The European Union's General Data Protection Regulation (GDPR): Implications on citizens' perception of safety, the enterprise and the technology sectors

By: Vivian Psylos

Word count: 6998

Prof. Karlyn Gorski

PBPL 22300: Policy Implementation

Winter 2024 Case Study

Introduction

On April 14th, 2016, the European Parliament and the Council of the European Union brought into law Resolution 2016/679, more commonly known as the General Data Protection Regulation (GDPR), which was put into effect on May 25th, 2018. This new piece of legislation defines mandatory rules about how companies and other organizations must use citizens' personal data. This includes both information such as the citizens' names, phone numbers, and addresses, as well as health information, interests, online habits, any and all information that could be used to identify a person. The GDPR also provides regulations about the principles according to which data collection can be made, the appropriate response to a data breach, and the amount that a company can be fined in case of breaching the GDPR. The GDPR provided what was the first comprehensive, widely-applicable framework on the appropriate use of users' private data, safeguarding the right to privacy of European citizens.

Considering the amounts of data collected by companies and other organizations over the Internet, the GDPR has had profound implications across a number of entities. As companies were forced to make their services compliant to the GDPR, the legislation resulted in significant amounts of implementation costs. Another particularly important aspect of the GDPR is its potential impact on technological development. While the end users can maintain their right to privacy, companies that would like to use personal data in fields such as artificial intelligence are now severely limited, thus hampering technological progress.

Furthermore, the GDPR has affected the lives of ordinary European citizens. The GDPR provides a comprehensive framework on how every organization they interact with must handle their private data. Yet, across different countries of the European Union, citizens show different levels of understanding what the GDPR actually entails, or they only partially understand what the legislation is about. Considering the breadth of regulations the GDPR brought forward, it can be assumed that discretion has been used by the members of the European Union in their implementation of the GDPR, leaving a lot to be desired.

In this paper, I will examine the history and background behind how the GDPR came to fruition. After analyzing the organizational actors involved in this legislation, I will focus my implementation analysis

on three main topics. Namely, the topics I will examine are the economic impact of the GDPR on enterprises, the impact of the GDPR on technological development and the technological sector in general, as well as the differences in the effective communication of the GDPR's aims among European citizens. Following this, I will provide policy implications on how to resolve the issues currently associated with this law, so that it can more effectively protect the rights of European Union citizens, allow technological development in the EU to prosper, and serve as an example for comprehensive data protection regulations around the world.

Historical Background

The General Data Protection Regulation was created as a result of two main factors. First, post-World War II Western Europe made significant effort into establishing and protecting the right of privacy for its citizens. Secondly, the continuous technological development, especially in the age of the Internet, resulted in the collection of ever-increasing amounts of data, challenging the right to privacy European governments sought to establish.

The right to privacy was enshrined in the European Convention of Human Rights (ECHR), which was first signed in 1950. However, up to 1995, there was no common European data protection law in place; every country was responsible for its own data protection legislation. However, the differences in data protection regulations significantly hampered the free flow of data within Europe, as data compliant with one country's regulations may not necessarily have complied with the regulations of another. Moreover, there was no overarching agency overseeing the enforcement of data protection regulations across European countries.

This changed on October 24th, 1995, as the European Community, the European Union's predecessor, adopted the Data Protection Directive (DPD) (Voigt and von dem Bussche 2017, p.2). This piece of legislation was the first common European effort to harmonize the protection of the right to privacy across the Community's member-states. Moreover, it also allowed the free flow of data across the member-states, as all member-states had to abide by the DPD.

Nevertheless, the DPD did not resolve all issues surrounding data protection. While it attempted to establish a common set of principles for data protection across the European Community's member states,

its power was limited. This is because “European directives are not directly applicable in all EU Member States but have to be transposed into national law” (Voigt and von dem Bussche 2017, p.2). As such, each country was still responsible to implement its own data protection legislation, allowing countries significant discretion in the process. In a way, the authorities of each member-state could be interpreted as street-level bureaucrats within the European Community’s (and subsequently, the European Union’s) framework. In this allegory, the EU could be seen as the manager who is “interested in achieving results consistent with agency objectives” (Lipsky 2010, pp.18-19), with the agency objectives being the DPD. On the other hand, each member-state had “considerable discretion in determining the nature, amount, and quality of benefits and sanctions” (Lipsky 2010, p.13) provided by the DPD. Thus, as Voigt and von dem Bussche (2017) describe, “Legal differences arose as a consequence of the implementing acts adopted by the various EU Member States. Data processing activities that were allowed in one EU Member State could be unlawful in another one with regard to the specific execution of data processing.” (p.2)

Moreover, the DPD was signed at a time when the Internet was at its infancy. The Internet itself had only existed for four years at the time, and digital storage was not yet as cost efficient as physical storage, thus limiting the amount of data that could be collected in the first place. A year later, however, digital storage became more affordable than physical storage, and in 1997, it was pointed out that the Internet was expanding 10-fold every year (World Economic Forum 2015). This paved the way for the unprecedented data collection ever since. At around 2005, the world entered the “Web 2.0” era, in which websites were integrated with vast databases (World Economic Forum 2015). While this allowed the formation of the Internet as we know it today, in which users are the primary generators of content through uploading it on popular websites, it also allowed for companies to more effectively process data for their own purposes, often against the will of the users themselves.

Inevitably, this increased collection of data raised concerns about the effectiveness of the DPD in protecting the data of European citizens. On June 22nd, the European Data Protection Supervisor published “A comprehensive approach on personal data protection in EU”, paving the way for negotiations over revamping the European data protection framework. (European Data Protection Supervisor 2018) These negotiations lasted for four years, until April 27th, 2016, when the European

Parliament and the Council of the European Union adopted the GDPR, to come into effect on May 25th, 2018. (European Data Protection Supervisor 2018)

Organizational Actors

The General Data Protection Regulation makes references to three principal organizational actors. As such, it can be safely assumed that the three are the main actors affected by the GDPR. Namely, these are the data subjects, the data controllers, and the data processors.

To begin with, the term "data subjects" refers to the people whose data are being collected. In particular, the official definition of a "data subject" under the GDPR refers to a person who is identifiable. In turn, a person is considered identifiable through their private data, which can consist of multiple pieces of information, ranging from the person's name and location to different aspects of a person's identity; as the GDPR text states, these can be "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Regulation 2016/679). Overall, the GDPR defines an extensive range of protected private data for the data subjects, who are the main beneficiaries of the GDPR.

The second term defined by the GDPR, "data controllers", refers to "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Resolution 2016/679). In other words, a data controller is the entity, most frequently in the form of an enterprise, which is responsible for the collection and processing of private data of individuals. Moreover, according to the Article 24 of the GDPR, "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" (Resolution 2016/679). Therefore, the GDPR considers the data controllers to be responsible over the nature of any data processing they perform.

Lastly, the third term defined, the "data processors", refers to any third party that may process data on behalf of the data controller (GDPR.eu 2018). These third parties can be particularly useful to companies that want to collect personal data on their clients, but ultimately lack the ability to devise their own means of processing their clients' data. Any company that performs data processing and analysis on behalf of

another entity can be considered to be a data processor. Examples of such firms include Google, Microsoft, and IBM.(knowledgehut.com 2022).

One notable aspect of the GDPR's definitions of data controllers and protectors is that the legislation does not exclusively apply to entities that are physically based in the European Union. Instead, the GDPR applies to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (European Commission 2023). This suggests that the GDPR has wide-reaching implications around the globe, as companies located outside of the EU, but offering services in the EU, must still abide by the GDPR, at least when interacting with European citizens.

Overall, my implementation analysis will consist of three components, namely its impact on individuals, enterprises, and the technological sector. These components demonstrate a loose association with these three main organizational actors that the GDPR defines. Specifically, European citizens are considered to be the data subjects, enterprises hold large amounts of data, making them data collectors, and specific companies in the tech sector are responsible for processing data of other companies, essentially turning them into the data processors. Nevertheless, this is not a perfect association; for instance, tech companies like Google and Microsoft can be both data controllers of the data they collect and processors for other controllers.

Aside from these, other organizational actors can also be considered. Perhaps the most significant one is the European Data Protection Board. This is an independent body that was established by the GDPR to ensure "ensure the consistent application of data protection rules throughout the European Union" (European Commission 2023). Its tasks consist of providing guidance on the GDPR, advising the European Commission on issues of data protection, and resolving any disputes that may arise on the topic between representatives of different member-states.

In turn, the European Data Protection Board is comprised of representatives of every EU member-state's national data protection agencies. In accordance to the Article 8 of the Charter of Fundamental Rights of the EU, every EU country must set up a national body responsible for the protection of its citizens' personal data (European Commission 2023). Therefore, each national data protection agency is

responsible for ensuring an accurate implementation of the GDPR within the borders of each member-state, and is also responsible for handing out fines to entities violating it. Nevertheless, those entities are not fully independent, as they all need to follow the GDPR, and they must ensure cooperation in enforcing the GDPR in cases concerning more than one member state (European Commission 2023).

Overall, the GDPR involves a great number of organizational actors, consisting of both individuals and enterprises, as well as any entity that owns and/or processes data of European citizens, regardless of the entity's physical location in the world. While the legislation places the interests of the citizens ahead of the enterprises' ones in theory, the implementation of the GDPR shows a number of issues, concerning every entity involved.

Implementation I: Implications on Individuals

As already mentioned, the GDPR has been enacted to ensure the protection of the data subjects' rights, i.e. the right of individuals to privacy. In order to achieve this, the GDPR has defined seven protection and accountability principles in Article 5, which intend to minimize the use of private data, while also establishing responsible methods of handling it. Namely, these principles are 'lawfulness, fairness, and transparency', 'purpose limitation', 'data minimization', 'accuracy', 'storage limitation', 'integrity and confidentiality', and 'accountability' (Resolution 2016/679). These principles demonstrate that, theoretically, the GDPR serves in the interest of the data subjects.

Moreover, the GDPR emphasizes the importance of data subjects giving consent to the collection of their private data, under terms that are advantageous to the subjects. In particular, Article 7 of the regulation suggests that "the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language" and that "it shall be as easy to withdraw as to give consent" (Resolution 2016/679). However, research suggests that the GDPR fails to reduce the information complexity in GDPR consent forms, and does not explicitly designate certain forms, such as pre-checked boxes, as valid forms of consent, leaving this responsibility to individual member-states (van Ooijen and Vrabec 2019, p.104). Therefore, according to the regulation, the citizens whose data are being processed may enjoy an extensive level of control over the processing of their data, allowing them to be fully informed over the terms under which they give consent, as well as

allowing them to withdraw freely. Yet, the implementation has not been perfect, with consent still being given under ambiguous conditions on occasion.

In addition, evidence from the first year of implementation of the GDPR suggests that there exists a level of awareness of the GDPR among citizens, as multiple reports have been made by citizens to the national data protection agencies about GDPR violations. More specifically, over the first nine months since the GDPR went into effect, the European Data Protection Board revealed that 206,326 cases of GDPR violations were reported to the national data protection agencies (Breitbarth 2019, p.12). The findings suggest that the majority of violations were either due to citizen complaints about telemarketing, promotional emails, and CCTV surveillance, or due to data breaches (Breitbarth 2019, p.12). As such, it is evident that citizens are generally responsive to the new legislation, and are willing to collaborate with the authorities to ensure that their rights are protected.

Nevertheless, the implementation of the GDPR has been imperfect. One reason is that there exist differences in implementation among member-states of the European Union. As the Center for Strategic and International Studies (2021) reports, "several Member States have been more proactive in issuing fines". For instance, in the years 2018-2021, Italy issued 88 fines for GDPR violations, Romania issued 62, and Germany issued 32 (CSIS 2021). As such, some countries seem more proactive than others in issuing fines for offenders, suggesting that some countries place higher emphasis on protecting the right to privacy. However, one must also consider that Germany was already considered as one of the frontrunners in respecting citizens' right to privacy, even before the GDPR was adopted, whereas Italy and Romania were under-performing (Custers et al. 2017, p.8). Therefore, since Germany already had established and highly-budgeted data protection authorities, most German companies had likely adopted GDPR procedures before the regulation was enforced, thus avoiding fines in the first place. Moreover, the relation between the number of fines and the total fine amount is non-linear; Spain issued more than eight times the number of fines Germany did over the three year period, yet the fine amount was approximately 53% higher for Germany than for Spain (CSIS 2021). This suggests that Spain issued more fines to smaller-sized companies, whereas Germany issued a smaller number of fines to larger-sized companies. Therefore, it appears that, even though the aim of the GDPR was common across European countries, its implementation was different on a per-country basis.

Differences also exist when accounting for the level of awareness citizens across different member-states of the European Union have about the GDPR. For instance, 90% of Swedes had heard of the GDPR, and 63% of them knew what the legislation was, according to the Commission's report; however, the corresponding amounts of French citizens were 44% and 18%, respectively (Breitbarth 2019, p.12). This could suggest that the member-states' efforts to raise awareness on the GDPR were not uniformly successful Nevertheless, one should also take into account the different "digital profiles" of citizens. Eurobarometer 91.2, a survey on Europeans' digital experiences and awareness of the GDPR, clustered citizens into four categories, based on their online activity; namely, from lowest to highest online activity and GDPR awareness, 'off-line citizens', 'social netizens', 'web citizens', and 'data citizens' (Rughinis et al. 2021, p.9). Of these categories, only the data citizens are considered to have high levels of GDPR awareness. Looking back on the comparison between Sweden and France, a third of the Swedish population could be classified as data citizens, compared to only one fifth of French citizens (Rughinis et al. 2021, p.12). In addition, countries like the Netherlands and Poland exhibit similar profiles to Sweden, both in terms of GDPR awareness and high relative prevalence of data citizens, whereas countries like Italy and Belgium exhibit similar profiles to France (Breitbarth 2019, p.12; Rughinis et al. 2021, p.12). Nevertheless, there exist exceptions to the rule, as the Czech Republic demonstrates high awareness of the GDPR, yet a low relative prevalence of data citizens, whereas the situation is reversed in Estonia (Breitbarth 2019, p.12; Rughinis et al. 2021, p.12). In general, the percentage of data citizens among the total population of member-states seems to be a relatively good indicator of the levels of GDPR awareness, suggesting that the citizens of some countries are less aware of the GDPR because it affects them less. Yet, the exceptions of the Czech Republic and Estonia signify that there are other factors behind different levels of GDPR awareness, indicating differences in how effectively the GDPR was communicated in different EU member-states.

Furthermore, it needs to be considered that, within countries of the European Union, citizens show different levels of awareness of what the GDPR is; that is to say, differences in GDPR awareness are not only present between member-states of the EU, but also among the citizens of a specific member-state themselves. In many cases, citizens have some sense of what the GDPR is, but do not precisely know what exactly the GDPR is. According to Rughinis et al. (2021), the levels of GDPR awareness within a

country can differ, based on the socioeconomic status of citizens, particularly their education, occupation, and generation (p. 13). Yet, even within a similar socioeconomic status, there still exist differences. For instance, a study on Hungarian university students suggested that, while approximately half of the students agreed with the statement "I understand the terms used in the GDPR", only a quarter of them agreed with the statement "I am knowledgeable about how my information will be used according to GDPR" (Gati and Simay 2020, p.8). This suggests that, even within a specific European member-state, there were varying levels of awareness of the GDPR, indicating a lack of uniform effectiveness in how the GDPR was communicated to different groups of citizens.

Overall, the implementation of the GDPR seems generally advantageous to European citizens, with the principles in place being supportive of their right to privacy, and the citizens actively collaborating with national data protection agencies in reporting GDPR violations. Nevertheless, the implementation of the GDPR differs on a country-by-country basis, with countries targeting differently-sized violators of the regulation, different levels of awareness of the GDPR between member-states, and differences within citizens of single European member-states.

Implementation II: Implications for the Enterprise

The GDPR does not follow what Berman (2022) describes as the 'economic style of reasoning'; instead of 'maintain[ing] a deep appreciation of markets as efficient allocators of resources' (p. 6), it focuses on promoting the right to privacy. As such, while it is beneficial to European citizens, the GDPR presents a number of challenges for enterprises.

In order to be able to operate in the European Union, any business collecting private data has to abide by the GDPR's guidelines. Because of this, companies have to implement a series of measures to ensure compliance, with regards to the principles of accountability and data security. Specifically, in order to be GDPR compliant, companies need to provide extensive documentation of how personal data is collected and processed, offer training to employees with regards to data protection, have Data Processing Agreement contracts with any data processors, designate Data Protection Officers, and implement any technical and organizational measures to ensure data safety (GDPR.eu 2018).

The regulations companies have to abide by, in order to ensure GDPR compliance, have resulted in large amounts of compliance costs. Research suggests that exposure to the GDPR has affected both the sales and profits of companies; in particular, according to Chen et al., exposure to the GDPR has reduced profits by 8.1% in 2018, the year when the GDPR was put into effect, and sales were decreased by 2.2% (p.12). Moreover, the aforementioned study suggests that, while companies of all sizes experienced a decrease in profits and sales, the impact if the GDPR was more pronounced on small firms, defined as companies with less than 500 employees (Chen et al. p.18). Therefore, it is shown that complying to the GDPR is a costly procedure for companies, and the cost is even more significant for smaller-sized companies.

One also needs to consider that different companies can respond to the challenges posed by the GDPR in ways that deviate from the aforementioned norm. This is particularly evident in the case of profits and sales for companies in the IT sector. Specifically, large IT companies seem to be less affected by the GDPR compared to most companies, with profits decreased by 4.6% and sales decreased by 0.7% (Chen et al., p.21). Yet, small companies in the same sector are at a greater disadvantage than the small-firm average, with a 12.1% decrease in profits and a 2.1% decrease in sales (Chen et al., p.21). This suggests that the GDPR may affect different sections of the economy in ways that differ from the average, as well as that the implementation of the GDPR may significantly put smaller-sized companies at a disadvantage compared to their larger-size counterparts.

Furthermore, the GDPR also obliges companies handling personal data of European citizens to report any data breaches within 72 hours from the event (GDPR.eu 2018). Because of this, any company in violation of this is subject to hefty GDPR fines, which are defined by the regulation as “up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher” (Resolution 2016/679). An instance of this was reported on CNN on November 30th, 2018, when Marriott revealed a data breach containing the personal data of millions of its hotels’ guests, which had occurred two years prior (Valinsky 2018). As the article states, “because the hack involves customers in the European Union and the United Kingdom, the company might be in violation of the recently enacted General Data Protection Regulation” (Valinsky 2018). This suggests that

companies in violation of the GDPR could be subjected to significant fines, especially when they are physically located outside the European Union, yet handling data of European citizens.

Yet, there is also significant evidence of discretion used by the national authorities of European member-states when determining the amount of the fine a company should be obliged to pay after a GDPR violation. This can be seen through two cases that occurred in January 2023. Specifically, on January 4th, 2023, Irish regulators fined Meta EUR 390 million over GDPR violations on Facebook and Instagram (Euronews). Nine days later, the French data protection agency fined ByteDance EUR 5 million over GDPR violations in how TikTok's cookies were handled (Euronews). While both companies were fined over similar grounds, there exists a staggering difference in the amount of the fine dealt to each company. This difference between the amount of fines different European member-states oblige GDPR offenders to pay is evident by a Center for Strategic and International Studies report, which shows that, among others, Italy has issued a total amount of EUR 84 million in fines from 2018-2021, compared to Spain's EUR 32 million (CSIS 2021). Therefore, it appears that the impact of a GDPR violation on a company may fluctuate, based on the country whose agency is responsible for the fine the company receives.

Lastly, the GDPR has been shown to affect lobbying practices within the European Union. From before the implementation of the GDPR, multiple companies and other organizations have been found to conduct lobbying against the GDPR, trying to limit its provisions. An article by Politico provides a series of examples of lobbying efforts. For instance, in 2017, before the GDPR came into effect, Amazon attempted to use lobbying to weaken support for the GDPR among European lawmakers (Kayali and Manancourt 2021). In addition, from the point the GDPR was put into effect, a number of European countries, supported by lobbying efforts, attempted to enforce limits on the GDPR, on the basis of detecting sexual abuse material and handling criminal cases (Kayali and Manancourt 2021). Moreover, some of the most prominent tech companies have become some of the biggest corporate spenders on lobbying, with Google, Meta, and Apple making the top 5 (Frey and Presidente). This serves as another example of the potential for serious repercussion the GDPR can have on companies violating it; nevertheless, it also highlights the effort made by a number of companies to use lobbying, in order to limit the implications the GDPR could have on them.

Overall, the GDPR appears to have a profoundly negative effect on the enterprise sector. In order to become GDPR compliant, companies are obliged to pay a significant amount of compliance costs, which can be particularly challenging for smaller-sized firms. In addition, the fines that can be imposed can potentially be very harmful to the companies found violating the GDPR. Nevertheless, there also exists evidence of discretion over the fine amounts for different cases, as well as lobbying efforts trying to limit the GDPR, so that potential implications for companies are mitigated.

Implementation III: Implications for Technological Development

Given how the GDPR is concerned with the protection of European citizens' private data, it is evident that companies in the technological sector are particularly affected by this piece of legislation. One way the GDPR affects those companies are fines. As mentioned in the previous section, companies can be charged a significant amount of fines, if they are found violating the GDPR in any way. For instance, Meta was fined EUR 1.2 billion by the Irish data protection agency in May 2023, because the company transferred personal data to the United States without adequate data protection mechanisms, whereas Amazon was fined EUR 746 million by the Luxembourgian authorities in July 2021, because the company used targeted advertising without the users' consent (Data Privacy Manager 2023). Nevertheless, companies often attempt to appeal those fines, and lobbying also attempts to mitigate the effects of the GDPR on these companies, as mentioned in the previous section of this study.

However, it also needs to be noted that the GDPR has resulted in tech companies suspending some services to the European Union. This is because, according to the regulation, Data Protection Authorities of European member-states are entitled to issue "a temporary or definitive ban on [data] processing" (European Commission) on companies violating the law. As such, services that rely on data collection that may violate the GDPR may not operate in the European Union. On May 11th, 2018, CNN reported that a number of small companies offering services such as social networking and online gaming had to either fully shut down their services, or block access to them from the European Union (Kottasova 2018). Furthermore, even two years after the GDPR was enforced, many American news outlets were not accessible from within the European Union, as they preferred to block access to Europeans than to comply to the GDPR (Digital Watch Observatory 2020). However, perhaps the most notable such suspension occurred with regards to the ChatGPT artificial intelligence model. In particular, access to the

model was blocked in Italy on April 1st, 2023 (McCallum 2023), as the Italian data protection authority accused OpenAI of unlawfully collecting users' private data. Access to the service was restored on April 28th of that year, as the company stated that the privacy issues that led to the block were addressed (Robertson 2023). Yet, in January 2024, Italian authorities once again accused OpenAI of GDPR violations, although the service was not banned in this case (Reuters 2024). Overall, the GDPR provides challenges to companies working in the tech sector, as they often have to rewrite the code behind their services, in order to be GDPR compliant, and any services that cannot be rewritten to abide by the GDPR principles could possibly be suspended.

However, aside from the general concerns about the GDPR being responsible for the suspension of services in the European Union, the example of OpenAI and ChatGPT presents a bigger issue, on how GDPR may affect technological development itself, with artificial intelligence being perhaps the biggest such battleground. This is because artificial intelligence models, in order to be trained before they are ready for production, require the processing of large amounts of data, a lot of which may be considered personal, and thus protected, by the GDPR. The European Parliamentary Research Service (EPRS, 2020) published a detailed study on the impact of the GDPR on the development of artificial intelligence, which highlights a number of challenges that have to be faced, in order to reconcile the data protection aim of the GDPR with the goal of advancing artificial intelligence models. In particular, the report states that a number of challenges exist when deploying artificial intelligence models, with regards to the collection of personal data, such as the ability to profile a person based on the data collected from them, the right to consent and the right to erasure of personal data, as well as concerns on how the automated decision-making process that AI models could affect data subjects (EPRS 2020, pp.74-75). While the report claims that the GDPR can be compatible with the growth of artificial intelligence models, it also states that the GDPR's clauses are vague and open-ended with regards to AI (EPRS 2020, pp.76-78). As such, it is evident that the GDPR did not seriously consider the potential of artificial intelligence in the regulation's text. Because of this, data protection agencies could exercise discretion and impose restrictions on artificial intelligence development.

Moreover, it appears that the GDPR may result in uneven technological development, stifling start-up innovation while benefiting already large tech companies. With regards to start-ups, the GDPR and

resulting changes in the European market could result in innovation exploiting the new regulatory environment, the GDPR has also shown to result in entrepreneurial discouragement, as these start-up companies are stifled by adhering to data minimization, as well as forced to suspend services that cannot be adjusted to be GDPR compliant (Martin et al 2019. p.1321). On the other hand, already big companies, such as Google, may exploit the disadvantageous situation for start-up companies, and use their own strengths to further consolidate their influence in the tech sector, as the limitations on data sharing may make companies collecting greater amounts of data have a greater competitive advantage, besides the higher ability to pay the GDPR compliance costs (Geradin et al 2021., p.63). Therefore, it appears that the GDPR has an unintended consequence of furthering the consolidation of power to larger companies in the tech sector, as it limits start-ups' ability to innovation, while also increasing the competitive advantage companies already collecting large amounts of personal data have.

Overall, the GDPR has profound implications on the tech sector. Given how companies in the sector are responsible for collecting vast amounts of data, they are particularly prone to GDPR violations, thus resulting in high fines and suspension of services in the European Union. Moreover, the GDPR fails to address some of the newest technologies available, such as new artificial intelligence models, and thus can limit technological innovation. This challenge to innovation is further aggravated by the GDPR's unintended consequence of consolidating power to the larger tech companies, while stifling start-up innovation.

Policy Implications

While the GDPR provides a solid basis on which the European citizens' right to privacy is protected, its current implementation is characterized by a number of flaws, harming enterprises and technological progress, as well as preventing the legislation from its maximum potential. As such, a number of policy implications could be considered to improve the GDPR, in order to both strengthen its ability to ensure the citizens' right to privacy, as well as to mitigate the negative impact on companies, especially smaller-sized ones, and technological innovation.

One of the most significant issues that exist with the GDPR is that it fails to effectively address the issue of discretion. While the consolidation of the previously existing national data protection regulations under

the oversight of the Data Protection Directive has been a major step in eliminating discretion away from European member-states, the GDPR remains actively enforced by the European member-states' national data protection agencies. Moreover, while the GDPR stipulates very high possible fines for companies violating the GDPR, the enforcement of the GDPR by national agencies has worked on companies' behalf, as they can conduct more effective lobbying campaigns and receive smaller fines than the ones they should expect. Given how the GDPR has resulted in the creation of the European Data Protection Board, the GDPR could be amended to further increase the authority of the Board, from a regulatory body overseeing national data protection agencies, to a pan-European agent enforcing the GDPR across all of the EU member-states.

Moreover, an issue the the GDPR has not effectively addressed is the right to consent. Under the existing regulations, the GDPR should, in theory, allow European citizens to provide unambiguous consent to any companies willing to process their personal data, as well as provide the right to easily withdraw consent previously given. Nonetheless, the GDPR has not effectively addressed whether all ways companies will use to obtain consent meet the criterion of unambiguity, leading to situations where there can be disputes over whether a user actually gave consent to the collection and processing of their private data. One possible solution to this issue could be to introduce a common form of providing consent, to be used across websites operating in the European Union, replacing the individual prompts websites now provide to their users., ensuring that consent is given in unambiguous terms.

In addition, creating more efficient means of communicating the GDPR to European citizens should be considered. Evidence suggests that there are multiple differences in the understanding of the GDPR by European citizens, affected by both the citizens' home country, as well as their socioeconomic status. Even when keeping those variables constant, there still exist differences in the level of understanding of the GDPR, suggesting that the current means of communicating what the GDPR is have different levels of effectiveness for various citizens. In order to alleviate this issue, the European Union should consider creating a comprehensive information campaign on what the GDPR entails for people across member-states and socioeconomic statuses, by using all possible forms of mass media.

In addition, the GDPR should also be amended, so that it addresses some of the issues it currently generates for a number of enterprises. For instance, it appears that the GDPR stifles start-ups and smaller-

sized companies in general, thus providing some indirect benefits to already established large companies. In order to ensure fairer competition, the European Union should attempt to alleviate the high GDPR compliance costs, by providing financial incentives to companies to become GDPR compliant, as well as providing financial aid to small companies willing to be GDPR compliant.

Moreover, an issue that should be addressed is the potential of the GDPR to limit technological innovation. On one hand, this issue could be alleviated by helping start-ups become GDPR compliant, thus fostering the entry to market of new, innovative companies. On the other hand, the GDPR also needs to address the advent of new technologies. In a way, the GDPR faces the same issue the Data Protection Directive faced in the 1990s: shortly after the legislation is put in effect, new technologies change the way data is being collected and processed, and the regulation fails to address the new challenges. In order to alleviate this issue, a two-component approach could be considered. To begin with, the European authorities could try to implement laws on top of the GDPR to provide a more concise and clear framework on using these new technologies in a way which will both advance technological process and respect users' personal data. This is already being addressed by the EU, as the European Parliament has already drafted a new AI Act, which will provide an ethical framework on the use of artificial intelligence (European Parliament 2023). However, the EU should also ensure that the advent of new technologies in the future can be more quickly addressed. Therefore, an agency monitoring new technological developments and the use of personal data they entail could be established, in order to more quickly observe technological developments and recommend new pieces of legislation, addressing those developments.

Overall, the GDPR provides a solid foundation on safeguarding the European citizens' right to privacy. However, a number of policy implications could still be considered, in order to further protect the citizens; rights and to mitigate negative effects of the law on enterprises.

Conclusion

On May 25th, 2018, the General Data Protection Regulation, perhaps the world's first comprehensive and large-scale data protection regulation, was enforced by the European Union. The new legislation has

affected individuals and companies around the world, as the regulation obliged companies to follow specific principles when collecting and processing the private data of European citizens.

This legislation attempted to resolve some of the decades-long issues that were present in previous approaches to data protection, with the most notable one being the Data Protection Directive, which guided the European data protection approach before the GDPR. In particular, through the GDPR, the European Union tried to address two major issues. On one hand, it tried to consolidate the multiple separate data protection regulations all EU member-states had before the enforcement of the GDPR, thus mitigating the effects of discretion by European countries. On the other hand, it also attempted to address the challenges raised by the exponential growth of the Internet, as well as the immense data collection that followed this growth. The implementation of the GDPR has been largely successful in these two aspects, although the maintained existence of national data protection agencies allows for discretion to persist.

In addition to changing the regulatory environment, the GDPR provided a clearer description of the organizational actors affected by the GDPR, by defining the data subjects, data controllers, and data processors. Moreover, the GDPR also established the European Data Protection Board, which now oversees the activities of national data protection agencies in enforcing the GDPR.

In general, the GDPR is mostly beneficial to the data subjects, as the principles that now guide data transactions act to the benefit of individuals against corporate interests. While the GDPR has largely been endorsed by European citizens, who seem to actively collaborate with the data protection agencies in enforcing the new legislation, a number of issues persist, as the users' right to privacy is challenged by ambiguity in giving consent, as well as substantial difference between the enforcement and communication of the GDPR across EU member-states.

On the contrary, the GDPR has been mostly harmful for the enterprise. In order to enforce the ethical principles of data collecting and processing, companies are now forced to implement a series of measures, in order to comply to the GDPR and keep offering their services. This has resulted in very high compliance costs, which have resulted in companies losing considerable amounts of profits and sales. Moreover, the GDPR also seems to introduce an unintended consequence of strengthening the bigger

companies against the smaller ones, as the compliance costs can be especially challenging for smaller companies, while larger ones seem better able to adapt to the new regulatory environment.

The GDPR has also particularly affected the tech sector. Given the prevalence of data collection within the sector, companies operating within it are particularly prone to GDPR violations, which can result in hefty fines or the outright suspension of services within the European Union. Moreover, the ambiguity surrounding new technologies such as artificial intelligence seems to cause harmful effects on technological development. Lastly, the tech sector is also prone to the aforementioned consequence of strengthening already established corporations at the expense of start-ups, thus also contributing to innovation stifling.

Because of these implementation flaws, the GDPR could be significantly amended through a series of policy implications, which would further assist the protection of users' private data, as well as mitigate the negative effect the GDPR ha on small enterprises and technological development. Nonetheless, the GDPR remains a monumental piece of legislation, which provides a solid basis upon which the private data of European citizens can be protected.

Sources

20 biggest GDPR fines so far. (2023, September 19). Data Privacy Manager. https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

3 years later: An analysis of GDPR enforcement | Strategic Technologies Blog | CSIS (Center for Strategic and International Studies). (2021). Retrieved February 26, 2024, from https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement

A brief history of big data everyone should read. (2015, February 25). World Economic Forum. https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/

Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI | News | European Parliament. (2023, December 9). https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

Berman, Elizabeth Popp (2022). Thinking Like an Economist. Princeton University Press.

Breitbarth, Paul. (July 2019). "The impact of GDPR one year on". Network Security, pp. 11-13.

Chen, Chinchih, et al. (January 6th, 2022)."Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally". Oxford Martin School, University of Oxford,

Custers, B., Dechesne, F., Sears, A., Tani, T., Van der Hof, S. (2017) A comparison of data protection legislation and policies across the EU, Computer Law & Security Review, DOI: 10.1016/j.clsr.2017.09.001

Damien Geradin, Theano Karanikioti & Dimitrios Katsifis. (2021). GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech, European Competition Journal, 17:1, 47-92, DOI: 10.1080/17441056.2020.1848059

Data Protection in the EU—European commission. (2023, July 4). https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

France fines TikTok €5 million for its handling of users' cookies. (2023, January 13). Euronews. https://www.euronews.com/next/2023/01/13/tiktok-slapped-with-a-5-million-fine-by-french-regulators-over-its-handling-of-users-cooki

Frey, Carl Benedikt, and Presidente, Giorgio. (2022, March 10). The GDPR effect: How data privacy regulation shaped firm performance globally. CEPR. https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally

Gati, Mirko, and Simay, Attila. (2020). "Perception of Privacy in the Light of GDPR". Proceedings of the European Marketing Academy.

Ireland fines Meta €390 million in latest privacy crackdown. (2023, January 4). Euronews. https://www.euronews.com/my-europe/2023/01/04/ireland-fines-meta-390-million-in-latest-privacy-crackdown

Kayali, Laura, and Manancourt, Vincent. (2021, February 10). How Europe's new privacy rules survived years of negotiations, lobbying and drama. POLITICO. https://www.politico.eu/article/europe-privacy-rules-survived-years-of-negotiations-lobbying/

Kottasová, I. (2018, May 11). These companies are getting killed by GDPR. CNNMoney. https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html

Lipsky, M. (2010). Street-level bureaucracy: Dilemmas of the individual in public service. Russell Sage Foundation.

Many US news sites unavailable due to GDPR non-compliance | Digital Watch Observatory. (2020, September 27). https://dig.watch/updates/many-us-news-sites-unavailable-due-gdpr-restrictions-compliance

Martin, N., Matt, C., Niebel, C. et al. (2019). How Data Protection Regulation Affects Startup Innovation. Inf Syst Front 21, 1307–1324. https://doi.org/10.1007/s10796-019-09974-2

McCallum, Shiona. (2023, March 31). ChatGPT banned in Italy over privacy concerns. https://www.bbc.com/news/technology-65139406

OpenAI's ChatGPT breaches privacy rules, says Italian watchdog. (2024, January 30). Reuters. https://www.reuters.com/technology/cybersecurity/italy-regulator-notifies-openai-privacy-breaches-chatgpt-2024-01-29/

Panel for the Future of Science and Technology. (June 2020). "The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence". European Parliamentary Research Service.

Regulation—2016/679—EN - gdpr—EUR-Lex. (n.d.). Retrieved February 27, 2024, from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Robertson, A. (2023, April 28). ChatGPT returns to Italy after ban. The Verge. https://www.theverge.com/2023/4/28/23702883/chatgpt-italy-ban-lifted-gpdp-data-protection-age-verification

Rughiniș, R., Rughiniș, C., Vulpe, S. N., & Rosner, D. (2021). From social netizens to data citizens: Variations of GDPR awareness in 28 European countries. Computer Law & Security Review, 42, 105585. https://doi.org/10.1016/j.clsr.2021.105585

The history of the general data protection regulation | European Data Protection Supervisor. (2018, May 25). https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Top 18 big data companies of 2024. (2022, November 4). https://www.knowledgehut.com/blog/big-data/big-data-companies

Valinsky, J. (2018, November 30). Marriott reveals data breach of 500 million Starwood guests | CNN Business. CNN. https://www.cnn.com/2018/11/30/tech/marriott-hotels-hacked/index.html

Van Ooijen, I. and Vrabec, Helena. (2019). "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective". Journal of Consumer Policy 42:91–107.

Voigt, Paul, and von dem Bussche, Alex. (2017). "The EU General Data Protection Regulation (GDPR): A Practical Guide". Springer.

What if my company/organisation fails to comply with the data protection rules? - European Commission. (n.d.). Retrieved March 1, 2024, from https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_en

What is GDPR, the EU's new data protection law? (2018, November 7). GDPR.Eu. https://gdpr.eu/what-is-gdpr/