. Indeed, it could be interesting to see if older generations have more knowledge about EU regulations on data protection than younger generations.

Lastly and as expected, the number drastically decreases when talking about the EHDS. In fact, only 4 participants out of the 197 knew about the EHDS initiative.

It is important to underline that this survey comes with some limitations as the considered population is small and limited to a particular age group.

An experiment

To better understand people's propensity to share personal health data and how they would react to the introduction of a third party, hence national agencies, Professor Di Cagno, Daniela, Professor Savona, Maria, and PhD candidate Lisovaia, Anastasiia have designed the following experiment. This experiment is expected to be carried out in the upcoming months at the Cesare Lab of LUISS University.

The experiment will consist of two treatments. Both of which will start with a 12-question questionnaire. Participants will be asked about their willingness to share personal data, including personal health data, and more generic questions. In addition, this questionnaire will give each participant 12 tokens.

Both treatments will then take part in a trust game. This type of experiment is very useful to better understand people's willingness to trust others with personal data. It can help determine to what extent people are willing to share information and how much they trust different entities.

In the first treatment, the participants will be divided into two groups: trustors and trustees. The trustor decides how many of their tokens to give to the trustee. This amount is then multiplied by a factor k > 1, equal for all, before being sent to the trustee. The trustee then will have to decide what to do with the tokens they just received. They can either reciprocate the trust by sending any amount of tokens back to the trustor, or they could share the tokens with another person, a friend, or simply do nothing. This process will be repeated three times, and each time the pairs of trustor-trustee will change. To better simulate the concept of "friends", the participants will be divided into groups of four, the other part of the people will be considered as friends, hence with whom the trustee can share the tokens received.

After this, the participants will take part in a public good game. This will help to understand how much people are willing to contribute to a common pool. As mentioned above, this is essential when considering the EHDS initiative since it is a public good. Each player will decide how much of their endowment to contribute to the common pool and will have a profit of $y = a_i + b \sum_{i=1}^{n} c_i$

Where c_i represents the contribution of player i to the common pool, b is the marginal per capita return from the public good, a_i is how much of their endowment the participant i keeps for themselves, and lastly n is the number of players.

After the public good game, participants will be presented with another 12-question questionnaire, followed by another round of the trust game. The aim of this is to assess how people's level of trust and willingness to share has changed throughout the experiment.

On the other hand, after the first questionnaire, the second treatment will also participate in a trust game. This time, however, the participants will be playing with a computer that represents the government. There will be three rounds. In the first one, the government will not reciprocate trust, and will not give back to the trustor. In the second and third rounds, the amount that the government, hence the trustee, returns will be completely random. The aim behind this is to better simulate reality. In practice, one might share their personal health data with the national bodies created by the EHDS, but the benefits of doing so may only arrive in a second moment and may vary due to various reasons, i.e., how medicine is advancing.

As seen in the survey results, the willingness to share personal health data with the government is lower than the willingness to share with other recipients. This poses a significant challenge to the implementation of the EHDS as such a thing is essential for it to work. Therefore, this experiment will help to better understand this issue and will provide further insights into people's behavior.

Conclusion

In a world that is becoming more and more digitalized, the European Union aims to become a global leader in the digital age. For this reason, it has started a substantial digital transformation. Indeed, the EU wants to create a genuine single market for data under the European Data Strategy.

To achieve this single market for data, the EU wants to create several data spaces in the main economic sectors and public domains. As seen throughout the thesis, the health sector is one of the first areas to undergo this digitalization process.

For this reason, the European Commission presented a proposal for the European Health Data Space in 2022. The goal of this framework is to create a cohesive European digital health system that would ensure a rapid answer to any future threats, would support medical research and innovation, and would ensure better and cross-border healthcare to patients.

The reason to do so is that the sharing of personal health data can be very beneficial both for patients and organizations, but also for Member States.

Healthcare providers would be able to access the patient’s detailed and accurate clinical, genetic, and pharmaceutical history. This would allow the medical staff to make more informed decisions since there would be no missing data in the patient's history. Furthermore, this information could be easily accessible for health professionals in case of emergency, for example, if a patient is unconscious.

Additionally, the sharing of a patient's data can help avoid duplication of tests. This happens when patients change doctors or go to multiple facilities without having all the previous health information available. Therefore, avoiding carrying out the same tests multiple times could save money since these tests are very expensive to run, and it could also allow researchers to be reallocated.

Furthermore, the re-use of digital health data for research purposes could drastically change the medical field. Indeed, it would provide larger and more representative datasets for researchers, and

this would improve the quality and reliability of their studies. Moreover, it would help identify the most cost-effective therapy, which could save money. It could also strengthen the European Union's response to future health crises, i.e., a pandemic.

However, these benefits are usually overlooked by individuals as their concerns take precedence.

Pelteret & Ophoff (2016) point out that individuals will encounter incomplete information, bounded rationality, and psychological distortions when trying to protect their data and privacy. An example of incomplete information could be privacy policies, which often just mention broad categories of recipients with which the data could be shared, without specifying any company or institution name. Furthermore, individuals are, typically, not able to fully process all the information they receive, and they might be unable to properly calculate and compare payoffs.

Another concern many individuals have is the potential discrimination as a result of group profiling through the organization and the combination of personal and non-personal data (resulting in big data). This big data could also lead to stereotyping by associating certain health risks or diseases with a specific demographic group, and that, even when there is no causation.

In the literature, these concerns were best summarized by Mason in 1986, back when he created a framework called PAPA: privacy, accuracy, property, and accessibility.

However, it is important to underline that these issues are tackled by European Union legislation. Indeed, privacy is the central component of many EU legislation, like the GDPR and the EHDS, which focus on individuals' rights to privacy and set strict guidelines for the sharing of personal data.

Furthermore, in this thesis, an analysis of existing research and experiments has been conducted to better understand people's willingness to share their personal health data.

It is important to underline that this topic is relatively new, so there is not much research available.

In general, studies have shown that the concerns mentioned above can affect people's willingness to share personal health information. Indeed, increased privacy concerns usually diminish the willingness to share. Furthermore, there are different factors that can influence people's perception of privacy concerns. For example, perceived privacy control can impact it, as an increased perceived privacy control usually reduces privacy concerns. Moreover, privacy concerns are also increased by an increase in perceived privacy risks. However, it is important to highlight that several different studies have shown that perceived benefits outweigh the perceived risks, and this reduces individuals' privacy concerns. Therefore, it could be useful to underline the benefits that derive from sharing personal health information in order to promote the sharing of such information. Furthermore, it was also found that as trust decreases, concerns usually increase.

In addition, studies have also found that individuals tend to value, to different extents, the level of involvement they have in the decision-making process about health data sharing, access, use, and reuse. Therefore, this represents another important characteristic that affects people's willingness to share information.

Additionally, health data sensitivity also raises important privacy concerns among individuals. Indeed, the more a piece of information is valued as sensitive, the more people will be concerned about privacy.

Therefore, it is essential to guarantee people's participation in managing the privacy of their own health data and to strengthen trust relations with consumers. For example, this could be done by writing clearer privacy policies.

Finally, a survey was conducted in order to better understand people's willingness to share personal health information. This survey obtained 287 answers, out of which 84 were incomplete and 8 were from non-EU participants; leaving 197 valid answers.

On the one hand, the survey found that the participants were inclined to share general information (i.e., email address, phone number, health information) if there were limitations on who the recipient

was and how much and what information was being shared. However, on the other hand, the majority of the people were unwilling to share financial information.

Furthermore, it was also found that the majority of the participants were willing to share their personal health data with healthcare providers. However, the number of participants willing to share such information with other recipients (i.e., researchers, friends, and the government) decreased. From what has been seen, the participants were the most reluctant to share their personal health data with the government. Considering that one of the key elements of the EHDS is the creation of national Health Data Access Bodies to manage data sharing, these results could present a serious problem and should be further investigated to understand the reason for that and what can be done about it.

Additionally, the survey revealed that less than 50% of the participants knew about the GDPR, and only 16% of the participants knew about their rights under the GDPR. Furthermore, when talking about the EHDS, the number of participants knowing about the European Union initiative drops to a very low 4 participants out of 197.

As it can be seen, these numbers are significantly low, and this could negatively impact the implementation of the EHDS. Indeed, it is important that people know about the EU legislation safeguarding their data protection rights in order for them to take well informed decisions because, without this knowledge, they may become even more reluctant to share their information.

However, it is important to note that this survey presents some limitations due to the low number of answers, and the lack of a diverse age group as a majority of its participants were aged between 19 to 27 years old.

Therefore, in light of these limitations, it would be interesting to run the same experiment and/or survey in the different Member States of the EU. Not only this would ensure a larger dataset for each country, but it would also help understand the societal differences there are between countries in the EU, providing guidance on how to strengthen the EU digital health system. Furthermore, it would also be interesting to study the differences between younger and older generations. Indeed, younger people are, generally, more familiar with technology so they might find it easier to use the EHDS.

However, they are also more aware of privacy risks, hence they might be more cautious when sharing data.

In conclusion, the survey revealed that people are very willing to share their personal health data with healthcare providers. Their willingness decreases with other recipients, respectively, researchers, friends, and government. Although this presents a good starting point for the implementation of the EHDS, it is not sufficient as individuals will have to share their personal information with government-run agencies. Therefore, it is fundamental to increase people's trust in the governments, diminish their privacy concerns, and increase their knowledge of the GDPR and the EHDS.

Bibliography

Ackfeld V.; Guth W. (2019). “Personal Information Disclosure under Competition for Benefits: Is Sharing Caring?”. MPI Collective Goods Discussion Paper, No. 2019/4.

Alós-Ferrer C.; Farolfi F. (2019). “Trust Games and Beyond”. Front. Neurosci., Vol. 13.

Berg J.; Dickhaut J.; McCabe K. (1995). “Trust, Reciprocity, and Social History”. Games and Economic Behavior, Vol. 10(1), pp 122-142.

Bosanac D.; Stevanovic A. (2022). “Trust in E-Health System and Willingness to Share Personal Health Data. Studies in health technology and informatics”, Vol. 289, pp 256–259.

Cambridge Dictionary (n.d.). “big data”. Retrieved from https://dictionary.cambridge.org/dictionary/english/big-data#google_vignette

Cherif E.; Bezaz N.; Mzoughi M. (2021). “Do personal health concerns and trust in healthcare providers mitigate privacy concerns? Effects on patients' intention to share personal health data on electronic health records”. Social science & medicine, Vol. 283, 114146.

Coleman J. (1990). “Foundations of Social Choice Theory”. Cambridge, MA: Harvard Univ. Press.

Council of Europe (1950). “Convention for the Protection of Human Rights and Fundamental Freedoms and Protocol”.

Council of Europe (n.d.a). “The Convention in 1950”. Retrieved from https://www.coe.int/en/web/human-rights-convention/the-convention-in-1950

Council of Europe (n.d.b). “Right of Privacy”. Retrieved from https://www.coe.int/en/web/impact-convention-human-rights/right-to-privacy

Courbier S.; Dimond R.; Bros-Facer, V. (2019). « Share and protect our health data: an evidence based approach to rare disease patients’ perspectives on data sharing and data protection - quantitative survey and recommendations”. Orphanet J Rare Dis, Vol. 14, No. 175.

Croson R.; Buchan N. (1999). "Gender and Culture: International Experimental Evidence from Trust Games." American Economic Review, Vol. 89 (2), pp 386–391.

de Terwangne C. (2021). “Council of Europe convention 108+: A modernised international treaty for the protection of personal data”. Computer Law & Security Review, Vol. 20, 105497.

Dienlin T. (2023). “Privacy Calculus: Theory, studies, and new perspectives.” In S. Trepte & P. Masur (Eds.), The Routledge Handbook of Privacy and Social Media. Routledge.

Dimodugno M.; Hallman S.; Plaisent M.; Bernard P. (2021). “The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach”. Journal of Physics: Conference Series, Vol. 2090, 012017.

Dinev T.; Albano V.; Xu H.; D’Atri A.; Hart P. (2016). “Individuals’ Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective”. In: Gupta, A., Patel, V., Greenes, R. (eds) Advances in Healthcare Informatics and Analytics. Annals of Information Systems, Vol. 19, Springer, Cham.

European Commission (2023). “Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-US Data Privacy Framework”. Official Journal of the European Union, L 231/228. Retrieved from https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj

European Commission (2024). “Commission welcomes European Parliament's adoption of the European Health Data Space and regulation on substances of human origin”. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_24_2250

European Commission (2024). “Factsheet on European Health Data Space”. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/FS_24_1347

European Commission (n.d.). “European Health Data Space”. Retrieved from https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

European Observatory on Health Systems and Policies; Hendolin M. (2021). “Towards the European health data space: from diversity to a common framework”. Eurohealth, Vol. 27, No. 2, pp 15-17.

European Parliament and Council of the European Union. (1995). “Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data”. Official Journal of the European Communities, L 281/31. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

European Parliament and Council of the European Union. (2016). “Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”. Official Journal of the European Union, L 119/1. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament and Council of the European Union. (2021). “Proposal for a regulation on the European Health Data Space”. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

European Parliament and Council of the European Union. (2022). “Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)”. Official Journal of the European Union, L 277/1. Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Fernando J. (2024). “What Are Public Goods? Definition, How They Work, and Example”. Retrieved from https://www.investopedia.com/terms/p/public-good.asp

Gajanayake R.; Iannella R.; Sahama T. (2014). “Consumer acceptance of accountable-eHealth systems.” Studies in Health Technology and Informatics, Vol. 205, pp 980-984.

Graham M. (2023). “Data for sale: trust, confidence and sharing health data with commercial companies”. Journal of medical ethics, Vol. 49(7), pp 515–522.

Hansen J.; Kirwan M.; Kroenman M.; van Veen E-B.; Verheij R., Verhoeven E.; Wilson P. (2021). “Assessment of the EU Member States’ rules on health data in the light of GDPR”. Retrieved from https://health.ec.europa.eu/system/files/2021-02/ms_rules_health-data_en_0.pdf

Hoofnagle C. J.; van der Sloot B.; Borgesius F. Z. (2019). “The European Union general data protection regulation: what it is and what it means”. Information & Communications Technology Law, Vol. 28(1), pp 65–98.

Hustinx P. (2014) “EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation”. Retrieved from https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en

Hussein R.; Balaur I.; Burmann A.; et al. (2024). “Getting ready for the European Health Data Space (EHDS): IDERHA's plan to align with the latest EHDS requirements for the secondary use of health data [version 1; peer review: awaiting peer review].” Open Res Europe 2024, 4:160.

Ingham S. (n.d.). “Public good”. Retrieved from https://www.britannica.com/money/public-good-economics

Isaac R. & Walker J. (1988). “Group size effects in public goods provision: The voluntary contributions mechanism”. Q. J. Econ, Vol. 103(1), pp 179–199.

Kovacs R. J.; Lagarde M.; Cairns J. (2019). “Measuring patient trust: Comparing measures from a survey and an economic experiment”. Health economics, Vol. 28(5), pp 641–652.

Kim K. K.; Joseph J. G.; Ohno-Machado L. (2015). “Comparison of consumers’ views on electronic data sharing for healthcare and research”. Journal of the American Medical Informatics Association, Vol. 22, No. 4, pp 821–830.

Kreps D. M. (1990). “Corporate Culture and Economic Theory.” In Perspectives on Positives Political Economy (J. Alt and K. Stepsle. Eds.). Cambridge: Cambridge Univ. Press.

Ledyard J. O. (1995). “Public goods: a survey of experimental research”. In The Handbook of Experimental Economics (eds Kagel, J. & Roth, A.), pp 111–194, Princeton University Press.

Menon G.; Block L.; Ramanathan S. (2002). “We're at As Much Risk As We Are Led to Believe: Effects of Message Cues on Judgments of Health Risk”. Journal of Consumer Research. Vol. 28, pp 533-49.

Menon G.; Raghubir P.; Agrawal N. (2006). “Health Risk Perceptions and Consumer Psychology”. SSRN Electronic Journal.

Mildebrath H. (2023). “Understanding EU data protection policy”. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf

Moon L. A. (2017). “Factors influencing health data sharing preferences of consumers: A critical review”. Health Policy and Technology, Vol. 6(2), pp 169-187.

Mulder T.; Tudorica M. (2019). “Privacy policies, cross-border health data and the GDPR”. Information & Communications Technology Law, 28(3), pp 261–274.

Nwebonyi N.; Silva S.; de Freitas C. (2022). « Public Views About Involvement in Decision-Making on Health Data Sharing, Access, Use and Reuse: The Importance of Trust in Science and Other Institutions”. Frontiers in public health, Vol. 10, 852971.

Olson M. (1965). “Logic of Collective Action: Public Goods and the Theory of Groups.” Harvard University Press

Ostherr K.; Borodina S.; Bracken R.; Lotterman C.; Storer E. (2017). “Trust and privacy in the context of user-generated health data”. Big Data & Society, Vol 4.

Otten K.; Frey U.J.; Buskens V.; Przepiorka W.; Ellemers N. (2022). “Human cooperation in changing groups in a large-scale public goods game”. Nature Communications, Vol. 13, No. 6399.

Pelteret M.; Ophoff J. (2016). “A review of information privacy and its importance to consumers and organizations”. Informing Science: the International Journal of an Emerging Transdiscipline, Vol. 19, pp 277-301.

Pereda M.; Tamarit I.; Antonioni A.; Cuesta J.A.; Hernández P.; Sánchez A. (2019). “Large scale and information effects on cooperation in public good games”. Scientific Reports, Vol. 9, No. 15023.

Platt J.; Kardia S. (2015). “Public trust in health information sharing: implications for biobanking and electronic health record systems”. Journal of personalized medicine, Vol. 5(1), pp 3–21.

Poullet Y. (2006). “EU data protection policy. The Directive 95/46/EC: Ten years after”. Computer Law & Security Review, Vol. 22(3), pp 206-217.

Quinn P.; Ellyne E.; Yao C. (2024) “Will the GDPR Restrain Health Data Access Bodies Under the European Health Data Space (EHDS)?” Computer Law & Security Review, Vol. 54, 105993.

Rafique G. (2017). “Personal Information Sharing Behavior of University Students via Online Social Networks.” Library Philosophy and Practice, Vol. 2017.

Shabani M.; Yilmaz S. (2022). “Lawfulness in secondary use of health data: Interplay between three regulatory frameworks of GDPR, DGA & EHDS”. Technology and Regulation, Vol. 2022, pp 128-134.

Shen N.; Bernier T.; Sequeira L.; Strauss J.; Silver M. P.; Carter-Langford A.; Wiljer D. (2019). “Understanding the patient privacy perspective on health information exchange: A systematic review”. International journal of medical informatics, Vol. 125, pp 1–12.

Slokenberga S. (2022). “Scientific research regime 2.0? : How the proposed EHDS Regulation may change the GDPR Research Regime”. Technology and Regulation, pp 135–147.

Tzanou M. (Ed.). (2021). “Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses”. Routledge

Vodicka E.; Kim K.; Devine E. B.; Gnanasakthy A.; Scoggins J. F.; Patrick D. L. (2015). “Inclusion of patient-reported outcome measures in registered clinical trials: Evidence from ClinicalTrials.gov (2007-2013)”. Contemporary clinical trials, Vol. 43, pp 1–9.

Wiewiórowski W. R. (2024). “EDPS formal comments on the draft Implementing Regulation laying down procedural rules for the cooperation with EMA as regards the joint clinical assessment and joint scientific consultation”. Retrieved from https://www.edps.europa.eu/data-protection/our-work/publications/formal-comments/2024-08-28-edps-regulation-procedural-rules-cooperation-ema-regards-joint-clinical-assessment-and-joint-scientific-consultation_en

Wu W-Y.; Sukoco B. M. (2010). “Why should I share? examining consumers' motives and trust on knowledge sharing”. Journal of Computer Information Systems, Vol. 50(4), pp 11-19.

Zaeem R. N.; Barber K. S. (2020). “The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise”. ACM Transactions on Management Information Systems (TMIS), Vol. 12(1), No. 2, pp 1-20.

Appendix

Appendix 1: The Survey

Introduction and presentation

Hello, I am Virginia Poliseno and I am a student in the master's program ‘Economics and Finance’ at LUISS University.

I am conducting a research for my master’s thesis regarding the European Union’s digital health system and people's willingness to share personal health information.

I would be grateful if you could take a few minutes of your time to answer a few questions. Your answers to this study will be used for academic purposes only, will be treated confidentially, and will remain completely anonymous.

Please answer as openly and honestly as possible; there are no right or wrong answers.

Thank you for your answers.

First Section: Sharing of general information

Would you share **your email address**?

- Yes, no matter with whom.
- Yes, but with limitations.
- No.

Would you share **your phone number**?

- Yes, no matter with whom.
- Yes, but with limitations.
- No.

Would you share **your location data (geolocation)?**

- Yes, no matter with whom.
- Yes, but with limitations.
- No.

Would you share **your financial information**?

- Yes, no matter with whom.
- Yes, but with limitations.
- No.

Would you share **your health information**?

- Yes, no matter with whom.
- Yes, but with limitations.
- No.

First Section (*optional, if answered 'Yes, but with limitations' at least once*): continued

What limitations would you consider when sharing your personal data?

- It depends on whom the information is shared with.
- It depends on the quantity of information that is being shared.
- Both of the above mentioned.
- Other: *[Insert Answer]*

Second Section: Sharing of information with whom?

Would you share the following information with...?

	Healthcare providers (i.e., doctors, nurses, laboratories, etc.)			Government agencies (public health authorities, etc.)			Researchers			Friends		
	Yes	No	Maybe	Yes	No	Maybe	Yes	No	Maybe	Yes	No	Maybe
Biometric data (i.e., health, weight, blood pressure, heart rate)												
Medical history (i.e., chronic conditions, allergies, prescription medications, past surgeries or treatments)												
Clinical data (i.e., diagnoses, laboratory results)												
Lifestyle and behavioral data (i.e., dietary habits, exercise habits, sleep schedule)												
Mental health data (i.e., diagnoses, treatments and medications)												

Third Section: Demographical questions

What is your gender?

- Male
- Female
- Other / Prefer not to say

How old are you?

[Insert Answer]

What is your nationality?

[Insert Answer]

What is the highest level of education you have completed?

- High school diploma
- Bachelor's degree
- Master's degree
- PhD

Fourth Section: Attitude towards data privacy

(Please rate your level of agreement with each question using the scale provided.)

I am concerned about the privacy of my personal information.

- Strongly disagree
- Disagree
- Agree
- Strongly agree

I trust companies to protect my personal data.

- Strongly disagree
- Disagree
- Agree
- Strongly agree

It is important for me to know how my data will be used before sharing it.

- Strongly disagree
- Disagree
- Agree
- Strongly agree

I feel that I have enough control over my personal data.

- Strongly disagree
- Disagree
- Agree
- Strongly agree

I often read the privacy policies before accepting them.

- Strongly disagree
- Disagree
- Agree
- Strongly agree

I am concerned about the privacy of my personal health information.

- Strongly disagree
- Disagree
- Agree
- Strongly agree

Fifth Section: GDPR awareness and consent

Do you know about the GDPR?

- Yes
- No
- Maybe

Do you know what rights you have under the GDPR?

- Yes
- No
- Only some

Have you ever exercised your rights to access, modify, or delete your data under GDPR?

- Yes
- No
- Unsure

How confident are you that companies and institutions comply with GDPR when handling your data?

- Not at all confident
- Slightly confident
- Moderately confident
- Very confident

How clear and easy do you think it is to give or withdraw consent when sharing data online?

- Not at all clear and easy
- Slightly clear and easy
- Moderately clear and easy
- Very clear and easy

Do you know about the EHDS initiative?

- Yes
- No

- Maybe

Concluding comment and thanks

We thank you for your time spent taking this survey.

Your response has been recorded.