General Data Protection Regulation Compliance on United States Based Small to Medium Sized Enterprises

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Parul Goswami

Spring 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

MC Forelle, Department of Engineering and Society

Introduction

In a world where technology is advancing and the internet continues to be highly connected, maintaining privacy and ownership of one's data becomes increasingly difficult. From comprehensive cookies to data privacy leaks, to the selling of one's data collected by a third-party company sold for advertising purposes, there is a growing concern amongst consumers of technology around the ability to safeguard their data – or at the very least consent to its use. Pew Research Center's 2023 survey corroborates this, finding that "More than half of Americans (56%) say they always, almost always or often click "agree" without reading privacy policies" and that "About six-in-ten Americans (61%) think they're ineffective at explaining how companies use people's data" (Faviero, 2023). Internationally, the European Union has established legislation to protect the data of its people.

The General Data Protection Regulation (GDPR) for residents of the European Union (EU) is a legislation of interest helping users gain more autonomy in how their personal identifiable data is stored and kept by entities (Marini et al., 2018). As GDPR applies to all companies operating within the European Union, this means US based organizations operating in the EU also fall under compliance needs. While creating more incentives around maintaining a user's data privacy, GDPR compliance uniquely places pressure on US-based small to medium sized enterprises (SMEs) specifically culminating into becoming a significant barrier to entry into the European market.

Announced in April 2016 but in effect since May 25th, 2018, the GDPR is one of the most comprehensive data protection policies in the world, aiming to protect individual's personal data by applying to businesses that collect said data on or offline (Marini et al., 2018). Specifically, the regulation applies to all people in the 27 member countries of the European

Union and the three member countries of the European Economic Area (EEA) Norway, Iceland and Liechtenstein (*EEA & UK General Data Protection Regulation (GDPR* , n.d.). This paper specifically discusses the EEA GDPR, referenced as just GDPR, rather than the UK GDPR that came into effect after the United Kingdom exited the European Union in 2021. Since the regulation applies to all people in the EU and EEA, companies operating internationally, offering their goods and services in the EU are also required to abide by these constraints (Singh, 2020). For companies with a primary influence in the US but with a growing interest in transitioning business into the EU, these constraints can be difficult to manage as they are geo-specific. Especially since such extensive data protection regulations are not present within the US to the same extent, other than the California Protection Act (CCPA) which provides different coverage and consequences, having to offer different data protection policies based on different geographic regional operations can be intensive for companies with limited resources such as small to medium sized enterprises. SMEs are internationally recognized as enterprises with 1-250 people in staff headcount and a turnover total of less than or equal to 43 million euros and balance sheet total of less than or equal to 50 million euros (*SME Definition - European Commission*, n.d.).

In general, the advent of GDPR and the consequent requirement for affected companies to remain compliant has had widespread effects on companies of all sizes. Compliance requires major data changes and reworkings to internal and customer-facing infrastructure that larger companies have the resources to dedicate towards compliance that smaller enterprises lack (Brodin, 2019). Thus, the research question of interest is: how does GDPR compliance uniquely impact US SMEs? The literature review will cover GDPR in more depth, examples of entities that must be in compliance, the state of SME compliance in early 2018 before the regulation

came into effect, and a discussion of the sociotechnical framework of interest, the social construction of technology. To conduct my analysis, I referenced the United States and EU government publications on GDPR compliance, journal articles from law, science, technology, and business journals, and chapters from books. These articles were published in anticipation of GDPR or after GDPR came into effect and were analyzed for compliance hurdles specifically for US SMEs. Through this analysis, I found that geographic location, the United States law landscape as compared to the EU, and incumbent competition in the field uniquely apply financial and resource pressure on US SMEs discouraging smaller to medium sized enterprises from entering the European market if not already present.

Literature Review

GDPR is based on the previous directive, DIR95, expanding the scope of protected data to include unstructured data. Moreover, GDPR includes any information combined with sensitive data that may identify an individual as protected data under the regulation's scope (Brodin, 2019). Common examples of sensitive data include social security numbers, health information as protected by the Health Insurance Portability and Accountability Act (HIPAA), and bank account login information, in the United States. These and many other examples are easy to recognize and comprehend by the US public as personally identifiable. However, there are several other identifiable data points, oftentimes based on someone's digital footprint, that GDPR also protects. For example, the judgment of *Scarlet Extended SA v Socidte belge des auteurs, compositeurs et editeurs SCRL (SABAM)* by the Court of Justice of the European Union found that internet service providers (ISPs) can use other information they gather with a user's IP address to identify the individual, establishing IP addresses as personal data within the European Union. In contrast, IP addresses are not considered personal data in the United States unless

specifically protected by an act. Examples of current US acts that protect IP addresses include HIPAA and the Children's Online Privacy Protection Act of 1998 (COPA) (Ducich & Fischer, 2018). Thus, this difference in data privacy coverage poses extra effort for GDPR compliance.

GDPR is a comprehensive and thorough piece of literature. Comprised of 99 articles and 173 recitals, some authors have analyzed the contents of the regulation to distill its essence in three distinct facets: lawful processing, data user's rights, and data controller's obligations. Each of these buckets relates to at least two of the principles of GDPR: legitimacy, proportionality, empowerment, transparency, accountability, and security (Irwin, 2022).

Looking deeper into the regulation, it becomes apparent how wide the definition of 'data controller' is, and how it does not just limit itself to profit-seeking entities like companies and institutions. One lesser-known group affected by GDPR is researchers. Researchers working with biometric, genetic, and other personal health data fall under GDPR compliance (Chassang, 2017). In general, researchers working with human subjects and thus data points that may contain personal identifiable information must be in compliance with GDPR, specifically in data wrangling methodologies to include pseudonymization or anonymization to protect the individual's data and still glean research results (Crutzen et al., 2019). Many reports have already been released on methodologies that can be used to pseudo-anonymize personal identifiable data, one case study includes techniques that have been used on mobile device information (Štarchoň & Pikulík, 2019). Researchers can work under a variety of institutions from political advocacy groups to institutions, with varying sizes and resources available for them to remain compliant under these data controller-specific aspects of the regulation, and as such, can be considered small to medium sized enterprises based on their circumstances.

The impact of GDPR on SMEs in general has been widely discussed for those operating from the EU, with expansive coverage on these SMEs versus larger enterprises. Based on a survey conducted by the Irish SME Association (ISME), 82% of businesses were aware of GDPR, as of January 2018 given that the regulation goes into effect four months later (ISMEs, 2018). However, given the proximity of the survey to the regulation beginning to go into effect, the preparedness of the EU SMEs surveyed has cause for concern. Of those surveyed, 70% did not know what steps are needed to be compliant, and 62% of businesses did not know what changes in compliance GDPR brings as compared to DIR95, a predecessor of current GDPR legislation (ISMEs, 2018).

Understanding the efforts behind GDPR compliance for US SMEs is important when considering the barriers to entry into the European market. Geographic market growth is a natural milestone for companies experiencing growth and success, and understanding how compliance impacts SMEs specifically will help companies strategize their European expansion efforts. Specifically, strategy can revolve around resource and time allocation, helping companies decide how to prioritize their efforts to achieve compliance in the smoothest way possible.

The sociotechnical theory I will use to analyze my results will be the Social Construction of Technology (SCOT) by Trevor Pinch and Wiebe Bjiker. The main idea of this theory is that technology is not constructed in a vacuum but instead, society and technology are co-constructed simultaneously. Specifically, I will be utilizing interpretative flexibility from the theory, the idea that there are differing interpretations of the natural world are available (Pinch & Bijker, 1984). I will analyze how US-based SMEs have a differing interpretation of GDPR compliance given the different hurdles uniquely placed upon them.

Methods

Specifically, I have looked at content about United States small to medium sized entities that are operating or that will be operating under GDPR compliance to conduct my case study analysis. For primary sources, I referenced articles published by the European Union and the United States government like the Federal Communications Commission. For secondary sources, I looked at articles from law journals like HeinOnline, science and technology journals like SciTech Law, and even biological journals and sections of books that discussed GDPR. I specifically sought out and analyzed articles that were published in anticipation of GDPR going into effect and beyond (years 2017 – present day). I included articles that were published before GDPR was set in place to account for productive insights and discussions that occurred at the time based on what was expected from GDPR, and opinions generated from its predecessor DIR95.

Analysis

GDPR imposes extra compliance requirements for United States businesses due to the United States law landscape. Differences between the state of data privacy laws in the United States and the European Union percolate in the need for additional requirements to remain GDPR compliant in contrast to that to remain compliant with similar privacy laws in the United States. For example, the definition of personal data differs in United States general law from that present in the vocabulary of the GDPR. Personal identifiable information (PII) has been found to be circumstantially protected in the United States (Ducich & Fischer, 2018). Stricter than PII, yet still a subsect of its definition, GDPR outlines personal data as any information that may result in the identification of an individual or data subject (Ducich & Fischer, 2018). As explored in the introduction, the inclusion of any information such as public information combined with personal information can be utilized together to identify individuals. This broader and more

flexible definition of data that is meant to be protected has been found to be not protected enough in US law to be compliant with GDPR for general US Law as a whole (McAllistar, 2017). Another example of where United States privacy laws and GDPR differ in the definitions of data breaches. These differing definitions yield different outcomes, with a stricter data breach definition in GDPR necessitating at most 72 hours to notify data officials (Ducich & Fischer, 2018). On the other hand, as outlined by the Federal Communications Commission, US law requires telecommunications carriers to notify Secret Service and FBI agencies immediately, and at most 7 business days of notification of the data breach (*Data Breach Reporting Requirements*, 2024).

These differences put extra pressure on United States SMEs because they are smaller and less likely to be able to pivot towards different compliance efforts towards a subsect of their users. Oftentimes, compliance requires the expensive efforts of a legal team embedded with the legal know-how of compliance law, and more efforts that will be discussed later, that further show how difficult it may be for an SME to break into the European Union market as compared to an EU-based SME.

In recent years, the law landscape has changed on a state-to-state basis, originating in California with the California Consumer Protection Act (CCPA). Influenced by GDPR, the CCPA passed in 2018 and has been in affect since January 1st, 2020, applies to the data of all California residents (Barrett, 2018). While having its own flavorings for data privacy tenents, in layman's terms, GDPR and CCPA hold the following rights in common: the right to be informed, the right to access and the right to object (Barrett, 2018). Still, differences exist and full compliance with CCPA does not maintain full coverage of compliance for GDPR from various facets such as GDPR's caveats with international data transfers.

While acknowledging strides United States law has made towards similar capacity data privacy coverage as GDPR, that does not change how the proximity of the United States to the European Union adversely applies financial pressure to SMEs easily pivoted by larger companies. One especially tricky use case of GDPR compliance for American companies regards data transfers and storage. GDPR makes international data transfers difficult to outside of the European Union. Specifically, GDPR states that data can be transferred to the destination country if the data safety laws are considered "adequate". As previously discussed, the United States does not hold such adequacy standards, even today with CCPA. Thus, extra precautions must be taken which is difficult for small businesses with limited resources and time (McAllister, 2017). For example, companies have various options for data storage capabilities from cloud storage to on-premise servers to data centers. Whereas previously SMEs were able to easily transport this now-protected data to on-premise United States servers and data centers, either expensive precautions must be taken or such data may be processed in the European Union. While SMEs must wrangle with these different options, altering their data storage schema and strategy for cost-effectiveness, larger United States businesses can avoid this data transfer use case altogether by either purchasing or building dedicated data centers for their data needs present in the European Union (McAllister, 2017). Such an expensive pivot does not come as easily to SMEs with limited resources, influence, and employees as larger technology companies with vast more connections.

As explored when considering geographic location, GDPR compliance favors incumbents, already compliant US-based companies, and larger US-based companies with greater access to money and personnel. The implementation and effect of GDPR did not come as a surprise, as it expanded on its predecessor DIR95. Moreover, GDPR was announced in 2016 and went into effect in 2018, leaving a period of time for companies to strategize how they were

going to continue business operations as normal, but this time under compliance. Larger US-based companies can generally afford to redirect employed personnel and adopt consultants for their compliance needs, restructuring their infrastructure quickly and expensively to remain compliant. As one article found,

> Major companies such as Facebook and Microsoft have already implemented procedures to ensure some compliance with the GDPR, whereas other companies, like Apple, are still assessing their products and services to ensure they are in full compliance. Companies in compliance have adopted one of two popular approaches to ensure compliance: (1) providing different rights to individuals depending upon their location; or (2) affording the same heightened GDPR privacy rights to all users globally. (Gosnell, 2019).

Following option one and providing a differentiated customer approach requires unintuitive redundancy in systems and hosting offerings for customers based on their location. For example, one "low hanging" fruit of GDPR compliance is gathering of user consent for the lawful processing of their personal data. In a scenario where this offering requires a lot of support and developer time, as well as different checks based on showing this question based on whether this user was present within the European Union or not, would require dedicated support and extra effort for this less cohesive internationalization effort. On the other hand, if a company were to offer option two where GDPR level data privacy rights were being offered to all customers, this would require the entire upheaval of data processing, transfers, storage and more to the entire company's logistical network –requiring a full scale and short turn around shift in the company, likely requiring all hands on deck. Neither option seems the most likely or easily available for an SME. Moreover, at the time of announcement and early days of compliance, understanding GDPR compliance was a difficult and jargon heavy process. While larger companies are able to

afford consultancy, SMEs will not be able to afford the same cuts to their profit margins. Buying compliance help can be expensive, as seen by “Microsoft's "Compliance Solutions" (which are really just Microsoft Office products) range in price between $5.00-$12.50 per month, per user. For a company of 250 people, GDPR compliance through Microsoft would automatically create a $15,000-$37,000 additional annual expense.” (Gosnell, 2019). Thus, with neither option one or two highly accessible, and employing consultancy tools expensive, it becomes clear that either way an SME may choose will require an upheaval of legacy systems and processing to an extent.

Yet some may argue that US-based SMEs are by no means required to undergo these trials and tribulations with GDPR compliance and can instead exit the European Union market. However, by stopping service to European Union customers due to GDPR compliance costs, SMEs are unfairly being pushed out of a market that previously served them and a subsect of customers and financial gains that larger company competitors can still access. Running the risk of compliance violation fees or expensive costs towards continued compliance through infrastructure and data storage changes, smaller enterprises simply must pay to “win” either path they choose to go about compliance. As Fendian observes,

> Consequently, small U.S. businesses are caught "between a rock and a hard place": either they pour vital resources into a complete reconfiguration of their data processing technology, likely threatening the revenue from whatever product or service they offer, or they are sanctioned with a GDPR violation fine that is so severe it nearly bankrupts them. (2019).

US-based SMEs are not alone in these struggles, with EU SMEs facing similar hurdles in the face of GDPR compliance. In 2019, with GDPR going into effect since May, 2018, GDPR compliance affected around 23 million SMEs with the EU. The 2019 GDPR Small Business

Survey found that around half of small businesses surveyed are failing GDPR compliance when it comes to describing the lawful basis on retaining a user's data and clearly stating how data will be processed (*Millions of small businesses aren't GDPR compliant, our survey finds*, 2019).

Conclusion

Since May 2018 when GDPR came into effect, enterprises must wrangle with GDPR compliance in order to continue their operations in the European Union. US-based SMEs in particular must contend with compliance with privacy laws in the United States and that of GDPR, posing stricter requirements on the handling of personal data. Moreover, the geographic location and associated distance of the US makes techniques to remain compliant more expensive such as viable data storage options. Adding on to financial and resource pressure, GDPR favors incumbents already established in the European Union market or with enough money to incur compliance penalty mistakes that US SMEs simply cannot spare. Thus, while compliance means the same outcomes for whichever entity must remain compliant under GDPR coverage, the nuances of compliance and the effort required diverge in meaning for US SMEs versus other entities, favoring those enterprises with more personnel and money to pivot and handle the hurdles GDPR compliance throws. All of these factors culminate as a significant barrier to entry into the European market for US-based SMEs, reducing competition from these entities and instead favoring industrial and geographical incumbents. These difficulties likely influence US SMEs to interpret GDPR compliance as an added barrier to other markets their peer enterprises have easier access to. While changes to GDPR are less likely to occur, these factors can be taken into account when a US SME is strategizing their entry into the European Union or taken into consideration when analyzing the success such entities experience in the EU.

I conducted this research with US SMEs interested in potentially entering the European market in mind. The discussion and findings in this paper hope to inform such entities a more well-rounded view of what compliance efforts may look like and how compliance requires a heftier dowry than that incurred by larger institutions. Future work can look at what EU SMEs face in order to compare and contrast such factors with those of US SMEs. Furthermore, future research can consist of a repository of lessons from a select few companies that have emerged and have not successfully entered the European market due to GDPR compliance woes. These lessons can be applied and shared with future generations of US SMEs, dispersing helpful tips and tricks relating to compliance, and encouraging competition in these markets.

References

Barrett, C. (2018). Are the EU GDPR and the California CCPA Becoming the Defacto Global Standards for Data Privacy and Protection. *SciTech Lawyer, 15*(3), 24–29.

Brodin, M. (2019) A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. *European Journal for Security Research* 4, 243–264. https://doi.org/10.1007/s41125-01900042-z

Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. *Ecancermedicalscience*, 11. https://doi.org/10.3332/ecancer.2017.709

Crutzen, R., Ygram Peters, G.-J., & Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. *Psychology & Health, 34*(11), 1347–1357. https://doi.org/10.1080/08870446.2019.1606222

Data Breach Reporting Requirements. (2024, February 12). Federal Register. https://www.federalregister.gov/documents/2024/02/12/2024-01667/data-breach reporting-requirements

Ducich, S., & Fischer, J. L. (2018). The General Data Protection Regulation: What U.S.-Based Companies Need to Know Survey - Cyberspace Law. *Business Lawyer, 74*(1), 205–216.

EEA & UK General Data Protection Regulation (GDPR). (n.d.). Retrieved April 5, 2024, from https://access.tufts.edu/eea-uk-general-data-protection-regulation-gdpr

Faverio, M. (2023, October 18). Key findings about Americans and data privacy. *Pew Research Center*.Retrieved April 5, 2024, from https://www.pewresearch.org/short reads/2023/10/18/key findings-about-americans-and-data-privacy/

Fendian, C. (2019). Now What? A New Direction for U.S. Businesses and Law in the Wake of the General Data Protection Regulation Notes. *Southern California Interdisciplinary Law Journal*, *29*(1), 129–154.

Gosnell, C. (2019). The General Data Protection Regulation: American Compliance Overview and the Future of the American Business Notes & Comments. *Journal of Business and Technology Law*, *15*(1), 165–188.

ISME (2018) Businesses unprepared for GDPR. Retrieved 5 June 2018, from https://www.isme.ie/report businesses-unprepared-gdpr/

McAllister, C. (2017). What about Small Businesses: The GDPR and Its Consequences for Small, U.S.-Based Companies Notes. *Brooklyn Journal of Corporate, Financial & Commercial Law*, *12*(1), 187–212.

Millions of small businesses aren't GDPR compliant, our survey finds. (2019, May 20). GDPR.Eu. https://gdpr.eu/2019-small-business-survey/

Pinch, T. J. & Bijker, W. E (1984). The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science, 14*, 399-441

SME definition—European Commission. (n.d.). Retrieved April 5, 2024, from https://single market economy.ec.europa.eu/smes/sme-definition_en