MASTERARBEIT | MASTER'S THESIS

Titel | Title

Protecting Privacy in The Digital Age: An Investigation of The General Data Protection Regulation's Impact on The Market and Ethical Practices of Personal Data.

verfasst von | submitted by

Michael Rowan Bowers

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien | Vienna, 2024

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 066 642
Studienrichtung lt. Studienblatt | Degree programme as it appears on the student record sheet:	Masterstudium Philosophy and Economics
Betreut von | Supervisor:	Univ.-Prof. Dr. Maarten Janssen

Table of Contents

1 Introduction

In the age of digital connectivity and the persistent collection of personal data, where every click, swipe, and scroll leaves a digital trace, the issue of privacy has become a central topic in academic and societal discussions. The General Data Protection Regulation (GDPR), a landmark legislation that took effect in May 2018, is a significant step in safeguarding personal data and ensuring privacy within the European Union. This paper delves into the ethical and market implications of the GDPR, examining its impact on data protection, individual rights, and organisational responsibilities.

Privacy is especially relevant today due to the overwhelming number of online interactions individuals have daily. Understanding the role of the GDPR in protecting individuals' privacy provides valuable insights into the ethical and economic impacts of regulations within the digital market.

This paper seeks to provide a comprehensive understanding of the GDPR's impact by integrating philosophical and economic perspectives and shedding light on the balance between ethical principles and market realities in the realm of data protection. Led by the question: **To what extent does the General Data Protection Regulation (GDPR) uphold the fundamentals for individual's privacy protection while balancing the need for market efficiency?**

This paper begins by examining the philosophical perspectives and ethical implications of privacy. It underscores the importance of privacy as a fundamental right, the protection of which is crucial. Once the foundations are established, privacy is then defined as control over personal information, with control, consent, and autonomy being key factors to safeguarding individuals' rights.

In the chapter on the economics of privacy, this paper delves into the economic perspective of privacy, incorporating theoretical investigations and empirical insights from previous research to provide a comprehensive overview of the economics of privacy.

The GDPR chapter highlights how the GDPR distinguishes itself from its predecessors through its key principles and consent through design by default. It emphasizes protecting individuals' rights with robust data security mandates while considering market implications.

2 Philosophical Perspective and Ethical Implications of Privacy

This chapter constructs an understanding of privacy that is suited to the digital world, in particular, the exchange of personal information. First, the chapter establishes privacy as a right. Setting up privacy as a right allows for a legal connotation rather than just a moral notion, which is important for regulations as it allows for the perpetrators of privacy to be held accountable for their violations. Once privacy is established as a right it is then reconceptualised as control over information. Therefore, creating a normative perspective for privacy (as a right) and an operational perspective (privacy is control over information) in order to apply the theory to the digital world.

After establishing a definition of privacy, the chapter dives into the behaviours of individuals and how they change under surveillance. Therefore, making the definition more applicable to the digital world in order to help produce an understanding of the fundamentals of individuals' privacy protection.

2.1 An Understanding of Privacy

2.1.1 Privacy as a Right

According to Thomson (1975, p.296), to understand privacy, we must first find instances where an individual's privacy is violated by contrasting instances where privacy is respected. In her analysis, Thomson (1975, p. 297) first considers a scenario of overhearing a couple argue through an open window. While this act of listening may be considered impolite Thomson (1975, p. 297-8) suggests that there is no privacy violation occurring. However, when a listening device is used to eavesdrop through a closed window, she asserts that privacy is indeed breached, as the arguing couples attempt to use their right to not be observed by others within their own home is disregarded. One could suggest that the argument resides in the fact that by closing or opening the window the couple is transferring

their argument from a private to public space. Hence, their right to not be heard within their property is waived once the window opens.

Additionally, Thomson (1975, p. 298) provides a scenario where an individual owns a pornographic picture which they deliberately take steps to safeguard by storing it in a locked safe and viewing it only under conditions when they know they are alone. In this scenario, an X-ray device is used to view the picture through the walls of the house and safe. Similar to the previous example it is a violation of the individual's privacy as they have property rights within their home and furthermore over the picture and therefore can decide who is allowed to view it. The fundamental difference between the two scenarios is that the first involves a physical space where there is an ambiguous line between public and private action whereas the second example is strictly a private space in which the property rights of the individual are being violated. Additionally, the picture is the individual's private property and therefore attached with its own set of property rights.

Benn's (1988, p. 266-277) coherentism view would claim that in Thomson's examples above, privacy is violated in all cases because, firstly, individuals have an inherent right to privacy and secondly, the information gathered through hearing the argument or seeing the picture reveals information about the individual's personhood which is a violation of said privacy. Benn (1988, p. 268) establishes privacy as context-relative and normative and states that it should be protected as a standalone right that is not derived from any other right. When the window is closed although Thomson and Benn's reasoning is different it comes to the same conclusion that a violation has occurred, for Thomson it is attached to property rights and for Benn it was a private conversation and therefore shouldn't have been listened to. However, unlike Thomson's, Benn's reasoning would also claim that with the window being open the violation of privacy is still present.

Benn's theory on privacy and how to protect it is rooted in defining what is and isn't private. Such a task is notoriously hard given that individuals may have a unique understanding to what is private and what isn't. Whereas Thomson's view on privacy allows for the protection of privacy to be based on property rights and therefore have a cleaner practicality as a binding legal base when used within regulations and laws. In Thomson's line of reasoning privacy exists within ones right to not be listened to in their own house (private space) which is only a granted right through the overarching protected right of property rights. Whereas Benn's

reasoning is the right to not be listened to in a private space exists within privacy. Benn (1988, p. 266-8) claims that privacy is inherently beneficial for individuals, as it ensures their choices are respected and ultimately enhances their well-being. Therefore, it is essential to respect others' privacy by refraining from infringing upon it.

According to Thomson (1975, p.307-10), there are clusters of rights that include within them multiple rights. For example, property rights would include intellectual property rights, physical property rights, selling rights, buying rights, and privacy, to name a few. Within the cluster of privacy rights would be the right to be left alone, the right to freedom, and the right to autonomy, among others. Thomson (1975, p.309-10), therefore, claims there are no rights in the right-to-privacy cluster that are not in some other right cluster. In the chapter on the GDPR we will return to this idea of clusters of rights as the GDPR has its own rights that fall under the right to privacy. This paper takes a normative stance in claiming that privacy is a right that may be connected to several other rights and could exists within other clusters of rights. If privacy is understood as a right, then individuals' privacy could be protected by the law, as other rights are.

In the next sub-chapter, we will discuss privacy as control over information. Viewing privacy as a sub-right of property will allow us to understand personal data or information as property of the individual and therefore should be protected as such. Therefore, given that Thomson's approach grants a binding legal basis, continuing we will view privacy as a sub-right of property right therefore granting it to be protected.

2.1.2 Privacy as Control Over Information

Building on the conceptualization of privacy as a sub-right Thomson borrows a noteworthy definition of privacy from Richard Parker's 1974 account of defining *privacy* as "control over when and by whom the various parts of us can be sensed by others" (Thomson, 1975 p.304 *footnotes*). Solove (2002, p.1112) argues that *control* in this sentence, particularly regarding information, can be understood as ownership. Thomson (1975, p.305) explains *parts of us* as the products of our bodies, including objects only accessible to us, therefore the information of oneself. The definition can be broken down further into

ownership of information of oneself. Such a conception of privacy parallels Locke's (2016, p.25) idea of property being the fruit of one's labour and therefore, an extension of self. The expansion of property rights that Locke formed created the understanding of intellectual property law. Solove (2002, p.1111-3) claims that property rights are gained when something emanates from oneself. Hence, information could be seen as property and therefore, protected by property rights.

Control-over-information essentially refers to the ability of individuals to have the authority to dictate the movement and usage of information about themselves. This theory suggests a way of safeguarding information from risks by transferring ownership of the individual's information to them directly; therefore, if they choose to share certain information with certain people or entities at particular times, they take responsibility for what comes of that information to a certain extent. Pairing with privacy as a sub-right allows the individual to protect their information through the mechanisms that property rights have protection. Having said that, the control-over-information theory is heavily criticised as a stand-alone conception of privacy. The main criticism comes from the definitions of control and information. According to Solove (2002, p. 1112), control is either understood too narrowly or too broadly by theorists. As understood above, a form of ownership can only be claimed when you assume privacy to be a sub-right within property rights. If we take another stance on the right of privacy, that being an inherent right, we may have different arguments for it to be a form of ownership. Furthermore, the theory fails to determine what types of information should be controlled. Therefore, a bigger criticism of the control-over-information theory comes from the definition of information. For some, information refers to private information, normally associated with personal, sensitive or confidential information, the type of information that individuals would consider intimate or potentially harmful if people they didn't want to know about it knew about it. Other theorists specify information as everything from personal identifiers (name, date of birth) and location data (home address, GPS coordinates) to personal preferences (habits, hobbies). Therefore, the concept of information is way too broad, making seemingly all interactions a transfer of information and potentially a violation. Thomson (1975, p.307) believes that individuals do not possess an unquestionable right to control facts or information about themselves to the extent that no one else will ever know this information. Solove (2002, p.1113) agrees, emphasising the inherent challenge posed by the transferability of information: once disclosed to others, it cannot be withdrawn, unlike physical property. However, both Thomson and Solove emphasise the

importance of individuals having some degree of control over their personal information despite the inherent difficulties in maintaining complete privacy in an interconnected world.

Although these critiques are valid when determining privacy as a general principle, I believe that by combining privacy as control-over-information and privacy as a sub-right, we are left with a dynamic understanding of privacy that can be adapted to multiple different interactions that occur in the digital world. Therefore, we can define privacy as a right of ownership over information distributed by the individual. Information is a context-dependent term; therefore, given that different interactions and transactions occur online, it can be defined in the context in which it finds itself. For example, when using Google Maps, the relevant (but not the only) information being processed is location data in which the individual can decide to allow the tracking of their location to receive the advantage of how long it will take them to get to where they are planning to travel to. Therefore, information about the individual's financial status or social relationships (romantic partners or family situation) is not relevant here and should not be considered a part of the collection of information the individual is willing to give at this time. In some cases, it could be that a collection of different types of information is present simultaneously; this only signifies the importance of such a dynamic understanding of information for the allowance of all three of these scenarios to occur and for the protection of privacy to be granted.

Furthermore, if we assume that privacy is control over information than we must also incorporate an understanding of consent. Burkhardt et al (2022, p.239-252), discuss a model which enhances the ethical understanding of personal information collection. The model suggests that for consent to be valid it must come from an informed individual which is when the individual has fully understood the relevant aspects of an agreement. Such an argument has been provided before and attacked by not incorporating those who agree to pop-ups or cookies without reading or attempting to understand that collection is occurring. If we accept the idea of consent in such a way, then it could be claimed that many collections of information online are unethical as the individual did not take the time to understand to the full extent what was happening. Therefore, Burkhardt et al (2022, p.241-250), raise an ethically significant recognition of those people who share their personal information under certain circumstances, such as clicking the accept all button on a pop-up, are still giving a valid form of consent, if it is given voluntarily and with substantial understanding. Therefore, when visiting a website and a pop-up appears and the individual has the option not only to

accept the terms and conditions but also to not accept them, and assuming that the purpose of the visit to the website is to simply enter it, then it is still satisfied, even if the individual blindly click to accept or not accept the terms, the consent has still been given. However, if the individual must click the accept all button for the website to function, then they are no longer acting voluntarily and instead are being coerced.

Moreover, the rights of the individual are best exercised through consent as a means to control to who and when information is shared. Consent enables individuals to have full power over their data which in turn gives them a greater sense of autonomy in the digital world.

2.2 Behaviour Under Surveillance

Benn (1988, p.272) claims that individuals' choices are confined when they are aware of surveillance. For example, Benn (1988, p.272) refers to a man hitting a donkey. The man only stops hitting the donkey once he is aware that other people are observing him. The man is no longer given the choice to remain unobserved with his continuous actions; therefore, his choice sets are shifted to being observed. The shift happened without consent. However, the observation fundamentally alters the context of his choices, highlighting the significance of being seen versus not being seen in influencing individual decision-making. Still, Benn's argument (1988, p.272) underscores the importance of the man's awareness of being observed while hitting the donkey. This awareness alters his decision-making process within the context of being observed, leading him to stop hitting the donkey. While observation itself may not violate privacy, as highlighted in Thomson's examples, Benn emphasizes that interfering with an individual's autonomy by inducing self-awareness and constraining their choices is a violation. The inherent challenge in this particular section of Benn's argument lies in the nature of public spaces, where privacy is inherently compromised, as Benn (1988, p.276) points out. In the digital world it could be claimed that we are no longer in the private space but only acting in a public space, moreover, always acting observed as opposed to unobserved.

In scenario A, the individual intends to Φ unobserved. They cannot Φ unobserved because they are being observed. Therefore, their new choice set is to Φ or not Φ observed, transformed from infinite possibilities to a limited selection. The individual is now forced to Φ in a way they would not have originally chosen. Even if they Φ the identical same way that they would have without being observed, their personhood, in terms of how they view themself, would be tainted due to the observation and therefore, privacy would be violated. In scenario B, the person intends to Φ unobserved however they Φ observed. Unlike scenario A, in which the individual is aware of being observed, they are now unaware of being observed. The individual, however, can still not Φ with the intention of being unobserved because the outcome remains the same. Yet, the individual's personhood is not harmed as they do not perceive themselves as someone being watched unless they become aware of the observation later on. It could be claimed that by using the internet most people are aware that they are acting observed, mainly by algorithms and cookie collection. In the cases where someone may not know they are acting observed, they are then acting as if they were unobserved, but they are in fact being observed.

2.3 Application to the Digital World

Protecting individual privacy has become a major concern in today's rapidly evolving digital world. As technology advances at an extraordinary pace, the ways in which personal information is collected, processed, and stored have undergone substantial transformations. Therefore, when discussing any regulations designed to safeguard privacy rights, they must be rigorous enough to prevent individuals from losing control over their information. One fundamental aspect of privacy rights in the digital age revolves around the concept of privacy as a sub-right. As the boundaries of collectable information are being tested, it is crucial that privacy and therefore individuals' control over information is protected as their property. Control-over-information theories attached to privacy as a sub-right allow individuals to dictate the flow and usage of their information.

The General Data Protection Regulation (GDPR), implemented by the European Union in 2018, is one of the most robust and most extensive privacy regulations, still active six years after implementation. The GDPR establishes strict guidelines for collecting, processing, and storing personal data, emphasising transparency, informed consent, and individual rights.

Under the GDPR, individuals have the right to access their personal data, request its deletion, and withdraw consent for its processing. Organisations that fail to comply with the GDPR can face significant fines and penalties, underscoring the importance of robust data protection measures.

One aspect that makes the GDPR a robust regulation is its efforts towards transparency in order for individuals to make informed decisions about their privacy and actively empower them to use their right of control over their information. Transparency allows our conception of consent to remain valid even during certain cases whereby the individual does not read nor care about what they are consenting to and chooses to click accept all to gain access to a website. This is achieved through the fact that GDPR allows for consent to be revoked at any time, such as after consenting, you may request that your data be deleted. Ultimately, ensuring that individuals retain control over their personal information in the digital age requires a dynamic approach that combines robust regulatory frameworks, transparent data practices, privacy-enhancing technologies, and individual empowerment initiatives. By prioritising privacy as a fundamental right and implementing comprehensive measures to protect it, we can create a digital ecosystem where individuals' privacy rights are respected, and their personal information remains under their control.

2.4 (Un)Informed Consent

As established, consent gives individuals control over their information (personal data). However, the question that remains is what is informed and uninformed consent? In other words, is it consent if the individual does not fully understand what they are consenting to? The term uninformed refers to individuals ignoring or lightly engaging with privacy policies online. According to Obar and Oeldorf-Hirsch (2022, p.4789-4790), most individuals will accept the privacy policies (terms and conditions) without reading it beforehand, leading to the conclusion that the majority of individuals are uninformed (in the sense that they ignore the text or lightly engage with it) when giving their consent to data collecting, processing and storing. However, the GDPR, according to Degeling et al. (2019, p. 345-346), has improved transparency and given users more control by allowing for the default option to not consent to all data collection. The empirical study showed that it may be that individuals still may not fully understand what they are consenting to. However, they at least have the option to opt-

out later down the line. The issue of uninformed consent is only valid when individuals click to accept all to the data privacy policies. Within the GDPR guidelines, individuals need to be given the option to not consent to the collection of data, and therein is the key to overcoming this problem.

2.5 Closing Chapter Remarks

This chapter established a normative perspective for privacy, as a right and an operational perspective where privacy is control by the individual over their own information. The fundamentals of privacy protection are consent (from the individual), compliance (from the firms), and transparency (from both parties). Therefore, the best way for a regulation such as the GDPR to be effective individuals must continue to have a right to privacy and need to be able to have control over their data. One possible way this can be achieved is by making it a default that information is not shared unless the individual consents first. This ensures that individuals will always have the rights attached to owning and controlling their own data. If the regulation is able to take legal or monetary action against agents that actively violate individuals' privacy in the digital world then individuals right to privacy would also be protected. Overall, the fundamentals of privacy protection rely on the regulation's emphasis on control over data through consent.

3 The Economics of Privacy

The economics of privacy is understanding how privacy protection can be implemented without impeding on the market. Forming the balance between empowering individuals and fostering information flow, leading to market efficiency. The balance can be found in investigating the transaction and therefore the trade-off between individuals' personal data and what they receive in return. Examples of some transactions of what individuals receive includes, targeted ads, website accessibility, search guidance and overall online convenience. This chapter will break down the economic value and consequences of personal data, discuss

the implication of asymmetric information and the externalities of personal data transactions before explaining the role of a regulation in the market for personal data.

3.1 Economic Value and Consequences

When discussing the economic value of personal data, we must investigate the trade-offs occurring within society when a transaction of data occurs. If we take the theme of secured personal information on one hand, we could conclude that when consumers trust that their online activities and their personal information is secured online, they are more likely to participate in online transactions, which in turn boosts e-commerce and contributes to economic growth. Such a transaction would be a positive trade-off (Acquisti et al., 2016, p.464-71). However, if we assume that due to increased privacy breaches, consumers have lost trust that their personal information is secured, we could, in the same logic as earlier, conclude that this could reduce online activities, thus slowing down economic activities and economic growth. Therefore, there is a value in securing personal data for the individual and for the firm. An alternative value of personal data is what it can transform into. For example, from the firms' point of view collecting personal data on preferences from their customers may allow them to better target advertisements to them that they may be interested in. Likewise, the customers benefit from a personalised marketing system designed to show them products they are interested in. The value aspect from the firms' side is that now they can make precise ads for the customer thus increasing their efficiency and on the customers side they are only being shown things that they are interested in and therefore do not need to waste time on irrelevant products.

With an increase of information comes an increase in developments towards goods and services. Innovation can advance when accurate information about customers is collected and shared therefore driving product differentiation and overall efficiency of the market. In a free market this may look different to a market with strong regulations in place. For example, regulations that do not allow collecting, processing or storing of personal data may not be able to provide the same accurate information about customers to those organizations that would benefit from it. Hence, it is important that a regulation does not completely deny the

collection and processing of data but rather finds a way to minimize the amount of data being collected to only the relevant and necessary data in relation to the purpose for what it is being processed for. Ensuring that only the minimum amount of data required is used which may then carry over benefits to the market and to the individual.

Restricting or allowing the use of data transaction can on one hand, benefit and on the other harm consumers (Acquisti et al., 2016, p. 473-6 *and* Baye and Sappington, 2019, p. 260-2). According to Baye and Sappington (2019, p.261), the impact of transaction data depends on factors such as a platform's ability to match consumers with products, prevention of monopolistic exploitation, and consumer sophistication. Baye and Sappington (2019, p.260-5) identify conditions for maximizing the total welfare platform's preferred privacy policy and the impact of opt-in opt-out mandates. According to Baye and Sappington (2019, p.261), a sophisticated consumer has a high level of understanding and awareness of the trade-offs regarding data sharing on online platforms. They are able to recognize the impact of both long and short-term data sharing, have the ability to signal preferences and understand the privacy policies. Baye and Sappington (2019, p.264–6) claim that sophisticated consumers benefit when data is shared, whereas unsophisticated consumers benefit when data is not shared; this is because the unsophisticated consumer does not expect their interaction with one merchant to have any effect with another merchant. Having an optimal policy for only one group of consumers, whether sophisticated or not, may harm the other group. For example, through their model, Baye and Sappington (2019, p.266–9) show that identity removal from data can have a huge impact on sophisticated consumers as it closes their usage of signalling, whereas it benefits the unsophisticated consumer.

The delicate balance between securing personal information and fostering innovation strongly influences societal economic welfare. As noted by Baye and Sappington (2019, p.260-72), the effectiveness of privacy measures relies on various factors, including consumer sophistication. While categorizing consumers as either sophisticated or not may seem overly simplistic, it serves to emphasise the complexity of the issue, showing that a uniform approach to privacy regulation is unsatisfactory. Instead, a regulation needs to be able to foster innovation while balancing the supply of personal data so that only relevant and specific data is collected and processed to help market efficiency.

3.2 Transactions in the Market for Personal Data

Transactions that occur in the market for personal data cannot be discussed without understanding the critical role that information asymmetry and externalities play. In this sub-chapter the paper will break down how information asymmetry can significantly affect transaction outcomes and suggest how transparency can mediate such a threat before discussing the positive and negative externalities that occur from these transactions. Leading to the conclusion that when both information asymmetry and certain externalities are accounted for it could foster trust and the protection of individuals privacy.

3.2.1 Information Asymmetry

Information asymmetry is when one party in a transaction possesses information that the other party lacks access to. At a fundamental level, both consumers and merchants leverage this information strategically to influence the prices of goods and services. For instance, consider a scenario where a consumer purchases a used car from its previous owner. The seller, holding information about any undisclosed maintenance or issues with the vehicle, may choose to withhold this information to maintain a higher selling price. On the other hand, the buyer, armed with knowledge about the car model's market value or potential resale opportunities, may negotiate a lower purchase price to maximize their profit upon resale. Where problems come into play with information asymmetry are adverse selection and moral hazards. In particular, hidden information and hidden action. The previous example discusses hidden information that could lead to adverse selection where the buyer is uncertain about the validity of the claims the seller makes. In comparison, a hidden action is the behaviour of either party after the transaction has occurred, such as the buyer selling the car onwards for a higher price. If we lived in a perfect world where everyone told the truth and trust was always given, then these problems would most likely not occur; however, full truth is not something that can be implemented outside of a thought experiment, so the next best thing is transparency. Having a regulation on the market that promotes transparency would build trust

among market participants and could reduce information asymmetry, allowing for more efficient transaction in the market.

The transaction type that occurs online may not always feel like a typical merchant-to-consumer, in the same way that buying and selling a car does. Typical everyday transactions that occur online look something along the lines of an individual googling gift ideas for a significant other. The individual may find the perfect gift through this transaction, and on the other hand, the data collected, such as gift preferences, sexual orientation or even if the individual is single or not, then get sold to third parties, or used internally with the firm's own marketing department, which use that information to help target the individual the next time they google something. The asymmetric aspect is that the individual most likely has no idea what data is being collected, nor do they know where said data will end up. On top of this, they are also unaware that the deals on the perfect gift they found could have been altered from their previous searches online, thus providing them with higher-priced goods. According to Pelchen (2024, p.1), that is just one transaction that occurred within a few minutes when, in reality, the average internet user spends just over six and a half hours online daily, leaving trails of information on their preferences. According to Pelchen (2024, p.1), the average (in the best case all) consumer should become better informed about how data is collected, the reasons for its collection, and the potential outcomes of sharing personal information online.

If there was a regulation that banned the collection and processing of personal data so that the above transaction where the person looking for a gift ends up paying a higher price (unique to them based off of their previous data collected) then this would not occur because the firm would not have the relevant data to make this calculated spike in price. However, this is not an efficient way of resource allocation for either party involved even if the individual ends up with the same product for cheaper. For the efficiency of the personal data markets firms require information about consumers as a way to help guide them. Naturally not all information is needed at all times and for a more efficient model of online data transaction it would be optimal if the relevant information only went to the relevant places where that data could be used to the benefit of the individual and to the market. In a broader economic context, accurate information (which can be derived from relevant information processed by

the relevant counterparts) contributes to efficient market operations by ensuring that consumers and firms make well-informed decisions. For instance, if we take the example from earlier with the individual finding the perfect gift, we can see how the optimization of relevant information could help guide the individual's search. If due to previous online behaviour by the individual that every year at the same time they search for gift ideas and mainly focus on jewellery brands then it would be more efficient for them to get targeted ads during this time that provided them with jewellery gift ideas, rather than say an ad for a new car.

The information based on previous online behaviour is the outcome of data collection and processing. Almost everyone who uses the internet has a similar stack of data stored about their online activities. The pop-up notification for data collection that appears on the screen when you enter a website with usually two or three options is how this information is allowed to be collected. One option on the pop-up is usually to accept all and the other to reject. By clicking accept all or even accept essential cookies, you agree to the collection and use of your personal data whilst on the webpage, essentially giving away your data to browse the site. However, consumers' limited awareness of the extent of data collection hinders their ability to make informed decisions about their privacy. This lack of awareness suggests that consumers may not accurately evaluate the trade-offs between privacy and convenience. This highlights the importance of enhancing consumer education and awareness in navigating privacy-related choices. A simple way to enhance consumer education is to rephrase highly complicated wording in the privacy policies so that the consumers become aware of what data is being collected and why it is being collected.

3.2.2 Externality

The standard definition of an *externality* provided by Hashimzade et al. (2017) is an unintended consequence of an activity that affects a third party not involved in the transaction. Externalities can have positive effects, such as an individual quitting smoking for the benefit of improved health, which could also benefit those around them by decreasing their exposure to second hand smoke. Externalities can also have negative effects, such as

playing loud music at night, which could have the unintended consequence of keeping your neighbours from getting a good night's sleep. Externalities, both positive and negative, occur with the trading of information for services online. Personal information about one individual can be informative about another individual, according to Goldfarb and Que (2023, p.267-8). The accumulation of mass information on individuals leads to connections that can be informative to firms looking for consumer information. For example, a positive externality that comes from the mass collection of information by an online retailer allows for the consumer to be shown products that are similar to what they are looking at currently and to be provided with other products that previous consumers have purchased along with the product they are looking at. This can help the consumer find what they want more easily and make them want to use the same retailer again when they are looking for a different product, a win-win positive externality situation for both the consumer and the merchant. According to Goldfarb and Que (2023, p.276), A negative externality of mass information collection could be an individual's willingness to pay being influenced by a data spillover effect from like-minded individuals. For example, consider a person who frequently shares and posts multiple photos and life updates on a social media platform, tagging friends and geotagging their locations daily. Now, imagine that one of their friends, who rarely posts anything personal, is tagged in these posts. This second individual experiences a loss of privacy without their consent due to their friend's oversharing.

Externalities can also affect asymmetric information. Assume two groups of people, one (A) who gives all available information about themselves away and the other (B) who does not give any information away. Members of group A have friends and family in group B and vice versa, and the two groups are connected socially. Because the two groups are connected, some people share similar interests, live in the same location and share other key identifying data points. Even though Group B never disclosed any information, their information will become known over time due to unravelling logic. Therefore, the collection of only some data, over time, will turn into the collection of all data. The more data collected about members from Group A, the more information will be revealed about members of Group B. Furthermore, members of Group A give away their information and benefit from it through the transactions they do online, and members of Group B do not receive the benefit yet still incur the cost due to the revealing of information by another person.

Considering externalities is crucial in privacy-related decision-making. When individuals and organizations do not take into account the broader impact of their privacy choices, it can lead to suboptimal outcomes in the market. For example, suppose individuals solely focus on their own privacy preferences without considering the positive externalities that may arise from sharing certain data. In that case, it may result in a lack of data availability for beneficial purposes such as traffic, public health, or general research. On the other hand, if individuals are unaware of the negative externalities associated with certain privacy practices or data-sharing arrangements, it may lead to businesses' excessive exploitation of personal information. In such cases, the market may fail to provide the right level of privacy protection or may oversupply privacy harming products or services.

3.3 The Role of Regulation

In digital privacy, reliance on market mechanisms often falls short of addressing key concerns, such as consent, control, and transparency. While some could argue that the market could efficiently respond to evolving consumer preferences in the absence of privacy regulations, this overlooks the inherent limitations of markets. Market failures, such as information asymmetry and social inequality, can hinder the efficient allocation of resources. There has been advances in security of personal data online through premium software that allow for individuals to surf the web without being traced or data being collected, however these come at a price which excludes many other individuals. Moreover, some individuals may lack sufficient information to make informed privacy choices, leading to exploitation and identity theft.

Therefore, regulation must address these market failures and ensure that individuals have control over their information regardless of willingness to pay and knowledge. An effective regulation should be able to strike a balance between empowering individuals and fostering information circulation. Without such regulation, privacy becomes a privilege accessible only to those with financial means, leaving the majority vulnerable to harm.

Regulation must satisfy economic incentives for businesses in the digital world in order to be implemented. For example, international compatibility, which due to the global nature of digitalisation, regulations should help facilitate cross-border data flows and trade. Moreover, there should not only be incentives to uphold the regulation for businesses and organizations but also consequences for non-compliance, such as fines. It is important that a sense of accountability is upheld by firms to foster trust accuracy and stability in the market. The regulation should ensure transparency in order to maintain consumer trust. Individuals who are aware of their privacy rights, along with those who are unaware or unbothered to inform themselves should at the very least have as a default, a basic level of privacy.

Nonetheless, the most important thing for a regulation to have in the digital world is the ability to adapt to the ever-changing landscape of new advancements in technology. The regulation does not need to include every conceivable way in which technology could change the way people interact and transact online; however, it should be broad enough to allow for the protection of both individuals and businesses once an advancement in technology happens. A good regulation safeguards the interests of the majority while also fostering robust economic development. It ensures that even the most disadvantaged individuals are shielded to the degree that maintains their willingness and ability to engage in the digital world. Having said that there is a cost to a regulation. The cost is not on the individual but rather on the firm that would need to have enough capital to invest in whatever changes need to be met to meet the guidelines of a regulation. A regulation for digital privacy should include control given to individuals regarding their own information (data) at any given time and should still be beneficial for the economy. For example, an individual may consent to information being used to help them navigate online; however, they should also be able to reclaim that information by disassociating their digital self from that data point. At the same time, once the data collection has been consented to, the data should be allowed to be used to the fullest extent, and if the individual decides that they no longer want the data to be associated with them, it should still be allowed to be used for economic benefit.

3.4 Closing Chapter Remarks

The economics of privacy is about finding the balance between empowering individuals and fostering information circulation leading to market efficiency. Overly restrictive regulations could impede on the collection of valuable data which could have negative effects on the market. However, regulations should restrict the collection of unnecessary data so that there is not a build-up of data creating confusion and inefficiency. Regulations must also have strong data security mandates to reduce the risk of data breaches, which is important for building and maintaining trust. For a regulation to be able to satisfy this balance there needs to be a set of limitations to what data is being collected, how much data is being collected and for what reason the data is being collected and then processed. Therefore, making the collection of data as transparent as possible. If a regulation is able to do this then I believe privacy in terms of individuals control over personal data can be implemented without impeding too much in the market.

4 The General Data Protection Regulation

This chapter will begin with a short introduction and brief history of the General Data Protection Regulation (GDPR) before breaking down how the GDPR prioritises consent. Explaining how consent implemented through design by default can create greater control and therefore autonomy for the individual. Then it will explain the core principles of the GDPR and how they relate to market efficiency. The chapter will continue with the rights of the consumers within the GDPR and how they are exercised through consent before discussing the role that the collectors and processors have within the GDPR guidelines.

4.1 Brief History of the Digital Privacy Regulations

The General Data Protection Regulation (GDPR) was established in 2016 and implemented two years later on May 25th, 2018. Since then, it has become a framework of fundamental principles with influence reaching far outside the European Union due to its strict enforcement and thorough scope. Before the GDPR, several other regulations, both within and outside the EU, were implemented for personal data protection. The GDPR emerged due

to existing data protection shortcomings, the complexity of the digital world and the growth of technological developments within the last thirty years.

In 1995, the Data Protection Directive (DPD) (Vander Maelen, 2020, p.232-5) created the foundations for digital data protection; however, more was needed. The DPD could not keep up with the dynamic environment, and gaps within the directive were exploited. In more recent years and with the surge in data breaches and privacy violations, such as Facebook-Cambridge Analytical, individuals were made aware of the scope in which data collection can be abused. Individuals started to become more aware of the connections that can be made based off of their data and how that can be exploited by marketing for commerce and politics alike. The reason that the GDPR can adapt than its predecessors thus far is due to its core principles and emphasis on consent. The GDPR is a tool that must be used now in order to protect not only the individuals of today but also those of tomorrow. The development of technology is rapid, and the GDPR must stay up to date on the ins and outs of such development to maintain that at the core of the regulation is the protection of individual privacy, such that data protection and consent stay in the foreground of refinement.

The GDPR has significantly transformed data protection with its strict requirements for collecting, processing and storing data. According to Schade (2023, p.478), the GDPR has strengthened the fundamental rights to privacy and data protection of the individual whilst simultaneously creating clear guidelines for businesses and other organizations in the digital age. Along with the strengthened individual rights, Schade (2023, p.478-80) claims that transparency and accountability from both the data subject and the data collector have been enhanced. This is brought upon by the implementation of impact assessments and data protection officers along with the following through of major monetary fines.

The impact of the GDPR extends outside the European economic zone and has a major influence on other countries' data protection laws. For example, (Usercentrics, June 2024) Brazil's *Lei Geral de Proteção de Dados* (LGPD) focuses heavily on consent, transparency and data subjects' rights, similar to the GDPR. Along with that, it has impact assessments and data protection officers integrated into the law. South Korea's *Personal Information Protection Act* (PIPA) was amended to align with the GDPR principles, such as stricter

consent requirements and higher penalties for violation, and to facilitate smoother data transfers between South Korea and the EU (Foitzick, 2022). As the digital world is inherently global, comprehensive data protection frameworks must be promoted to elevate the international standard of data protection.

Multinational corporations are also moving towards adopting GDPR-compliant practices globally to ensure a more seamless data collection throughout all their jurisdictions. However, this is not the case for all large corporations; in fact, some are purposely not fully adopting in all their geographical locations. For example, Facebook (now Meta) abides by the GDPR within their EU-based customers, but for all customers outside of the EU protection, they do not have the same protection granted. (Laybats and Davies 2018, p.82) This is because Meta's finance relies on their users' data (Meta Platforms Inc., 2023, p.60-9). Meta profits from the collection and processing of their user's data across multiple platforms globally, the reasoning could be made from a profit-based analysis in which choosing to not fully adapt to the guidelines of the GDPR in areas where they are not required too yet could be generating more profit for them. However, the time will come when they must fully adapt. With that adaption will come new innovations which could help boost profit under the strict guidelines of the GDPR.

4.2 Consent Through Design by Default

A key difference between the GDPR and previous regulations is the prerequisite of consent. Through promoting and enforcing active consent on all EU websites the GDPR has increased the empowerment of individuals autonomy over their own data. In particular, there is the emphasis of informed decision-making through opt-in consent. Opt-in refers to the consumer actively clicking consent to data collection when entering a new website (Laybats and Davies, 2018, p.81). In the past, the default option was opt-out, meaning the individual automatically consents to everything unless they actively state otherwise. Such a small act greatly changed how data collectors can obtain individual data. For example, the small pop-up that presents itself when you enter a webpage normally has three options: to accept all, to reject all (unessential) or to customize your preferences for data collection, processing and storage. Before the regulation, a default setting was that by entering the website, the consumer was consenting and would need to opt-out if they did not want their data to be

collected, processed or stored. This was causing individuals who either did not care or were uninformed to be disadvantaged as a default. The disadvantage in the sense that their data was not being protected by default and their right to privacy was not being protected. Whereas now, if the same individual does not care or is uninformed, at least the default is that their privacy is being protected. Therefore, the individual has the control and power over their personal data yet does not have the burden of needing to protect their information online by themselves. Moreover, the individual has more control on what type of data is stored, who it is allowed to be shared with, and they have the choice to control their data differently on each website they visit. Leading to a key point of consent that a consent to one action and given to one person does not mean consent to all actions done by all. Therefore, each websites makes you give explicit consenting agreements to what data they are allowed to collect, process and store. This too can be tedious when you must always first accept, reject or manage your data collection settings before entering into a website however, the alternatives as of yet are not adequate enough.

4.3 Encouraging Trust and Accuracy

Trust and accuracy are central topics in Economics, and in particular, transactions. In the market for personal data, data subjects need to trust that the data collectors remain true to the contractual agreement, and they need to trust that if the data collector does not uphold the contract, then consequences will be brought upon them. Naturally, one could conclude that the individual only needs to trust in the regulation that overlooks the transaction and ensures their data is safe rather than trusting that the collector does it correctly. Meaning that only the information they agreed to be collected is collected and only those how have their permission to access their data have access to it. Trust in this case is protected by the GDPR making sure that all agents are compliant through substantial fines and restrictions made such as data limitation. Accuracy refers directly to the information and is crucial to the firms and how they understand the individuals' preferences. For example, if the information that is collected is not true or if there is an overload of information that it is hard to extract exactly what is needed then it makes it hard for firms to use this to their advantage in painting a picture of what the individual wants.

The GDPR has core principles that encourage trust and accuracy to flourish. This sub-chapter will begin with briefly defining each principle and then discuss its relation to market efficiency.

4.3.1 Core Principles

The GDPR has many principles and guidelines to help ensure the protection of personal data without completely banning the profitability of data markets. There exist different names for some of the seven core principles extracted out of the official GDPR text the ones provided in this text are based on several data protection firms. Purpose Limitation, Fairness, Lawfulness and Transparency, Data Minimization, Storage Limitation, Accuracy, Confidentiality and Integrity, and Accountability (European Parliament and Council of the European Union, 2016, UHI 2024 and, OneTrust 2021)

Purpose Limitation: Data being collected should only be for specified, explicit, and legitimate purposes. This means it should not and cannot be processed in a way that was not originally stated when the individual gave consent. *Fairness, lawfulness, and Transparency*: Data collecting, processing, and storing must be lawful, fair, and transparent to the data subject. *Data Minimization*: Personal data should be relevant and limited to what is necessary in relation to the purpose it was processed for. This principle ensures that only the minimum amount of data required is used. *Storage Limitation*: Data cannot be stored for longer than necessary for the purpose for which the individual originally consented. *Accuracy:* Both parties should keep personal data accurate and up to date. *Confidentiality and Integrity*: The collecting, processing, and storage of personal data should ensure protection against theft, loss, or destruction. *Accountability*: The data controller is responsible for upholding the principles of the GDPR.

4.3.2 Application to Market efficiency

The seven core principles can be divided into two groups, trust and accuracy based on their effect on market efficiency.

Trust, for example, includes *purpose limitation*, *fairness*, *lawfulness*, *transparency*, *confidentiality*, and *integrity*, all of which boost trust between all market participants. Limiting the data collected by its purpose increases trust and predictability and could lead to a more efficient allocation of resources. Remaining lawful, fair, and transparent also builds trust among market participants and can reduce information asymmetry, allowing for more efficient data trading. Moreover, securing data collection could help build trust and reduce the risk of data breaches, which, when left unsecured, could disrupt market operations and lead to inefficiencies. *Accountability*, a key factor in market stability, is directly linked to data collectors, processors, and storers. The goal of the GDPR is the protection of individuals rights to their personal data. However, if that was its only goal then it could be more efficient to ban all data collection and processing which would most likely shut down the official market for personal data in the digital world. For the market to continue to function in a way that satisfies privacy protection, regulations need to be put in place and participants such as firms using the data must adhere to the guidelines provided to them, to ensure compliance. This, in turn, fosters trust, accuracy, and stability in the market. Trust is crucial for market efficiency in particular in the market for personal data. If the consumer does not trust that their data is not being protected or that they do not have enough control to only give the data that they are willing to give then they will most likely stop using whatever website, platform or business that is operating in this way. On the other hand, it could be that the individual does not know of an alternative and in that case may continue to be a consumer even though they do not trust that their data is being protected.

Accuracy is important for market efficiency because it ensures that the data available to market participants correctly reflects the reality of the assets and transactions. On the one hand, accuracy refers to correct and current information given to market participants so they can make decisions based on it and on the other hand, accuracy can also refer to how *data minimization* and *storage limitations* help reduce the buildup of information by only accepting what is necessary for the transaction could potentially help maintain the relevance and accuracy of information which in turn could promote efficiency.

4.4 Rights of Data Subjects Under the GDPR

Within the GDPR, several branches of sub-rights are associated with the right to privacy and autonomy. As previously discussed in the chapter on philosophical perspectives and ethical implications of privacy, privacy is a right that can sometimes be associated with other rights such as property right, allowing for a legal basis of protection. Within privacy there are multiple sub-rights that fall under privacy, for example, the right to be forgotten claims that individuals have the right to have their personal identity removed from data that may have already been given therefore dissociating the individual from the data as a way of control over their data. The rights provided to the individual consumer (data subject) is to empower them to claim control over their data and allow them an easy way to exercise their right. Repeating Solove's (2002, p.1112) point from earlier that control can be understood as ownership. Therefore, the sub-rights are granted to the individual through the GDPR to empower them to claim ownership of their data. Found in the regulation's official text (European Parliament and Council of the European Union., 2016, L 119/41), there are five key sub-rights protected and enhanced by the GDPR; they are as follows: the right to access, rectification, erasure, data portability, and to object. To elaborate further, the right to access allows the individual to request access to the data associated with them, thus ensuring a sense of transparency. The right to rectification allows for the individual to be able to correct any misinformation collected about them. The right to erasure, or as it is sometimes referred to as, the right to be forgotten, allows, under certain conditions, data to be completely deleted. Therefore, giving the individual, the ability to withdraw their consent to the processing of already collected data by requesting that the collector deletes it. In some cases, it is not deleted but rather no longer associated with the individual in question. Fourth is the right to data portability which allows for already collected data by one collector to be transferred to another where possible. Lastly, the right to object, which allows the individual to object to certain data collection, in particular that which would be used for marketing purposes. This allows the individual to have control and consent to process activities that align with their preferences and values. As already mentioned, all of these sub-rights fall under the right to privacy in so far as they are directly relating to control over data.

The rights of the data subjects within the GDPR are exercised through consent and protected as individuals' privacy. Consent enables the individual to have full power over data collection, processing, and storage. Permission given actively, to those they choose, and being able to be taken back once granted, is a definition of consent. This is what makes the

GDPR stand out from its predecessors and what will allow it to last with the changing and advancement of technology. As technology develops and new more efficient ways to process and collect data are practiced should have no negative impact on individuals control over their data so long as consent is still required. With the GDPR in place future data controllers are encouraged to be more transparent and accountable which fosters a secure data processing environment.

4.5 The role of the Data Controllers/Processors

An integral aspect of the GDPR is that it leads to data protection by design and by default. Therefore, data collectors and processors have to integrate data protection principles within their systems to ensure that the privacy of the individual is considered and protected at every step of collection, processing and storage. It is crucial that records are documented at all stages of collecting, processing, and storing data, which is why the GDPR (European Parliament and Council of the European Union, 2016, L 119/16) sets the obligation to make detailed accounts of such to show compliance with the GDPR rules and support accountability to the individual. Data collectors are required to run data protection impact assessments, which help to mitigate risks associated with processing data. Along with impact assessments, collectors need to appoint data protection officers within their organization that ensure compliance with the GDPR and act as a key bridge between data subjects (individuals) and the authorities. If a data breach occurs, the collector is given 72 hours, once aware, to inform the relevant authority and in certain cases, to issue a statement to the affected data subjects (European Parliament and Council of the European Union, 2016, L 119/17). A short window ensures a timely response to minimize further potential harm.

The enforcement of these obligations are imposed through penalties for violation. The penalties could be monetary fines of €10 Million to €20 Million or 2% to 4% of the total annual worldwide turnover of the preceding financial year, whichever is higher, depending on the violations committed (European Parliament and Council of the European Union, 2016, L 119/82-83). However, it is up to each member state and its supervisory authorities to determine the different penalties for minor and major violations; jurisprudence naturally plays a role in the final decisions made within the European Union. On top of fines, potential

consequences include reputational damage, where the trust of the customers is lost; along with this, legal action backed by customers could also damage the organization's finances and reputation. Under the GDPR (European Parliament and Council of the European Union, 2016, L 119/69-70) supervisory authorities have three main powers in which they exercise to maintain compliance in their jurisdiction:

1. Investigative powers: If the authorities suspect non-compliance with the regulation, they can require the organization or data collectors and processors to provide necessary proof of compliance and information.
2. Corrective powers: This allows them to issue warnings and impose limitations on processing until the activities are in compliance.
3. Advisory powers: These are where they can provide guidance on the GDPR and provide best practices for compliance.

Understanding common compliance issues is key to avoiding them. Data mapping, consent management, and cross-border data transfers are areas where many organizations struggle to comply with the GDPR. For instance, in 2019, Google was fined €50 million by the French data protection authority (European Data Protection Board, January 2019) CNIL for not complying with consent requirements. The reason was that they did not provide users with clear and specific information about their data and how it would be used, claiming it was too broad. Another example is the Austrian data protection authority fining the Österreichische Post AG €18 million for violating the GDPR by selling personal data on individuals' political preferences for advertising purpose without consent (European Data Protection Board, October 2019). These real-world examples highlight the importance of understanding and adhering to the GDPR regulations in order to avoid such reputational and financially damaging situations.

4.6 Relationship Between Privacy and Market Efficiency

This paper has mentioned a trade-off between privacy and market efficiency whereby the GDPR for example, may impose limits on personal data usage of businesses thus potentially reducing market efficiency. A trade-off argument suggests that the stricter the privacy protection regulation the less efficient the market is, this might be due to a reduce in available

data, increase in compliance costs or slowing down of innovation. However, there is also a harmony argument to be made between privacy and market efficiency. For example, that privacy protection can enhance market efficiency by fostering trust and improving accuracy of data. The GDPR is able to balance these two arguments as its goal is to protect individual privacy rights while also enhancing the foundations for a stable market. For example, through data minimization and consent requirements the GDPR is able to provide the market accurate personal data of individual to be used for specific purposes that they have agreed to.

One potential measure that the GDPR could implement to promote further market efficiency is a standardized data-sharing framework. Introducing a standardized framework for companies to share data in a controlled and privacy-protecting manner could boost innovation and reduce the saturation of data collection. Secure and compliant data sharing between companies could enhance innovation through collaborating on data-driven projects. Furthermore, and in line with the GDPR's core principle of limiting unnecessary data collection, a data-sharing framework could help reduce data duplication. Without this framework within the GDPR, the potential for market growth and innovation is limited. Companies may be reluctant to join a data-sharing system without the GDPR guidelines, fearing non-compliance with current rules. The GDPR could introduce a certification system for data-sharing practices, acknowledging compliant frameworks and promoting privacy while encouraging collaboration.

4.7 Closing Chapter Remarks

In conclusion, the GDPR has set and maintained a high global standard for data protection. It has increased awareness, enhanced data security and made progress in regulatory enforcement within the EU. Establishing consent at the foreground of the GDPR guideline has increased individuals' autonomy and their ability to control their personal data and therefore achieve privacy. Having an opt-in default has transformed the regulation from a mediocre protector of privacy to a well-established one. It has not only promoted autonomy through consent for the individual but moreover has accounted for those who do not care or are not well educated in the field of data privacy to know what is happening with their data in the digital world. This way at least they are protected by default and have control over their

data if they choose to act upon it. Through the core principles of the GDPR broken down into trust and accuracy we can see how the regulation is able to improve market efficiency.

Challenges do remain, however, and as technology evolves, so must the GDPR. There are some future developments in technology that could undermine the GDPR. For example, artificial intelligence and machine learning are rapidly growing, requiring large amounts of data to function. This system could also process data in ways that may not have been agreed to when consent was given, therefore undermining the regulation. A way that the GDPR could combat this is by providing specific guidelines for how technologies like AI should comply and imposing fines on companies that violate the GDPR principles. Emerging technologies may be built with the GDPR in mind, but this may not always be the case, and as such, the current regulations may not fully address these gaps. Therefore, potential amendments and updates will likely be necessary in order to maintain transparency, consent, and consumer rights. What is crucial is that the burden of compliance should not be on the individual but rather on the data collector, processor and storer. This means that we should not move back into an opt-out setting for data protection but remain in an opt-in environment whereby the default is to protect the individual.

Amendments to regulations are a time-consuming process, and given the pace of technological innovation, the GDPR, like many regulations, appears to lag behind. However, this is not a sign of failure but a reflection of a typical cat-and-mouse chase. The GDPR needs to ensure that it does not lag too far behind, or else it may result in greater harm than good to society.

5 Conclusion

This paper has explored the extent to which the General Data Protection Regulation (GDPR) upholds the fundamentals of individuals' privacy protection while balancing the need for market efficiency. The GDPR effectively upholds the fundamentals for individuals' privacy protection while balancing the need for market efficiency by requiring that individuals have control of their own data through consent, which enhances individuals' autonomy without the need for overly restrictive measures to be placed on the firms.

Privacy, from a philosophical point of view, has both a normative and operational perspective, in the sense that privacy is a right, and it is also a way for individuals to control their own information. Therefore, the job of a good regulation, such as the GDPR needs to be able to protect these two characterisations of privacy. The fundamentals of privacy protection are consent, compliance and transparency. When individuals have the ability to consent, then they have control over their data by default, and with the strong enforcement mechanisms of the GDPR, compliance on the firm's end (collectors, processors and storers) is ensured. When this is done in a transparent way by both parties, then both parties will be able to benefit from the transactions while still maintaining the fundamentals of privacy protection.

The GDPR has set a high standard for data protection with its consent-based regulation and increased security and regulatory enforcement. The GDPR has removed the burden of compliance from the individual and placed it on the firm (collectors, processors and storers) through the introduction of opt-in as a default, which accounts for those less informed individuals. The core principles, led by two key themes of trust and accuracy, are central to improving market efficiency. However, the GDPR also has a significant compliance cost that firms, in particular smaller ones that do not have the capital to adapt to the regulations at hand, may suffer from. Moreover, when businesses face increased operational costs, they sometimes tend to pass these costs onto consumers in the form of higher prices.

Finding the balance between individual empowerment and market efficiency is a challenging task; however, the GDPR has been able to make great leaps in the right direction with the introduction of consent. With overly restrictive regulations both the individual and the firm will not benefit due to the hindering of valuable data collection. Therefore, the market will not be acting efficiently. The balance then is restricting unnecessary data collection, limiting the collection of data that may cause confusion or inefficiency later own down the chain. For example, only collecting the information that will be needed and giving it to those processors who can use that information efficiently. Thus, having a threshold for the collection of data based on necessity, amount, and purpose can strike a balance between overly restrictive and non-restrictive. The market efficiency for data collection is heavily affected by theft, breaches and loss of data, and therefore, it is important that strong security measures are in place to solidify trust and create stability within the market.

A multidisciplinary approach is highly suitable for developing robust solutions to serious problems. Therefore, the GDPR and privacy issues in the digital world must be assessed from

a philosophical and economic perspective rather than only one of the two separately. The combination of these two perspectives not only defends privacy as an ethical necessity but also critically examines the practical limitations of protection within the market, making us aware of the challenges we face. By only assessing the GDPR from an economic perspective, it may be easier to move away from the ethical implications that arise as long as welfare and the market are stable. Vice versa, ignoring the effect of regulation on the market may have a larger effect on the support and implementation of the GDPR.

In conclusion, the GDPR successfully upholds individuals' privacy protection fundamentals while attempting to balance the need for market efficiency. The regulation gives individuals greater control over their personal data through consent, enhances data security through compliance regulation, and fosters trust in the digital economy between all market participants. These key points are essential for maintaining individuals' privacy by ensuring personal data is handled responsibly. The GDPR's guidelines displays a strong commitment to protecting individual privacy rights, but its economic implications require careful oversight to maintain a balanced and efficient market for personal data. As the digital world continues to grow and develop, so must the GDPR, ensuring that privacy and market efficiency are upheld together.

6 References

Acquisti, Alessandro and Taylor, Curtis and Wagman, Liad. “The Economics of Privacy”. *Journal of Economic Literature* (2016): 442-492. http://dx.doi.org/10.1257/jel.52.2.442

Baye, Michael and Sappington, David. "Revealing Transactions Data to Third Parties: Implications of Privacy Regimes for Welfare in Online Markets". *Journal of Economics & Management Strategy,* (2019) https://doi.org/10.1111/jems.12337

Benn, Stanley. “Chapter 14 – The Principle of Privacy.” *A Theory of Freedom*, Cambridge University Press (1988): 264-280. http://dx.doi.org/10.1017/CBO9780511609114.016

Burkhardt, Gary and Boy, Frederic and Doneddu, Daniele and Haji, Nick. “Privacy Behaviour: A Model for Online Informed Consent”. *Journal of Business Ethics*, (2022): 237-255. https://doi.org/10.1007/s10551-022-05202-1.

Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. “We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR’s Impact on Web Privacy.” *Informatik-Spektrum* 42, no. 5 (2019): 345–46. https://doi.org/10.1007/s00287-019-01201-1.

European Data Protection Board. "Administrative Criminal Proceedings of the Austrian Data Protection Authority Against Österreichische Post AG (Austrian Postal Service)." October 23, (2019): https://www.edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority_en

European Data Protection Board. "The CNIL’s Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against Google LLC." January 21, (2019): https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en

European Parliament and Council of the European Union. *Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).* OJ L 119, May 4, (2016), 1–88. ELI: http://data.europa.eu/eli/reg/2016/679/oj.

Foitzick, Klaus. “South Korea’s Personal Information Protection Act (PIPA).” *Activemind.legal*, 12 July (2022): https://www.activemind.legal/guides/pipa-south-korea/

Goldfarb, A. and Que, V.F. "The Economics of Digital Privacy". *Annual review of economics,* (2023): 267–286. https://doi.org/10.1146/annurev-economics-082322-014346.

Hashimzade, Nigar and Myles, Gareth and Black, John. *A Dictionary of Economics (5 ed.)* (2017):https://www.oxfordreference.com/view/10.1093/acref/9780198759430.001.0001/acref-9780198759430.

Laybats, Claire, and John Davies. “GDPR: Implementing the Regulations.” *Business Information Review* 35, no. 2 (2018): 81–83. https://doi.org/10.1177/0266382118777808.

Locke, John. *Second Treatise of Government*, The Floating Press, 2016. https://uaccess.univie.ac.at/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1403597&site=ehost-live

Meta Platforms, Inc. *Annual Report on Form 10-K for the Fiscal Year Ended December 31, 2023.* Washington, D.C.: U.S. Securities and Exchange Commission, (2024): https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/8395af04-55bd-45cd-a201-fa0d2d3d57ec.html

Obar, Jonathan A., and Anne Oeldorf-Hirsch. "Older Adults and ‘the Biggest Lie on the Internet’: From Ignoring Social Media Policies to the Privacy Paradox." *International journal of communication* [Online] 16 (2022): 4779-4800. *Gale Literature Resource Center*. https://link-gale-com.uaccess.univie.ac.at/apps/doc/A726954054/LitRC?u=43wien&sid=summon&xid=7eaaa52b.

OneTrust. "Understanding the 7 Principles of the GDPR." Last modified May 17, (2021): https://www.onetrust.com/blog/understanding-the-7-principles-of-the-gdpr.

Pelchen, Lexie. "Internet Usage Statistics In 2024." Reviewed by Samantha Allen. *Forbes*, March 1, (2024). https://www.forbes.com/home-improvement/internet/internet-statistics/.

Schade, Frederik. “Dark Sides of Data Transparency: Organized Immaturity After GDPR?” *Business Ethics Quarterly* 33, no. 3 (2023): 473–501. https://doi.org/10.1017/beq.2022.30.

Solove, Daniel J. "Conceptualizing Privacy." *California Law Review* 90, no. 4 (July 2002): 1087-1155. https://www.jstor.org/stable/3481326.

Thomson, Judith Jarvis. “The Right to Privacy”, *Philosophy & Public Affairs,* Wiley (1975) https://www.jstor.org/stable/2265075

UHI - University of the Highlands and Islands. "The Seven Principles." (2024): https://www.uhi.ac.uk/en/governance/policies-and-regulations/data-protection/the-seven-principles.

Usercentrics. "Brazil’s General Data Protection Law / Lei Geral de Proteção de Dados (LGPD) – An Overview." *Usercentrics*, June 3, (2024): https://usercentrics.com/knowledge-hub/brazil-lgpd-general-data-protection-law-overview/

Vander Maelen, Carl. “Codes of (Mis)conduct? An Appraisal of Articles 40-41 GDPR in View of the 1995 Data Protection Directive and Its Shortcomings.” *European Data Protection Law Review (Internet)* 6, no. 2 (2020): 231–42. https://doi.org/10.21552/edpl/2020/2/9.

7 Appendix

Abstract (English):

In the age of digital connectivity and the persistent collection of personal data, where every click, swipe, and scroll leaves a trace, the issue of privacy has become a central topic of discussion. The General Data Protection Regulation (GDPR) is a significant step in safeguarding personal data and ensuring privacy protection within the European Union. This paper explores the ethical and market implications of the GDPR, evaluating its impact on data protection, individual rights, and organizational responsibilities. It argues that privacy is both a fundamental right and a tool for personal autonomy, emphasising the importance of control, consent, and transparency. The paper highlights the GDPR's challenge in balancing privacy protection with market efficiency, claiming that its core principles shift the burden of data protection responsibility from individuals to firms. While the GDPR upholds privacy fundamentals, it also imposes considerable compliance costs, which could influence market dynamics. Finally, the paper concludes that the GDPR effectively protects individuals' privacy while maintaining market efficiency, however this balancing act will require constant adjustments in the future.

Abstrakt (Deutsch):

Im Zeitalter der digitalen Vernetzung und der ständigen Erfassung personenbezogener Daten, bei der jeder Klick, jedes Wischen und jedes Scrollen eine Spur hinterlässt, ist die Frage des Datenschutzes zu einem zentralen Thema der Diskussion geworden. Die General Data Protection Regulation (GDPR) ist ein wichtiger Schritt zur Sicherung personenbezogener Daten und zur Gewährleistung des Schutzes der Privatsphäre in der Europäischen Union. In dieser Masterarbeit werden die ethischen und marktwirtschaftlichen Auswirkungen der GDPR untersucht und ihre Auswirkungen auf den Datenschutz, die Rechte des Einzelnen und die Verantwortung der Unternehmen bewertet. Es wird argumentiert, dass der Schutz der Privatsphäre sowohl ein Grundrecht als auch ein Instrument für die persönliche Autonomie ist, wobei die Bedeutung von Kontrolle, Zustimmung und Transparenz betont wird. Diese Masterarbeit hebt die Herausforderung der GDPR hervor, den Schutz der Privatsphäre mit der Markteffizienz in Einklang zu bringen, und argumentiert, dass ihre Kernprinzipien die Verantwortung für den Datenschutz von Einzelpersonen auf Unternehmen verlagern. Während die GDPR die Grundprinzipien des Datenschutzes aufrechterhält, verursacht sie auch erhebliche Kosten für die Einhaltung der Vorschriften, was die Marktdynamik beeinflussen könnte. Abschließend kommt diese Masterarbeit zu dem Schluss, dass die GDPR die Privatsphäre des Einzelnen wirksam schützt und gleichzeitig die Markteffizienz aufrechterhält, wobei dieser Balanceakt in Zukunft ständige Anpassungen erfordern wird.