Divergences in Data Protection: A Comprehensive Analysis of GDPR Implementation in Germany, Austria, and Ireland

Sarah Elizabeth Russell

Sara Wallace Goodman
May 27, 2024

Acknowledgements

I am tremendously grateful to my amazing thesis advisor, whose support and advice has been instrumental for my academic career. I also could not have produced this thesis without the support from my family and friends who stood by me through it all. I love you more than I could ever communicate.

Table of Contents

I. Abstract

This paper examines the role of the General Data Protection Regulation (GDPR) and its implementation and effectiveness at enhancing the data protection laws of the EU and its member states. Prior to the implementation of the GDPR, multiple countries have different iterations of data protection laws, which led to confusion when trying to resolve disputes across differing jurisdictions. But by adopting a harmonizing framework, the GDPR has enhanced the overall data protection environment of the EU, and provides an overarching goal for EU member states to create a "one stop shop" for anything related to data protection. By examining laws, regulations and case studies, I provide examples of the protections at work, illustrating benefits of coordination. And, moreover, the costs of violating shared rules are significant, taking the form of either fines or in some cases, imprisonment if the data breach is severe. To illustrate the benefits and costs of shared policy, I examine a spectrum of decisions relating to types of data breaches and infractions and case outcomes in three countries; Germany, Austria, and Ireland, along with the outcomes of said cases. Through this comparison, I illustrate the benefit of increased data protection for the citizens of the EU. Another provision of the GDPR that will be researched is the addition of the open clauses provision, that allows for member states to create adjustments to the GDPR at a national level to better suit their needs, potentially creating a divergence in practices across member states.

II. Introduction

Research Questions:

This paper aims to discuss and uncover why we see a divergence in different practices in data security among EU member states. In particular, I will focus on (1) Why do Germany, Austria, and Ireland have differing data subject privacy practices; (2) How do these differences in data security practices among these EU member states reflect their unique national adoption of the GDPR; and (3) What challenges and opportunities do these divergent data subject privacy practices present for the effectiveness of the GDPR in harmonizing data protection laws across the EU?

Theoretical Policy Motivation:

Since May 2016, The European Union (EU) created a legal framework that aims to ensure a high level of protection of personal data in all of the EU member states by defining directly applicable rules for personal data processing thereby harmonizing the legal situation across the EU. However, for this data protection reform to be enforceable across all member states, the assistance of "open clauses" were required to allow for member states to openly interpret their national provisions in accordance to the EU's GDPR guidelines. The open clauses provision has contributed heavily to variation among the national provisions of member states, which we can view as otherwise convergent or divergent from the initial GDPR regulation.

Research shows how the GDPR affects certain areas such as policy, economics, or more niche areas such as health data. However, there is very little research surrounding how open clauses contribute to the differences in national data security practices, as well as the challenges and opportunities these open clauses present for the effectiveness of the GDPR in harmonizing data protection laws across the EU. Additionally, current research neglects to analyze how open clauses and case laws have impacted the way member states shape their national provisions, and by proxy, their interpretation of data protection laws.

This paper examines the use of open clauses among the member states of the EU, and if they prove to further enhance the GDPR. I find that the inclusion of the open clauses of the GDPR to be a key element in the implementation process that took place, as it gives member states the ability to granularly tailor the regulation to their existing legal frameworks surrounding data protection. In conducting case study research in Germany, Austria, and Ireland, I show how these uses of the open clauses add or detract to the GDPR's overarching goal. In doing so, my goal is to better understand how member states' utilized open clauses interact with the GDPR and across member state borders. This evidence will then allow me to evaluate the GDPR as a whole and how effective it has been at reaching the mandate of a unified data protection regulation for the whole of the EU.

III. Background

From Directive to Regulation: The Evolution of the GDPR

The fundamental rights established by the GDPR provide understanding how data protection is woven into its fabric, underscoring its importance as a cornerstone of human rights in recent years. The Data Protection Directive (Directive 95/46/EC) (DPD) was the first EU-wide directive adopted to ensure the protection of individuals concerning the processing of personal data and the free movement of such data. The DPD formed the groundwork for the comprehensive approach taken by the GDPR, marking a significant step in the evolution of data protection laws to meet the demands of an increasingly digital world. [1]

However, many do not recognize how large of an impact that human rights have had on creation of data protection laws, since the mid-20th century, data protection laws have been intertwined with human rights. Many people feel that the right to data protection and the right to process our personal data is a fundamental right that each individual is granted. Under the EU Charter of Fundamental Rights' (ECFR) Title 2 *"Freedoms"*, in Article 8, its stated that:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority. [2]

The European Convention of Human Rights (ECHR) serves to safeguard and develop the rules instituted by the Convention, which guides "the mission of the system set up by the Convention is thus to determine, in the general interest, issues of public policy, thereby raising the standards of protection of human rights and extending human rights jurisprudence throughout the community of the Convention States [3]." The GDPR was adopted with the fundamental aim of enhancing transparency and boating confidence among individuals within the digital economy. As emphasized by Commissioner Jourova in her address during a GDPR conference, the essence of data protection is intrinsically linked to trust: 'Data protection is directly linked to trust. When individuals are afraid that others will not respect their privacy or fail to guarantee the security of their data, they lose confidence and become reluctant to share that data. Trust is thus a key resource of the digital economy.' [4] This statement underscores the critical relationship between robust data protection measures and the willingness of individuals to participate in digital interactions, which are the backbone of the modern economy.

Implementing such a sweeping regulation across diverse legal systems within the EU presented significant challenges. To facilitate compliance and enforcement across all member states, the GDPR incorporated 'open clauses.' These clauses provide the necessary flexibility, allowing member states to interpret and integrate GDPR mandates with their national legal frameworks, which vary widely across the Union. While these open clauses were essential for the adoption of the GDPR across the EU, they also introduced a level of variability. This variability can lead to discrepancies among national provisions, resulting in interpretations and

implementations that may either align closely with, or diverge significantly from, the original intentions of the GDPR.

The strategic use of open clauses are pivotal in accommodating the diverse legal, cultural, and regulatory landscapes across Europe. Open clauses allow member states to adapt the overarching principles of the GDPR to suit local contexts, enhancing the regulations's applicability and effectiveness. However, this flexibility also poses a challenge, as it can lead to a fragmented approach to data protection, potentially undermining the uniformity that the GDPR aims to establish. These variations require continuous dialogue and coordination among national data protection authorities to ensure that the core objectives of the GDPR – upholding the rights of individuals and fostering trust in the digital ecosystem – are achieved consistently across the EU.

In this light, the ongoing evaluation adjustments of these open clauses are crucial. They must be carefully balanced to maintain the integrity of the GDPR's protective measures while allowing for regional adaptations. This balance is essential for the GDPR to function not just as a regulatory framework, but as a dynamic system that supports an ever-evolving digital economy and effectively protects personal data.

In January of 2012, the EC initiated a pivotal shift in the landscape of digital protection by proposing a comprehensive reform aimed at overhauling online privacy rights and enhancing Europe's digital economy. This proposal was designed to replace the outdated Data Protection Directive (DPD 95/46/EC), which had been in place since 1995, with a much more robust framework capable of addressing the challenges posed by the rapidly evolving digital environment. The genesis of the GDPR involved extensive consultations and a participatory approach where feedback was solicited from a diverse array of stakeholders. Businesses, legal

experts, civil society groups and privacy advocates were all involved in a series of rigorous discussions and proposal evaluations to ensure that the emerging regulation would offer comprehensive protections for individuals' data.

On March 7th 2012, this iterative process was further enriched by the European Data Protection Supervisor (EDPS), who issued a critical opinion on the EC's data protection reform package. [5] The opinion emphasized the principle of accountability, a cornerstone of the proposed regulation, which mandated that data processors and their associated third parties demonstrate compliance with established data protection principles through concrete measures. This includes maintaining detailed documentation of their data processing methods, which would not only align with their legal obligations but also provide a transparent account of their data handling practices. Additionally, the EDPS advocated for mandatory data protection impact assessments, compelling data processors to evaluate and improve how their systems managed and secured personal data, thus enhancing the overall integrity of data protection practices.

The role of the EDPS evolved to replace Article 29 Working Party (Art. 29 WP), which had previously addressed issues related to privacy and personal data under the DPD. This transition marked a significant step in streamlining and strengthening the oversight and advisory capacities in European data protection regulations. The EDPS's guidance continued to play a vital role in the transitional period leading up to the implementation of the GDPR on May 25, 2019. [6]

The preparatory work, characterized by collaborative efforts and the incorporation of multiple people's input, underscored the EU's commitment to crafting a data protection framework that was not only comprehensive, but also adaptive to the nuances of the digital age. This proactive and forward-thinking approach taken with the GDPR's development reflects an

understanding that data protection isn't just a legal requirement but a critical component of consumer confidence and business innovation in the 21st century. By focusing on the protection of personal data, the EU not only protects its citizens but also champions a global standard for privacy, thus encouraging other countries to elevate the protection of the data protection of their citizens in today's online ecosystem.

The implementation of the GDPR marks a pivotal step in fortifying the fundamental rights essential in our increasingly digital society. Through its rigorous standards, the GDPR introduces several critical protections – each designed to empower the individuals and ensure a higher level of personal data security. The 'Right to Erasure' offers citizens the power to have their data deleted without undue delay, addressing concerns about lingering personal information in databases. Similarly the 'Right to Data Portability' allows individuals to retrieve their data in a standardized format, and promotes autonomy over their personal information. The 'Right to Rectification' ensures that inaccuracies in personal data can be swiftly corrected, reflecting the dynamic nature of personal information. Additionally, the 'Right of Access' provides individuals with the ability to verify the processing of their data, fostering transparency and trust. [7]

Under the GDPR (EU, 2016/679), personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, can also constitute personal data. [8] The EU's GDPR protects personal data regardless of the technology used for processing that data. It is neutral and applies to both automated and manual processing of data, provided that the data is organized in accordance with a pre-defined criteria. It also does not matter how this data is stored, in all cases, personal data is subjected to the protection requirements that are laid out in the GDPR. [9]

The EU's Data Protection laws have been regarded for a long time as the gold standard across the world. [10] For this gold standard to remain, the laws regarding data protection have to be constantly evolving to incorporate new advancements. In order for this to remain, the assistance of "open clauses" in the GDPR were used to allow for member states to adapt and adhere to the new standard. As the predecessor to the Data Protection Directive (Directive 95/46/EC) (DPD), the GDPR established as a regulation[1] unlike the DPD which operated as a directive[2]. The key differences between a regulation and a directive being, is that a regulation is a binding legislative act that applies across the EU & a directive is a legislative act that sets a goal for the EU to achieve.

While the GDPR is certainly not a new and entertaining topic for many, there have been multiple research studies based around it and the impact it has had on the EU as a whole, to help identify whether it has contributed to member states' economic factors, policy decisions, impacted health regulations, and even cybersecurity measures. However, there is very little research about how the GDPR affects the way countries organize and design their national provisions in order to encompass the values that the GDPR has to offer. Most papers that discuss the GDPR focus on the overall regulatory measures that the GDPR implements, which may include how each nation interprets it and how these regulatory measures affect each specific field. As a regulatory body, interpretation of these provisions is necessary in order for them to operate under the legal system of each country, meaning they're actively changing and being readvised depending on court cases that come about. I will focus on these regulatory differences and how cases help to create an ever changing system that allows for these national provisions to be changing.

1

2

The GDPR, while it is an EU regulation, has a far reach as it also affects foreign companies wishing to do business within the EU. For example, if a U.S. based company wishes to do business within the EU, they must first determine if any part of their business is in the EU. This includes data processing, which pertains to goods and services rendered or the monitoring of online behavior. After that, it will need to determine if their current operations comply with the GDPR. The conditions for processing can be quite difficult to adhere to as well. As stated in Article 7 of the GDPR, the requirements for processors to clearly demonstrate that the data subject has given their consent, the request for consent needs to be clear and understandable while also being distinct from other matters, along with provisions for data subjects to withdraw their consent at any time, and proof that the data is conditional. [11].

As background to how we came to the GDPR, a significant ruling was the Data Protection Directive (95/46/EC) which the European Union adopted in 1995 during the infancy of the internet. [12] The Data Protection Directive (DPD) was composed of seven main categories stemming from the intention to protect individuals with a regard to the processing of personal data and the free movement of such data. [13] As the DPD was in use, the European Parliament (EP) recognized a few flaws as it was operating as a directive and not as a regulation. As a directive, the DPD operated as a legislative act that had a set goal that the EU countries must achieve, however, it was left up to the individual member states to devise their own laws and how they would go about implementing them. [14] The European Commision (EC) recognized that data flows were being hindered by the various data privacy laws throughout member states, which defeated the intention the EU had of removing barriers when adopting EU wide policies. This pushed the EU to adopt The Organisation for Economic Co-Operation and Development (OECD) guidelines into the DPD in order to create a binding set of compliance

across the EU. [15] The DPD was the standard across the EU until June 2011 when the European Data Protection Supervisor (EDPS) published an opinion on the EC's communication proposal, which included a solution of data formation by underscoring how important it is to listen to the EC's push for adapting to the new technological and societal changes while also reinforcing individual rights. After two glaring flaws in the DPD were highlighted over its lifetime. First, the inability to keep up with current technological advancements; mainly because it was designed in an era before the widespread use of the internet and other digital technologies. Secondly, with the rapid growth of online services, social media, and cloud computing, came a strong need to reform the DPD into a flexible set of regulations that would be able to adapt and evolve as our technological advances further developed the data industry. [16]

In January of 2012, the EC proposed a reform of online privacy rights and digital economy to replace the DPD (95/46/EC) and boost Europe's digital economy. [17] The creation of the GDPR went through many discussions, proposals, and feedback from various stakeholders, including businesses, legal experts, and civil society, to ensure it would be robust enough to protect Individuals' data in the digital age. On March 7, 2012, the EDPS adopted an opinion on the EC's data protection reform package. This opinion piece focused mainly on the accountability principle, meaning that data processors or any third parties that worked with them in the processing of data, be required to show that they are in compliance with standard data protection principles. As an example, this could include the documentation of the current processing methods that data processors have adopted in relation to the obligations that they would now be held to. In some cases, processors would be compelled to conduct a data protection impact assessment, to better understand how well their systems were handling and safeguarding data. Following this, the EDPS replaced Article 29 Working Party (Art.29 WP)

which was established by the DPD to deal with issues relating to protection of privacy and personal data until May 25, 2018 when the EU's newly formed GDPR went into effect. [18]

In March 2014, the European Parliament (EP) adopted the GDPR with a strong support by voting plenary 621 votes in favor, 10 against, and 22 abstentions. [19] The overarching goal for the GDPR was to essentially be a single repository for multinational data protection matters. When established in member states or where individuals in other member states could be affected, the supervisory authority in the member state where said organization is headquartered will be deemed the lead authority, and ultimately responsible for adopting measures directed at the organization, in cooperation with all involved authorities. The EP broke down the GDPR into four 'Pillars' or building blocks, of which the regulation is formed. Pillar one, has a focus on "One Continent; One Law", which would provide regulations for both the public and private sectors, creating a coherent legal framework that can be built upon and enhanced over time. [20] Pillar two, revolves around enforcement for Non-European countries, and how it levels the playing field for all in the European digital industry. The reasoning for this pillar is relatively simple; if foreign companies would offer services or goods to EU consumers, they should have to adhere to the same levels of protection of personal data and play by the same rules. [21] Pillar three, is built around the Right to be Forgotten / Right to Erasure. This right already builds on existing regulations to better protect data subjects from risks online. With a focus on empowering EU citizens, specifically teenagers, to take control of their online identities. In the instance where an individual wants their data to no longer be processed or stored by the controlling organization, and if there is no legitimate reason for keeping said data, the data should be erased from systems. [22] The final pillar, Pillar four, focuses on the creation of a "one-stop-shop" for EU citizens and businesses. Pillar four centers around simplification and making it easier for established

companies that are in several member states to only have to deal with a single DPA, where they're headquartered. This not only makes it easier for businesses as well as citizens, who with the passage of the GDPR now only have to deal with the DPA in their member state, and not have to use another language in order to file complaints. [23] Later in December 2015, the EP Council and EC reached an agreement on the GDPR which the WP followed up with a planned course of action for the implementation of the GDPR. While the GDPR was to replace the outdated DPD, the EP did include some of the rules from the DPD into the GDPR. According to the GDPR, the purpose is as follows:

> (3) Directive 95/46/EC of the European Parliament and of the Council seeks to harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between member states.

The GDPR was adopted to inspire transparency and confidence among individuals of the EU, as Commissioner Jourova stated during her GDPR conference speech "Data protection is directly linked to trust. When individuals are afraid that others will not respect their privacy or fail to guarantee the security of their data, they lose confidence and become reluctant to share that data. Trust is thus a key resource of the digital economy."

The effectiveness of these rights provided by the GDPR remain an area ripe for exploration. Questions persist regarding the adequacy of the mechanisms in place to enforce these rights and the real-world impact on individuals' control over their personal data. Are these rights sufficiently robust to cope with the rapid advancements in technology and data usage?

How do different socio-cultural contexts within the EU influence the interpretation and application of these rights?

However, as for the GDPR to be enforceable across all member states, the assistance of "open clauses" are required to allow member states to openly interpret their own national provisions to adhere to the GDPR's strict standards. These open clauses contributed to the discrepancies among national provisions which we can view as either convergent or divergent from the initial GDPR regulations. It is however, important to note that the allowances of the open clauses, allow member states to more finely tune the broader privacy framework of the GDPR to their specific laws and cultures.

The GDPR consists of a total of 70 different provisions that allow for both regulated mandates and options for customization at the national level. As background, the EU has a legislative hierarchy, which a regulation is a binding legislative act which must be uniformly applied to all member states. A directive on the other hand, is a legislative act that sets goals that member states must achieve, but gives each member state the freedom to decide on if the goals should then be written into their own national laws. Even though the GDPR is a mandatory regulation, it provides flexibility for each member state to retain and reinforce their already existing national regulations in specific ways. These alterations are permitted, as long as they do not interfere with the European Single Market, examples of provisions to not be altered include tax laws, social security, press laws, and labor laws. The flexibility provided within the GDPR is attributed to the open clauses section of the GDPR, which enables a member state to further refine and adapt the generalized outlines of the GDPR to create a more tailored set of laws and procedures that are more relevant to their nation. The scope and application of each clause is at the discretion of the individual member states, and are usually detailed within the clause itself.

Interpretation and application of each clause, however, must always align with the overarching principles and objectives of the GDPR. This system of open clauses helps to ensure that while the GDPR sets a uniform standard for data protection across the EU, it also respects and allows for accommodations of each member state's unique legal and regulatory landscapes. The GDPR works towards a convergent approach to data protection, which can be fine-tuned to address specific national cases, without undermining the integrity of the EU's Single Market.

IV. Literature Review

The GDPR, which was implemented in 2018, represents a significant milestone in data protection within the EU. This regulation has been extensively studied across various disciplines, resulting in a wide array of literature from differing viewpoints. This review will touch on several sources, picking out key points from each academic article and how they add to our understanding of the GDPR's legal framework, impact, and practical applications.

In the commentary, "The EU General Data Protection Regulation (GDPR): A Commentary", by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Dreschler provide an in-depth analysis of each article of the GDPR, exploring the context and significance for each. [24] The best summation of the GDPR I have found so far is from this commentary and is what I've based my understanding of the implementation process off of:

> The story of the GDPR's birth is long, intricate and often difficult to follow. At the same time, it is both fascinating and instructive, not just in terms of showing how data protection has developed within the EU but also in terms of the insights it provides on the mechanics of the EU legislative process more generally. It demonstrates the complexities of that process, as well as the growing significance of data protection in economic, social and political terms and the strengthening of the fundamental right to data protection in the EU legal order. The GDPR's route through the EU legislative procedure and the way its text evolved further illustrates its major concepts and the changes that it made to EU data protection law.

Furthermore, the commentary provides insight regarding the modernization process of the DPD (95/46/EC), and how the CJEU failed its main objective of harmonizing member states' data protection laws through the use of the DPD. On March 7th 2007, the Commission concluded that they would not revise the DPD. Throughout the remainder of the introduction part of the commentary it goes into further detail of the legislative background of the GDPR and its implementation and drafting process.

Another important aspect to the GDPR is the economic impact it has had on the EU. In the essay "Consumer Law and Economics", by Klaus Mathis and Avishalom Tor, they detail the extent to which companies like Facebook or Google have access to personal data about you. [25] This includes information such as photos, search history, videos watched, any messages ever sent, login location, the type of device, contacts saved in a user's phone, etc. Further, the authors also go into detail of various data breaches that affect millions of users, as shown here:

> Consider the following examples. Uber's data was breached in 2016, affecting 50 million riders and 7 million drivers, as well as disclosing some 600,000 U.S. driver license numbers. In September 2018, the company reached a settlement, agreeing to pay $148 million that was distributed among the U.S. states. In the same month, Google confirmed that "Hundreds of apps are able to scan and share data from the email inboxes of Gmail accounts". Perhaps most conspicuously, a huge public protest erupted earlier that year as a response to the Facebook-Cambridge Analytica data scandal, where the data of millions of people's Facebook profiles was harvested. Thereafter, Facebook's CEO Mark Zuckerberg testified about the firm's privacy practices before two Senate committees.

As shown, the data industry has access to large amounts of user data without much oversight outside of the EU. As we've seen, the EU has had a long standing history with a focus on citizens' rights, of which it considers privacy as a human right and it is focused on providing data protection rights. The authors go on to state how the GDPR seeks to level the playing field to give data subjects control of their personal data, as stipulated by the EU. This in turn affects companies and requires more transparency around data collection and how that data is processed.

In "Deficient by Design? The Transnational Enforcement of the GDPR", the article looks at the implementation status of the GDPR after four years, and raises significant questions in relation to the GDPR's enforceability especially in transnational situations. [26] The authors, Giulia Gentile and Orla Lynskey, go on to identify the systemic flaws in the GDPR's procedures, going so far as to suggest that they may be "deficient by design", as the title states. The first flaw that the article points to is the composite administrative procedures provided by the GDPR, which lead to ambiguities and divergences in oversight and enforcement processes. This also shows an important balance between the independence of national administration and the uniform enforcement of the GDPR across the EU. The second failure that was found was the GDPR's failure to recognize the equality of national supervisory authorities (NSAs), by placing higher importance to the "lead supervisory authority" over other NSAs. The third flaw found was that the GDPR presents a host of weaknesses from a fairness viewpoint, which translate to interference in the right such as the right to erasure or right to accessibility of data subjects. The fourth flaw found by the authors occurs in the national approaches towards the enforcement of the GDPR is not applied equally across the EU, thus enabling potential breaches of the core tenet of the regulation. Furthermore the authors argue that these flaws contribute to an

under-enforcement of the GDPR's goal to enhance the data subject's fundamental rights to data protection.

The solutions suggested for fixing these flaws are quite simple, as many of the identified flaws are able to be rectified using the existing framework of the GDPR, encouraging cooperation among NSAs and the European Data Protection Board to act strongly with the general principles of EU law. In the event where such encouragement fails, it will then fall to the Commission to apply enforcement action, or have the CJEU intervene if needed.

A key focus of the GDPR is data protection, and one of the more important types of data that requires extensive security and handling measures is healthcare data. In the article "Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden", the authors state that healthcare and health-related data sectors can both be characterized by a convergence in infrastructure across the EU. [27] Of which, the intended goal for this convergence is the planned creation of a European Health Data Space (EHDS), which would create an EU-wide platform for the processing of data for healthcare and scientific research purposes. The problem that is posed by the article is the planned infrastructure is not yet detailed in relation to current data protection laws. Drawing major concern in this area, is the divergences we see in member states' implementations of the GDPR that affect data sharing between healthcare and science institutes, as the use of the open clauses provision of the GDPR could introduce potential issues for said institutes when the sharing of data is required. The article scrutinizes four member states' data sharing laws in the context of the GDPR, in relation to six-health related fields regarding data sharing across the healthcare and research sectors and between the main actors of said sectors. One of the member states that they had

targeted for research was Germany, and had coincided with my own research. The article calls out the main rule of the BDSG as it applies to health-related data processing by non-public organizations, for example; a privately owned hospital. The issue being that the BDSG is secondary to state hospital laws, which are designated as *leges specialis* and take precedence over the BDSG's data protection laws in the case of publicly owned hospitals. Provisions on patient rights are also scattered across various state laws and must be applied according to their relation to their relation *lex specialis* or *lex generalis.* One such law is the Genetic Diagnostics Act (GDA) as it defines genetic data processing for diagnostic purposes but the processing of said data for research lies outside the scope of the GDA, and general rules that are not defined by the BDSG or GDA are applied instead. [28]

For health-related data to be processed in Germany, the rules set forth by Articles 9(2)(h) and Article 6(1)(b) of the GDPR are to be followed, using the treatment contract as the legal basis for data processing.. [29] [30] In addition, there is no provision in state or federal law that specifically excludes the waiving of the processing ban for the sensitive data cited in Article 9(1) by the GDPR, in order for Article 9(2)(a) to be applied directly to the processing procedure. [31] This oversight is coupled with the sector specific requirements for genetic processing using the basis of Article 9(4) of the GDPR, which mandate the informed written consent of the data subject as stated by Section 8 of the GDA. [32] [33] As I have covered the opening clauses are widely used across the EU, and have potential for enhancing national data protection as a whole. This often comes at the detriment of the overall goal of the GDPR, and the article agrees; stating:

> The GDPR opening clauses are widely used, and the comparative insight shows clear lack of uniformity for health and genetic data sharing among different actors for purposes of healthcare and research. All four member states have general implementations of the GDPR as well as sector-specific rules that apply to healthcare and scientific research data processing and to data sharing within and between those areas. Taken together with the directly binding parts of the GDPR, it remains cumbersome to define the applicable law in individual member states. The legal techniques of implementation are similar in that they integrate different legal areas, for example, in Germany and Latvia, civil law rules related to the doctor-patient relationship, in Greece, ethics assessments, and they take the criminal law perspective on professional secrecy into account in all four countries. Because the affected areas and the regulatory structure are individual to member states, comparison of applicable laws relevant for data protection remains an exhausting legal task and requires extensive knowledge of the national legal framework.

As we can see, the addition of the open clauses provisions, while necessary, adds additional complexity to an already complex set of regulations. With the implementation of the EHDS, to enable a more efficient exchange and direct access to health data across the EU while staying within compliance of the GDPR. Being built upon three pillars, the EHDS aims to create a unified governance system for the health data space and clear rules for data exchange, guarantee of data integrity, and the development of the digital infrastructure needed to facilitate this, while remaining within the bounds of the GDPR.

Kiersten E Todt states in her article *Data Privacy and Protection: What Businesses Should Do,* one significant challenge in data protection is encouraging businesses to adopt proactive measures, arguing that businesses often rely on outdated security methods, which fail to keep pace with current technological progress. [34] As Todt notes, businesses such as Facebook, Google, Twitter, and YouTube collect & aggregate large amounts of data at a rate that has previously been unseen. She points to recent examples of the security breaches that Target, Equifax, Marriott and Facebook have recently suffered, stating that companies that hold large amounts of user data need to have a clear focus on their cyber security practices as they have forced the U.S. government and other businesses to reevaluate their current security postures. Todt goes on to say that most organizations are unaware of the risks critical data can pose, emphasizing that not all businesses take the same disciplined approach needed for sensitive information. She states:

> 1) Companies need to be educated that, regardless of the mission of their organization (i.e., pizza parlor or public utility), some or even most of the data they hold are critical and needs to be protected. Companies have to make risk management decisions, based on their corporate mission and functions, regarding how much they invest protecting their data. A public utility, for example, will invest more in the protection and security of its data than a pizza parlor.
>
> 2) Companies must know the voluntary steps they can and should take to protect their data. All types of data are not equal. Companies need to understand the data they have and identify what is critical and what should be prioritized to ensure they are appropriately protected.

Todt further mentions that the EU has taken a large step in the right direction with the passage of the GDPR, stating that through the regulation, the EU has asserted when it comes to security and privacy, organizations need to be regulated and the threat of significant administrative fines. She further compares the differing approaches to privacy that the US and Germany have between themselves; with the US having a far more liberal approach to privacy which is a concept originating in the US Bill of Rights, than to countries such as Germany who have a far more defined approach to privacy laws. She concludes that businesses should be focusing on three primary courses of action: inventory of data, public projection of data privacy policies, and the implementation of a robust incident response team. These concepts that Todt proposes are included in the GDPR's guidelines, as it is the main focus of pillar two of the GDPR is to have a uniform adherence to the same levels of protection of personal data and play by the same rules, whether the organization be local to the EU or international.

In Peter H. Chase's prepared remarks to the Committee on Banking, Housing, and Urban Affairs of the United States Senate, also found in "Perspectives on the General Data Protection Regulation Of the European Union", he remarks on the expansiveness of the GDPR's scope which affects the global economy. [35] Chase goes on to argue the EU's need to prevent member states from having differing regulations that could potentially obstruct integration between states. Further, he says that Europeans have argued for a universal approach to data protection being a more effective method of security than a fragmented one, which may only cover specific institutions rather than the data that is being processed. To present a counterpoint in his argument, Chase states that the officials of the EU recognize that the GDPR may be heavy handed in places where there could be a benefit to broad data analytics. Furthermore, Chase notes that the "real" target of the GDPR is the prevention of personal data monetization. This

includes the monetization carried out by advertising agencies, and also touches on the politically-driven micro-targeting of messages to data subjects. He concludes that the GDPR would provide useful insight for U.S. lawmakers as they consider whether the U.S. should adopt a similar form of legislation, but with one caveat; the EU has had a considerable amount of time to develop their data privacy laws, and so have specifics tied to the shared history among member states. Chase finally cautions that the U.S., while not being the first to the table for data privacy laws, it might benefit more from being second as the U.S. could learn from the shortcomings of the GDPR.

Shraddha Kulhari, in their work on the book, "Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity", has a chapter relating to the "Demystification" of the GDPR, which provides thorough analysis and incorporates perspectives from various industries. [36] A key section of the work focuses on the profiling of individuals, as shown:

> Autonomic profiling is specifically targeted in the GDPR by bringing it under the umbrella of automatic personal data processing. Nevertheless, profiling is chastised in the circumstances where profiling produces 'legal effects' concerning the data subject or 'similarly significantly' affects the data subject. The limitation of the right against being profiled only in so far as it produces 'legal effects', e.g., being rejected for a loan, being re‑jected for a job after an e-recruitment procedure, etc.) and grouping the myriad possibilities arising from profiling in a loosely worded manner, highlights the shortsightedness of this provision. The effectiveness of this provision is questionable in light of the complexity associated with profiling. For instance the nature of group

> profiling is that it represents a group and reveals the applicability of attributes to the individuals constituting such a group. This in turn means that the profile is not inferred solely from the personal data of the person so profiled, rather it makes use of large amount of data relating to many other people which may or may not be anonymised. The risk that emerges from this kind of profiling is more vicious than individual profiling because 'the process results in attributing certain characteristics to an individual derived from the probability that he or she belongs to a group and not from data communicated or collected about him or her.' This strikes at the very identity of an individual and takes maintaining the sanctity of her identity beyond the realm of her personal autonomy.

She further states that the threat of profiling threatens the identity that the data subject has built for themselves, and that it would be in the interest of the data subject if the GDPR acknowledged the complexity of said profiling by addressing it and introducing a new right; the right to identity. This would then allow for automated data profiling to be confined by allowing for the data subject to exercise their right to identity if needed. Such a right, Kulhari argues, would provide a necessary mandate to implement an identity management solution to secure personal data.

Furthermore De Busser, Els, et al examine the implications of conflicting data privacy laws in"Big Data: The Conflict Between Protecting Privacy and Securing Nations". [37] They state that the potential for conflicts to arise have increased due to the mandate that the GDPR has set forth due to its nature, as it affects not only companies that process data inside of the EU but also countries that process data that relate to citizens of the EU even if those companies reside outside of EU jurisdiction. They argue that said conflicts in law create legal uncertainty and confusion for law enforcement and other intelligence agencies, whose efforts in collecting

cross-border information and intelligence could be blocked as a result. For instance, if an organization were to proceed with the collecting of information, said data would then be inadmissible as evidence for a criminal trial. De Busser states that if the prior example were to occur, and a trial took place in a country that follows the “fruit of the poisonous tree” chain of evidence, all evidence collected would be thrown out; wasting time and resources, as well as acting as a deterrent to law enforcement. Furthermore De Busser argues that it is the citizens whose personal data is at the heart of these conflicting laws and regulations, which in some cases could be problematic for an individual to submit a complaint to have it go unresolved. An example that the authors use is the lack of redress for EU citizens that were affected by the US Privacy Act of 1974, which resulted in years of negotiations between parties and the passage of the 2016 Judicial Redress Act [38] A solution to conflicting laws are the addition of ad hoc agreements, says Busser. With these agreements, resolutions can be reached by presenting a hierarchy between conflicting laws and provisions. As De Busser states:

> After the entry into force of Directive 95/46/EC, any transfer of personal data to a third country had to be preceded by an assessment of the recipient country’s level of data protection. If the level of data protection was not considered adequate, the transfer would not happen unless appropriate safeguards for processing the data were in place. Because the US level of data protection was not considered adequate and in order to maintain trade, a compromise was reached consisting of the self-certification system called the Safe Harbor agreement. After Safe Harbor’s annulment by the Court of Justice of the EU in 2015, the EU-US Privacy Shield replaced it.

Extrapolating this argument, we can further apply this to member states of the EU, and their national implementations of open clauses. While the GDPR provides a framework for member state interactions, it does not provide guidelines on how international bodies interact with member states and the EU's data protection rights. This is where the ad hoc agreements could come into use as understandings can then be established for further interactions, when a conflict in law or regulation occurs.

The GDPR has now been active for 6 years, and research is being carried out in multiple disciplines. While it covers a broad array of topics, there are several improvements that can be made. In many cases, the GDPR has become a standard for - even in countries that are not covered by the protections put in place, as companies find it easier to have a single privacy standard in place rather than risk a non-compliance infringement by the GDPR. A real world example of this is the recent implementation that we see in web browsers today, which stems from the GDPR's tough stance on data harvesting and monetization through the use of advertising. The addition of harsh fines present a deterrent for companies to neglect their security posture, as a breach in personal data of data subjects could prove to be a significant punishment totalling into the millions of euros.

As we continue to navigate the ever growing complexities of digital privacy, the GDPR serves as an important tool in the balancing of the protection for individual rights with the technological advances and economic interests of the digital age. The ongoing discussions, legal challenges, and adaptations by various member states underscore the quickly changing nature of data protection legislation. More importantly, the GDPR not only addresses past inadequacies but also provides a forward-looking approach, making sure that data protection standards evolve alongside technological progress and societal changes.

V. Methodology and Case Studies

Case Justification:

To understand how the GDPR has changed the face of data protection in the EU, I examine how member states draft, implement and enforce various aspects of the GDPR. I selected 3 case studies for my research; Germany, Austria, and Ireland. I selected Germany due to its history with the widespread data collection practices carried out by the Nazi regime, such as the collection of racial, sexual, religious, and political beliefs. After the downfall of the Nazi Party we saw a shifting of German data protection policy with the passage of the German Basic Law, that would form the basis of protection for the collection of data. My second selection for study was Austria where their data protection law, the Datenschutzgesetz (DSG) provides specific adjustments to the GDPR's requirements, focusing on areas such as public sector data processing and national security exemptions. The final selection for my research was Ireland, as unlike Germany and Austria, Ireland uses the open clauses provisions not to protect national precedent but to pursue active enforcement of the GDPR. I first began with looking into the history behind many member state's data protection laws, and how they came into being.

At the time of the GDPR going into effect, only 4 member states out of 29, Germany Belgium, Austria, and Slovakia were able to pass their national provisions in time to meet the May 25, 2018 deadline. This is due to each member state having to have their specific laws relating to GDPR implementation, ratified by the deadline. As noted in Article 9 of the GDPR, the article gives the member state the ability to decide on exceptions to the banning of the processing of specific categories of personal data, such as ethnicity, religious beliefs, health and sexual orientation.This allows member states to process such data facilitate research or to support employment law or other substantial public interest, while needing to clearly spell out any

derogations in the implementations of their regulatory laws relating to the GDPR. The first member state to lay the necessary groundwork for their own GDPR implementations. [39]

Having now identified at risk types of data that were pertinent to Germany's protection laws, I narrowed my search to specific laws and regulations regarding such information. I selected this member state as my first candidate to compare to the GDPR as a whole to see which variations to the open clauses exist within Germany's legal framework. The research into the data collection that had been carried out by the Nazi party led me to the Population Census Act which Germany passed in 1982. This law contained provisions for the collection of information such as addresses, names, telephone numbers, gender, birthdates, marital status, religious denomination, employment type, employer, and the methods of commute. The overall length of said census totaled more than 150 questions. Information gathered was not to be used solely for statistical purposes, but also to be used for updating local registries. [40] The Population Census Act was met with a large amount of resistance due to Germany's past history with data collection, eventually reaching the German Constitutional Court. This case, aptly named the "Population Census Case (1993) brought forth a set of safeguards that are still used as central tenets to current day data protection laws. During the proceedings more of the questions asked by the consensus to be within the bounds of the constitution, provided the adherence to the following safeguards: strict prohibition of the transfer of data from the national to local governments for the purpose of updating the local registries and the restriction of the collection's scope. It also had to include the right of informational self-determination [41], in Art. 1 paragraph 1, and Art. 1 paragraph 2, the Basic Law states the right of human dignity and the right of personal liberty respectively. [42] As stated in the text, it is from these two principles where the individual is able to freely develop one's personality, and have the ability to

voluntarily disclose information about themselves. The Population Census Case reaffirmed that in order for individuals to develop their personalities, individuals require protections against unlimited collection, storage, use and disclosure of their personal information. Additionally, the court ruled that the individual's protections have limits, which could be overruled in the interest of public safety. Public interest must be statutory, as the legislative body has observed the principles of proportionality, clarity, and the implementation of organization and procedural safeguards to protect the integrity of the individual's information. [43] The Population Census Case was a foundational case for Germany's Bundesdatenschutzgesetz (BDSG) and would be updated to the BDSG-New to better comply with the GDPR in 2018. The transition to GDPR compliance was not insignificant, as throughout Germany's legal landscape, each German state has their own individual interpretations of data protection, which have since then evolved over time from the late 1970's to now. The most notable examples being the Broadcast Media Act [44] and the Telecommunications Act. [45] These two acts were important pieces to the formation of the update of the BDSG, as there was confusion as to which of these provisions would be overridden by the GDPR, and which would remain applicable going forward. At the local and state levels, we can see that micro adjustments were made and continue to be made at the local and state levels regarding the Broadcast media Act and Telecommunications Act. With how early German Data Protection laws contributed to the complex legal landscape, the former precedent set forth by the German Basic Law in 1949, these early German data protection laws will likely continue to influence future protection laws in Germany.

The BDSG can be broken down into four main parts, with Part 1 being comprised of provisions that are applicable to both the GDPR and Directive (EU) 2016/680 in conjunction with the processing of personal data that is beyond the scope of Sections 1 and 21 of the BDSG.

[46] Part 1 consists of 6 chapters; scopes and definitions, legal basis for processing personal data, data protection officers of public bodies, Federal Commissioner for Data Protection and Freedom of Information (BfDI), representation on the EDPB, single contact points, cooperation among federal supervisory authorities and those of the state concerning EU matters, and legal remedies. Part 2 of the BDSG is focused on the implementation of provisions for processing purposes in adherence to Art. 2 of the GDPR. Similarly to Part 1, the structure of Part 2 is composed of 6 chapters: legal subject, obligations of controllers and processors, supervisory authorities for data processing by private bodies, penalties, and legal remedies. Part 3 implements provisions for processing purposes in accordance with Art. 1 (1) of the Directive (EU) 2016/680. [47] Consisting of 7 chapters, Part 3 deals with: scope, definitions and general principles for processing personal data, legal basis for processing personal data, rights of the data subject, obligations of controllers, and processors, transfer of data to third countries and to international organizations, cooperation among supervisory authorities, and liabilities and penalties. Comparative to the previous three sections, Part 4 is very minimal in regards to regulations. Made up of only a single section, Section 85 is concerned with the processing of personal data in the context of activities outside the scope of the GDPR and Directive (EU) 2016/680.

Where Germany has some of the strictest data protection laws, Austria and Ireland exhibit distinct variation. Austria, while slightly similar to Germany, in culture and history; legal pretexts are where we start to see deviations from their neighbor. Where Germany focuses more on specific rules and regulations for data protection officers, employee data processing, and extended rights of data subjects. A case I will look at later is DSB-D213.1508, which relates to the usage of video cameras in a middle school, where the school had installed cameras in various

corridors. The purpose of these cameras was to enhance security by monitoring activities to prevent theft or damage.

Finally, Ireland represents a case that, unlike Germany and Austria, used the open clause provision not to protect national precedent but to pursue active enforcement of the GDPR. As a major hub for a vast amount of corporations, Ireland for instance, is responsible for imposing record €1.2 billion euros in penalties and fines. [48] Although Ireland is responsible for the vast majority of penalties and sanctions to major corporations, the Data Protection Act (2018) (DPA) does not differ greatly from the GDPR's original mandate, compared to Germany or Austria. The Act itself establishes the Data Protection Commission (DPC) as a supervisory authority responsible for monitoring the application and enforcement of data protection laws in Ireland. This body plays a crucial role in safeguarding personal data, ensuring that data processing practices comply with the law, and enhancing the rights of individuals by giving them greater control over their personal data. The DPA is heavy on the enforcement side with provisions for administrative fines and penalties for non-compliance, ensuring that data protection framework not only supports the rights of individuals, but also holds violators accountable, thereby fostering a culture of compliance and security.

As we navigate the growing complexities of digital privacy, the GDPR stands as a pivotal framework, balancing individual rights with the technological and economic interests of the digital age. The ongoing debates, legal challenges, and adjustments by member states highlight the fluid nature of data protection laws. The GDPR addresses past shortcomings while providing a forward-looking framework that ensures data protection standards keep pace with technological and societal developments. However, my investigation focuses on whether national provisions are influenced by the member states' use of the GDPR's open clauses, and how this

choice impacts the rigidity or flexibility of their implementations. In this paper I will be discussing the differences and similarities between various member states utilizations of the open clauses provided by the GDPR. I will study various legal cases that have affected each regional legal landscape of Germany, Austria, and Ireland.

For my research, I took an aggregation of various cases and national laws throughout the chosen EU member states.With a strong foundation for analyzing the harmonization or divergences in data security practices and the interactions between various member states with different cultural backgrounds. Examining historical context and specific data protection laws of Germany, Austria, and Ireland, provided a well rounded understanding how different countries interpret and have implemented the GDPR at the national level. Using this approach helped to further answer the research questions posed at the beginning of this thesis.

Several cases, most notably originating in Ireland, present themselves as examples of how member states have implemented the GDPR's regulatory guidelines relating to active enforcement into their national laws. While this may not be initially relevant to my first question, this detail plays a crucial role in answering my other two questions that I posed at the start of my paper. While Ireland is more focused on being a trade hub for the EU, the country is also focused on being one of the stricter countries for means of enforcement, as seen in the WhatsApp case IN-18-5-6. In addition, Austria stands as an example of the protections provided to minors' data privacy, as shown in the case DSB 2022-0.858.901.

The aim for the selected cases is to provide a broad array of topics that are covered by the GDPR, from the protection of employee records, to corporate negligence relating to security practices & transparency. With these case studies, I have struck a balance to what is possible for the implementations of the GDPR to accomplish, given enough forethought and care.

German Cases:

Germany's Federal Data Protection Act (BDSG) is the core of their data protection legislation, which is designed to protect the privacy of individuals with regard to the processing of personal data. Enacted initially to align with the EU's GDPR, the BDSG addresses areas specific to Germany that are outside the scope of the GDPR or where a member state is permitted to enact national provisions. The BDSG stipulates comprehensive guidelines on the processing of personal data both by public and private sectors. For public bodies, the BDSG outlines that data processing is permissible when it is necessary for the performance of their public functions or when other laws do not provide specific guidelines. For private entities, the law applies mainly to automated data processing, or non-automated processing that forms part of a filing system. The BDSG emphasizes the balance between the need to process personal data for legitimate purposes, and for the protection of the individual's privacy rights, thus ensuring a high standard of data protection and enhancing trust in data processing activities. [49] The following cases center around rulings relating to the GDPR within the context of the BDSG's subset of rules.

Case I: VGH München - 6 ZB 23.530 [50]

This first case examines the legal intricacies involved in the removal and destruction of documents from a personnel file of a former federal police officer. The case centers on the rights of a civil servant to have specific documents removed from their personnel file and the corresponding obligations of the employer under several legal standards, including the BBG (Federal Civil Service Act) [51], the GDPR, and the VwGO (Administrative Court Procedure

Act). [52] This case also highlights the balance that is needed between data accuracy, completeness, and the rights of an individual to protect their reputation and privacy of their data.

The plaintiff, who was a federal police officer, sought to have several documents removed from his personnel file, specifically those that related to his health and past disciplinary actions taken against him. On the other hand, the defendant, representing the Federal Police, argued against the deletion of several statements that were in the personnel file related to the officer's reinstatement review. Afterwards, the court found no that there was no substantive legal protection interest for the plaintiff's request, as the documents in question were no longer in his personnel file. It was then also ruled that the plaintiff's claim, under BGB Section 112, was unfounded on the basis that the documents in the plaintiff's personnel file did not contain accusations of misconduct, but were related to his health assessments and fitness for duty. [53] They also emphasized the importance of maintaining a complete and accurate personnel file for potential future reinstatement.

Later, both the defendant and plaintiff filed for an appeal of the court's initial decision. The plaintiff argued for further deletion on the grounds of data minimization and accuracy under the GDPR, and the defendant argued that the order for deletion of a specific statement from the plaintiff's procedural file, was factual and relevant. The decision that was handed down by the court was upheld by the appeals court after reviewing both applications, and found that the majority of the documents the plaintiff wanted to be deleted did not meet the criteria for deletion under the laws previously cited in the first ruling. The court reiterated the personnel file should provide an objective and complete record of a civil servant's career. Also included were health-related documents, which although potentially unfavorable, are important for assessing future reinstatement. Important to my study was the court's application of the GDPR's data

retention principles. The court ruled that data collected during the employment of a civil servant should remain and are necessary even after the eventual termination of employment. It also stated that the deletion of said data could potentially contravene the principle of data accuracy, as historical context is essential for a true representation of employment. Another major piece of this case involved the court's ruling on defamatory content in statements made by the plaintiff's former supervisor. The court found that these statements were both inaccurate and insulting, resulting in their removal under BGB Section 1004. [54]

Overall, this case shows how the complex nature between multiple legal texts relating to personnel files in the federal government of Germany. It also shows the need to maintain accurate records, while ensuring the rights to and individuals privacy and protection from defamation are upheld. The court's decision to reject both the plaintiff's and defendant's appeals demonstrate the importance of these principles in data protection and management against document removal and destruction as stated in the GDPR.

Case II: LG Magdeburg - DE 9-O-1571-20 [55]

The second case that I researched serves as an example of the balance between data protection laws and credit reporting practices is needed. This dispute centered around the incorrect application of a debt with a credit agency, which then led to significant financial and personal issues for the plaintiff. The highlights of this case show the implications of the GDPR in relation to false credit entries and the legal responsibilities that are required of data controllers.

On December 1, 2019, the defendant had registered an old debt with Sch. H. AG, a credit agency, despite the debt having been settled in 2013. This incorrect entry had significant repercussions for the plaintiff, including the denial of financing to purchase a property and the inability to secure a more favorable contract for an energy supplier. The plaintiff argued that these denials resulted in a financial loss of more than €40,000, and argued to be compensated for non-material damages, initially requesting €10,000 as compensation. The crux of this lawsuit centers around the GDPR, specifically Article 82 [56], which provides compensation for damages resulting from violations of data protection regulations. The regulation states that any person who has suffered material or non-material damages due to a breach is entitled to receive compensation from the data controller or processor responsible for said breach.

The court had found that the defendant violated the GDPR by illegally registering a new debt with his credit agency. This registration lacked the lawful basis needed under Article 6(1) [57] of the GDPR, and that the incorrect data entry resulted in a transfer of personal data without a legitimate request by the plaintiff, which was then breaching the data accuracy and the lawfulness of said processing. Ultimately the court partially dismissed the plaintiff's claim for €10,000, as the court found insufficient evidence to justify the higher amount based on the damages presented. They did however, award the plaintiff €4,000 in compensation for non-material damages, acknowledging the personal harm and stress the wrongful data entry caused, and deemed that this amount was much more appropriate given the severity and duration of the violation.

The case shows us the vital role of the GDPR in protecting individuals from the adverse effects of incorrect data processing and reporting, and serves as a reminder to data controllers their responsibilities to maintain accurate records to ensure that data processing complies with

current legal standards. By examining this case, I was able to gain further insight into the practical application of the GDPR and the court system's approach to addressing such violations, providing me with a valuable reference for further case examination.

Case III: BAG - 9 AZR 383/19 [58]

In the Federal Labor Court case 9 AZR 383/19, a significant legal issue was addressed regarding the compatibility of two different roles within a single company. The employee in question was the chairman of the works council, who had also served as the DPO. This case shows the potential conflict of interest that might happen if an employee were holding these two positions at the same time, while also providing key insight into the application of data protection laws in an organizational setting.

The plaintiff, who had been an employee of a company belonging to the X group since 1993, had served as the chairman of the works council. On June 16, 2015, he was additionally appointed as the company's DPO, a role which is responsible for ensuring compliance with data protection laws, including the GDPR and the BDSG. In 2017, the Thuringian state commissioner for data protection had raised concerns about the plaintiff's dual roles, suggesting the overlap could potentially result in a conflict of interest for the X group. Following this, the company revoked the plaintiff's appointment as DPO on December 1, 2017, and again on May 25, 2018, citing the incompatibility between the two roles.

From this case, there were two key provisions that were important to this case was Article 38 of the GDPR, which emphasized the independence of the DPO and prohibits holding another role that could potentially result in a conflict of interest. [59] The second provision important to the case is Section 6 of the BDSG, which outlined the requirements and grounds for the appointment and dismissal of a DPO, citing the need for reliability and absence of conflicts of interest. [60]

Initially, the Dresden Labor Court and the Saxon State Labor court had both ruled in favor of the plaintiff, maintaining their stance that this dual position was valid. However, it wasn't until later that the Federal Labor Court overturned these decisions, citing that the dual roles of works council chairman and DPO inherently conflicted, compromising the plaintiff's ability to perform the duties of the DPO independently and without bias.

The rulings from this case highlight the importance of maintaining a separation of roles to exist between a DPO and any position involved in the decision making process, in order to avoid conflicts of interest from occurring. The Federal Court's decision made clear that these types of roles are incompatible due to the potential conflicts of interest and serves to illustrate the practical implications of the GDPR for organizational roles and the necessity for companies to more closely adhere to data protection laws. By requiring the DPO's independence from other roles, organizations/companies can then better comply with data protection regulations set forth by the GDPR.

Austrian Cases:

The Austrian Data Protection laws are very similar to Germany's, in that they both serve to implement and complement the European Union's GDPR, ensuring that data protection standards align across member states, while allowing some room for national specifics. Both Germany and Austria place a high degree of focus on the scope and application of their respective laws, along with establishing independent data protection authorities responsible for monitoring and enforcing data protection standards within their respective countries. Where they start to diverge however, is in the detail and scope that reflect the specific legal, cultural, and administrative contexts of Austria and Germany. These nuances are important for entities operating in both jurisdictions to be aware of and to understand and comply with them. [61]

Case IV: C-498/16 [62]

The case of Schrems v. Facebook Ireland (C-498/16) is a landmark legal case that highlights the complexities of differing jurisdictions and consumer rights within the EU. Initiated by Maximilian Schrems, an Austrian privacy activist, the case addresses significant questions about the scope of consumer protections and the ability to consolidate claims across borders. Schrems, who was a long-time user of Facebook, and had been actively involved in challenging many of Facebook's data protection practices. Initially he had used the platform for personal purposes, which Schrems later engaged in other professional activities related to his advocacy, which included publishing books, giving lectures, and fundraising. He also organized legal actions against Facebook, receiving claim assignments from other Facebook users around the world. Schrems had filed the lawsuit against Facebook Ireland in the Regional Civil Court of Vienna, seeking injunctions and compensation for alleged data protection violations. He claimed

that this included both his personal grievances and those assigned to him by other users. While this case was decided before the GDPR's implementation, the issues addressed are deeply connected with the overall principles provisioned by the GDPR, with this case somewhat foreshadowing the eventual creation of the GDPR and data protection laws in general for the EU.

The case presents two primary legal questions to the CJEU. Firstly; Does a user lose their status as a "consumer" under EU law if they engage in activities related to their advocacy, such as publishing books and lecturing? And two; Can a consumer bring a lawsuit in their local court that includes claims assigned to them by other consumers from different jurisdictions? The CJEU's analysis focused on the interpretations of Articles 15 and 16 of Council Regulation (EC) No 44/2001, which governs the jurisdiction and the recognition and enforcement of judgements in civil and commercial matters. [63] The court reaffirmed that the concept of a "consumer" should be interpreted very strictly as "someone who acts outside their trade or professional activities". The court also ruled that Schrems's additional activities, such as publishing and lecturing, did not strip him of his consumer status regarding his personal Facebook use. Thus, he remained entitled to consumer protections, which allowed him to bring his case against Facebook Ireland forward within Austria's jurisdiction.

On January 25, 2018, the CJEU passed judgment, stating that Schrems retained his status as a consumer, despite his professional activities related to his advocacy, and that Schrems could not bring claims assigned to him by other consumers in the Austrian court. Specifically, citing Regulation No 44/2001 [64], as the only applicable regulation relating to claims brought forth by individual consumers.

The key takeaways of this case and how it relates to the GDPR are how it seemed to have influenced the drafting of specific Articles in the regulation. For example, in relation to Article

15 of the GDPR, Schrems's demands for disclosure of how his data was handled relate to the GDPR's right of access, which allows individuals the right to obtain information about data processing activities. In addition, the Schrems case sought to challenge the terms and conditions laid out by Facebook, which closely relate to the GDPR's Articles 16 and 17, which provide an individual the right to request a correction or deletion of their personal data. [65] While the CJEU ruled that Schrems could not bring forward claims that were assigned to him by other consumers in the same lawsuit, the GDPR provides avenues for non-profit organizations to lodge complaints on their behalf, in the same vein as to the collective enforcement approach that Schrems sought after. [66].

This case not only sets the precedent for several Articles of the GDPR, but it also highlights the importance of data subject rights, transparency, accountability, and very strict regulatory laws. Not only that, but this case has also contributed to steering the discussion around data privacy and protection to this day, and will probably remain as a reference point in the ongoing evolution of data protection within the EU.

Case V: G 287/2022-16, G 288/2022-14 [67]

In this case, I examined the Austrian Constitutional Court's decision regarding the constitutionality of Section 9(1) of the DSG. [68] The primary issue I found within the case revolved around "media privilege", which exempts media companies / organizations from several data protection requirements under both the DSG and the GDPR. Section 9(1) of the DSG states that several provisions shall not apply for personal data by media owners, editors, copy editors, and employees of media companies and must be used for journalistic purposes.

This includes exemptions from DSG principles, the rights of the data subject, the responsibilities of data controllers and processors, and the cooperation and coherence of provisions provided by the GDPR. Austria's Federal Administrative Court questioned the constitutionality of this section, and argued that this section of the DSG undermines the fundamental right to data protection and violated principles of equality and the right to a legal judge, if it were to be kept in the original state it was in.

The key issues being argued in this case concern the media's privilege granted by the DSG and how it effectively removed the protection afforded by data protection laws to individuals when their personal data is processed for journalistic purposes. As such, this could leave individuals without access to a DPA to address alleged violations of their data protection rights. In addition, the court argued that Section 9(1) of the DSG creates an unjustifiable distinction between media companies and other entities. The distinction was not seen to be justified and as a result, was in violation of the principle of equality under Austria's constitutional law. The exclusion of media privilege from the jurisdiction of the DPA, violates the right to a legal judge as protected under both Austrian law and the ECHR.

The court found that the broad exclusion provided by Section 9(1) of the DSG was fairly disproportionate and was then deemed that the exemption undermined the fundamental right to data protection without a sufficient balancing of interests. To be more specific, the exemption essentially prevented individuals from using their data protection rights under the DSG, along with the exclusion of the DPA's jurisdiction meant that individuals could not seek compensation for their data protection rights, which then led to unequal treatment of individuals based on whether their personal data was processed by media companies or other entities. As of the

writing of this paper, the repeal of Section 9(1) is scheduled to go into effect on June 30, 2024, allowing for a transition period to allow for legislative adjustments to data protection rights.

The Constitutional Court's decision impresses the importance of the need to balance the right to data protection, with the right to freedom of expression and freedom of information. While recognizing the need for journalistic freedom, the court stated that such freedoms should not disproportionately infringe on an individuals' right to data protection. This case is one of the many ongoing challenges in the work to protect both privacy and right to freedom of expression.

Case VI: DSB 2022-0.858.901 [69]

In another case, a decision that was made by the Austrian DPA regarding the use of video surveillance in a middle school, and serves to highlight the complexities of balancing security needs with privacy rights, particularly with the context of minors in a public education setting. The middle school in question installed four cameras to monitor various hallways and entrance areas due to prior incidents of break-ins. The recordings from these cameras were kept for a period of 48 hours, and were intended to protect people and school property. The use of these cameras, however, was viewed through the lenses of the GDPR and other national data protection laws. Specifically, the court had examined the violations of Articles 6 and 8 of the GDPR, which relate to the continuous recording of students during school hours without sufficient legal authorization, and the violation of the special protection of children's personal data respectively. [70] [71]

In the end, the school was ordered to limit the processing of images by either turning off the cameras during school hours, or ensuring that no recordings were made during school hours.

In addition, the school was then required to, after a six week period, provide evidence of compliance to the previously mentioned rulings. This decision is important because of the strict requirements that are placed on educational institutions, in which security measures such as surveillance cameras must be necessary but also proportionate, especially when involving vulnerable groups such as children. While protecting individuals and property is an important factor and should not be overlooked, this case exemplifies the importance of also complying with data protection regulations to ensure that measures taken to enhance physical security do not also infringe on the privacy rights of individuals, particularly students.

Irish Cases:

In Ireland, the focus has been more geared towards the practicality of GDPR provisions, especially in terms of international data transfers and the protection of data subjects' rights. Ireland's Data Protection Commission plays a critical role in supervising GDPR implementation, particularly given the presence of many multinational corporations' European headquarters in Ireland. The Irish approach emphasizes compliance, transparency, and accountability of data controllers and processors, aligning closely with the GDPR's objectives to enhance the privacy rights of individuals and to fortify data protection across the EU. [72]

Case VII: IN-20-7-2 [73]

This particular case involves the Bank of Ireland (BOI) being found in violation of several GDPR Articles. After further investigation by the DPC in Ireland, they found that the BOI failed to implement proper technical and organizational measures to ensure the security of customer data on its Banking365 platform. The investigation was brought about after the BOI had reported ten breaches that had involved personal data of their clients between January and May of 2020. The substance of the breaches included unauthorized access to customer accounts due to either staff / clerical errors, or flaws in the bank's networks or systems.

The DPC found that the BOI did not implement adequate security measures in order to protect their customer's data, which led to the breaches of confidentiality and integrity as referenced in Article 5(1)(f) of the GDPR. [74] In addition to the breach of Article 5(1)(f), the DPC also found that the BOI was in breach of Article 32(1) of the GDPR, which states that the data processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. [75] The DPC also found that, upon discovering the flaws, the BOI took an excessive amount of time to implement effective remediations. For instance, the CIS flaw that had been identified in 2019 was not fully resolved until 2021.

The result of this was that the DPC imposed two corrective measures on the BOI in relation to the data breaches. Firstly, the BOI was ordered to bring their processing operations into compliance with the GDPR by improving the data verification and quality assurance controls, improving the training of staff, and to also implement strong testing measures. The last part of the rulings was a €750,000 fine, that was to be proportional to the nature, seriousness and the duration of the breached of security, along with the amount of data subjects affected, and the degree of negligence exhibited. The reasoning provided by the DPC for this fine is cited in Article 83(1) of the GDPR. [76]

Due to the nature of financial institutions, and the risk involved in handling large sums of other people's money, the DPC's ruling against the BOI sets an example of the enforcement of the strong requirements listed in the GDPR. This case shows us a prime example of the need for the continuous updating of data protection practices and laws/regulations to better protect the personal information of data subjects.

Case VIII: IN-18-5-6 [77]

As I've come to find in my research, the GDPR has established stringent requirements for data privacy and protection, which significantly impact organizations that process personal data within the EU. This lawsuit exemplifies the possibilities of a strong GDPR that protects the data subjects in the EU. The initial complaint was lodged by JG, who was a user represented by the European Center for Digital Rights (NOYB) and was first handled by the Hamburg Data Protection Authority before being transferred to the German Federal Data Protection Authority, then finally to the Irish DPC. The complaint was centered around WhatsApp's updated Terms of Service (ToS) and Privacy Policy, which was introduced in April of 2018, ahead of the GDPR's enforcement date on May 25th, 2018.

The issues that were presented in the case primarily involved whether WhatsApp's requirement for users to accept the updated ToS constituted "forced consent", if they could legally process user data based on the necessity of performing a contract under Article 6(1)(b) of the GDPR, or whether they had provided sufficient transparency (Article 12(1) and Article 13(1)) for their legal basis of data processing activities. [78] [79] [80]

In order to comply with the GDPR, WhatsApp had updated its ToS, by requiring their users to accept the new terms to continue using their service. This update included an updated Privacy Policy detailing how user data would be processed by WhatsApp. Users were presented with a dialogue box, which users had to scroll through with an "Agree and Continue" button at the bottom, which JG argued left him no legitimate choice but to either accept the terms of service or quit using WhatsApp's service in its entirety. As far as the legal basis for data processing is concerned, Article 7(4) of the GDPR states that data processing must be grounded upon a legal basis, such as consent, contractual necessity, or legitimate interests. [81] It should be noted that WhatsApp then argued that its data processing was essential to fulfill its contractual obligation to their users, as stated under Article 6(1)(b) of the GDPR. JG however, contended that WhatsApp's approach equated to forced consent and lacked the transparency needed to allow for users to make an informed decision.

The DPC's investigation focused on the legitimacy of WhatsApp's reliance on the contractual need for the processing of personal data, and concluded that WhatsApp didn't seek to rely on consent, but on the necessity of performing said processing. As such, the acceptance of the ToS was not an act of consent within the bounds of the GDPR. With the investigations finished, the DPC made an order citing Article 58(2)(d) of the GDPR, which required WhatsApp to bring their processing into compliance within a six month period, starting on the following day of the court's decision. In addition to the compliance order, the DPC also imposed another penalty of €5,500,000 as a punitive action, citing Article 83 of the GDPR. [82]

This case shows how effective active enforcement can be handled as the consequences are significant. The findings of the case align with the GDPR's mandate of tough enforcement on transparency and providing legal basis for consent. While Ireland does not utilize the open

clauses to lower the administrative fines, there is potential for other member states to do so, thus introducing an additional divergence from the GDPR.

As EC Commissioner Jourova stated in her GDPR speech "This is of course not the end of the road, but a beginning of a new chapter." [83] This opens the gateway for us to understand why the purpose of "open clauses" were necessary for the adoption of the GDPR and cohesive compliance across the EU. It also will illuminate the general approach that these member states take when tackling their national provisional laws.

As demonstrated, Germany and Austria exemplify countries that have the GDPR's framework to meet their specific needs, demonstrating the flexibility and adaptability of the GDPR. The added flexibility provided by the available open clauses works to ensure that each member state is able to apply the GDPR to their country in a relevant way, with the benefits being available to their citizenry. In contrast, Ireland's implementation of the GDPR emphasizes strict enforcement and robust protection of individual rights, showcasing the regulation's broad scope and its focus on increasing accountability and transparency among data controllers and processors.

VI. Findings

The study of the case law in Germany, Austria, and Ireland revealed significant divergences from the GDPR caused by their national provisions. While divergent practices can provide challenges for harmonizing data protection laws across the EU, they also provide opportunities for better data security standards and tailored regulations. The open clauses provide flexibility that can be interpreted as either a strength or a weakness, continuous revising and coordination among the EU to ensure that the GDPR's standard is met is necessary to achieve its goal. Understanding these differences will be crucial to navigating the complexity of data protection in the EU and in each member state.

Opportunities:

With the GDPR's open clauses, member states can tailor their data protection laws to their specific legal, administrative contexts, and enhance the regulation's relevance and effectiveness to as little or as much as they'd like. Using Austria's advocacy on data protection for minors as an example, we can see how they have used the GDPR to better enhance their existing laws relating to said protections. In case DSB 2022-0.858.901, the DPA ruled that the recordings made from the cctv cameras, with the intended use to protect people and property, were to limit the processing of images by either turning the cameras off during school hours, or ensuring that no recordings were being made during school hours.

With the use of open clauses, it can help to influence other countries to enforce more rigorous standards (such as Germany and Austria) which can help to improve data protection

laws across the EU. This divergent approach can also provide an opportunity for member states to share and learn from each country's experiences, to foster a collaborative and engaged approach to constantly revising the national and EU contexts.

The opportunities for enhanced protection stems from the ability for member states to apply more stringent rules for data protection. This can be extrapolated for various applications such as LG Magdeburg - DE 9-O-1571-20, for example. As shown in the case, the processor applied an incorrect debt to the plaintiff's credit agency, which led to financial and personal repercussions for the plaintiff. With the open clauses provision, the German courts could implement a law stating that data processors (in this case a credit agency), would need to adhere to data verification standards to ensure that incorrect applications of debt do not get applied to future data subjects. This can be further expanded upon by looking at the Bank of Ireland case, IN-20-7-2, where the BOI failed to implement appropriate technical security measures to ensure a level of security appropriate to the risk.

Challenges:

The extensive compliance standards that are present within the GDPR and the resulting national laws and provisions, present an issue when it comes to interpretations and rulings, as it will take experts who are specialized in the specific legalities tied to the GDPR. On the whole, the GDPR has a total of eleven chapters which are then made up of multiple different sections and those sections themselves being composed of articles. In total for the whole GDPR regulation there are ninety nine articles, of which topics range from Rights (such as the Right to

Erasure as explored earlier), to regulations relating to the competency of potential DPA heads. [84]

With the provision of the open clauses by the GDPR, there is potential for fragmentation among the differing member states, with implementations of contradictory laws. This would invariably add to the complexity that is already present among different jurisdictions of the EU. Though the GDPR is designed to alleviate the difficulty of interactions amongst member states, that does not always translate to a smooth court case, as was the case in the WhatsApp trial, IN-18-5-6. The plaintiff first lodged his complaint against WhatsApp in Germany, and was being handled by the Hamburg Data Protection Authority. He was then promptly transferred to the German Federal Data Protection Authority, and then finally being transferred to the Irish DPC.

The large amount of regulations present within the GDPR has the potential to create confusion with different interpretations from one court to another. While one court could be lenient on an infringement, another court in a different member state could rule for a harsher penalty, given similar complaints.

VII. Discussion

The central goal of this paper was to determine why we see a divergence in practices in data security among EU member states. Of which, I have identified several patterns among member states and their various implementations of the open clauses for the GDPR. While some of these patterns were to be expected, such as Germany's strict stance for their citizens' privacy rights, there were others that surprised me. For example, Ireland's take on the enforcement related open clauses were not expected. The case of WhatsApp was particularly surprising as it shows the willingness of the DPC to administer large fines amounting to a total in the millions. The issues that had been presented involved a perceived "forced consent" and a lack of transparency needed for users to make an informed decision. This had violated several articles of the GDPR, Article 5(1)(a) and Article 6(1). This is compounded with previous infringements which had violated transparency rules related to Articles 12(1) and 13(1)(c) of the GDPR as well. As previously mentioned, the total of the administrative fine was a sum of €5.5 million, showing how serious Ireland's DPC takes these violations.

The implications that are present in these cases shine a light on the potential for member states to expand upon areas where the GDPR may be a weak application in their country relative to others, thus allowing for the hardening of protection policies and the overall improvement for their citizens' data privacy. Based on my previous findings, the likelihood of other member states updating their current data protection laws, is within the near future as data protection laws seem to be updated regularly to help combat new threats to data privacy. In scenarios where this would work well is in areas such as schools. We see this in the Austrian case, DSB 2022-0.858.90, where the school had inadvertently violated Article (6) and (8) of the GDPR, by having their

CCTV cameras record video of the property with minors in view. This protection can therefore be extrapolated further to protect other vulnerable groups such as the elderly.

Through the course of my research, I found that even with the GDPR's large scope, the regulation as a whole had been implemented across the EU in a very effective manner. Providing an overall framework for the member states to work with, and also provide clauses to where they can more granularly tune the regulations to fit their nation's existing data protection laws, or all together replace them with newer, updated versions. This isn't to say that my research has not run into roadblocks, several times I had run into an impasse of finding cases that were relevant to my research questions. While I had expected to face some difficulty in this area, I believed that access to these cases would be easier to obtain, due to the nature of how the GDPR's "transparency" is supposed to have this information easily accessible. Instead, more often than not, I had to find source material from cited cases through either member state databases, legislations, or even the official GDPR website in order to find relevant cases that would shine light onto my thesis questions. However, this isn't to say that the results from my research do not show excellent examples of how varying the provisions of the GDPR can be, and its implementations into national contexts.

Future research may benefit from looking at cases that focus on specific areas of the GDPR, such as transparency issues, or issues related to data breaches as this could prove beneficial to find common causes of these infringements. This could potentially improve the compliance rates in these areas if the root cause of the infringements were to be identified, so that we could better understand why these infringements keep taking place.

VIII. Conclusion

This thesis identifies a few advantages and disadvantages that arise from these divergent data practices among member states. The variation in each country's national context creates a difficult-to-navigate legal landscape for multinational and international businesses that are looking to operate in the EU countries. The utilization of "open clauses" from the GDPR is meant to allow for flexibility for national provisions, may also undermine the uniformity that the GDPR is trying to establish and could potentially lead to confusion or uncertainty for individuals and businesses. It also highlights the disparities in level of strictness for data protection laws that we can see each member state take. We can also see how all the cases we have studied exemplify and highlight not only the real-world application of the GDPR, but as well as how crucial it will be for maintaining and advocating for individual rights as we continue to progress in the digital age.

The findings highlight how the GDPR provides a unified framework for data protection across the EU and uncovers the reasons behind the similarities and differences in the data protection practices. It also discusses how these member states utilize the open clauses and the complexity of implementing the GDPR into their national contexts. The research provided by this paper may be particularly interesting to corporations and policy makers as they can use it as insight to further improve harmonization across the EU and businesses can gain a better understanding of the legal landscape and compliance to allow them to navigate these varying levels of legal requirements. Furthermore, for those who operate as researchers or academics, the use of this research may prove useful to build upon further exploring the dynamic of the GDPR and its relationship to data protection and individuals rights.

While this paper has provided a comprehensive analysis and description of the GDPR and its implementation into a few member states, there are still several areas that could benefit from further exploration. For example, the impact the GDPR has on smaller EU member states or economic benefits and incentives the GDPR provides for member states. Additionally, examining the role of how technology and its integration into the GDPR compliance could provide practical insight, such as in the instance of "E-Privacy" which still hasn't been formally introduced into the GDPR clauses as of date. The significance of this research lies in its contribution to understanding the broader implication of the GDPR implementation for data protection across the EU. By highlighting these variations and commonalities in national contexts, we can provide valuable insight into the advantages and disadvantages for achieving a fully convergent data protection regulation that can continue to effectively protect data protection rights. Which brings us back to my original questions.

Firstly, "Why do Germany, Austria, and Ireland have differing data subject privacy practices?" I believe that my research into the GDPR and its various divergences throughout Europe's member states, has shown that through different means, each member state can work to achieve the same goal that the GDPR sets out to accomplish; which is the enhancement of data protection for EU citizens. Taking into consideration Germany's history with past data collection, we see where their strict approach to data protection stems from, and comparing the changes Germany made to the open clauses, to that of Austria's fine tuning of the DSG to better integrate with the GDPR. Out of the member states I had selected, the one that surprised me the most was Ireland, and the extent to which they take enforcement. This was a factor that I had not taken into consideration at the onset of my research. I believe it shows that the enforcement side of the GDPR is where we'll see the more significant changes to data protection as a whole, as in the

long run it would prove to be unprofitable for companies to be lax on their data protection standards if such fines as €5.5 million or more are on the table.

In regards to my second question, "How do these differences in data security practices among these EU member states reflect their unique national adoption of the GDPR?" It's readily apparent from Germany's rigid and comprehensive data protection laws, that they drew heavily from past laws as a guideline to create a very privacy oriented framework. With Austria, they took a more tailored approach to their laws to address specific national concerns for data privacy and are one of the main champions of data protection rights for minors. Finally, with Ireland being a hub for multinational corporations, this naturally has led to the regulations they have worked towards implementing to be more focused on enforcement, which we have seen throughout this paper several times with various cases being referred to the Irish DPC for adjudication.

Finally, the last question is, "What challenges and opportunities do these divergent data subject privacy practices present for the effectiveness of the GDPR in harmonizing data protection laws across the EU?" There have been many challenges and opportunities that have arisen from these divergent practices in data subject privacy rights. One challenge for example, is that Germany's strict data protection rights might create a compliance issue for international businesses. In contrast, Ireland's heavy enforcement could potentially deter infringements from taking place. Still, they also pose the risk of over-penalizing organizations they do find to be in breach of regulation, whether it be through negligence or otherwise. Austria seems to have struck an excellent balance, which presents opportunities for harmonization with the GDPR as a whole, while also highlighting the need for clarity in the GDPR's application.

After thoroughly examining several member states' and respective case studies and data protection laws, I have found that the flexibility provided by the GDPR's open clauses introduce a fragmentation of the original mandate of the GDPR; a unified data protection regulation for all of the EU. Through ongoing evaluations of member state's utilized open clauses, and a continuous dialogue between other members, the EU can work to further enhance the GDPR and more closely achieve their goal.

IX. Glossary

Term	Definition
Austrian Data Protection Act (DSG)	Austria's main national law on data protection and privacy. The DSG supplements the General Data Protection Regulation and came into effect May 25, 2018. Protects the personal data of legal persons and gives the Data Protection Authority (DSB) additional powers, duties, and responsibilities.
Charter of Fundamental Rights of the European Union (ECFR)	First declared in 2000 and came into force in December 2009, the Charter enshrines the rights to personal freedom, beliefs, and other rights into one legally binding document.
Court of Justice of the European Union (CJEU)	The judicial authority of the European Union.
Data Protection Authority (DPA)	An independent public body that monitors and enforces data protection laws at the national level. Each Member State has their own DPA.
Data Protection Commission (DPC)	An independent authority in Ireland that protects the personal data of individuals. The DPC is also tasked with the supervision and enforcement of the General Data Protection Regulation.
Data Protection Directive (DPD)	European Union directive that regulates how personal data is processed and collected within the EU.
Datenschutzbehörde (DSB)	Austria's federal data protection authority responsible for enforcing the General Data Protection Regulation.
European Commission (EC)	The European Commission is the executive branch of the European Union and is responsible for the day-to-day running of the European Union.
European Convention of Human Rights (ECHR)	An international treaty that protects the rights and political freedoms of people in counties that belong to the Council of Europe.
European Data Protection Board (EDPB)	An independent body of the European Union that works to ensure that the General Data Protection Regulation is applied consistently across the European Union to promote cooperation between

Term	Definition
	the EU's data protection authorities.
European Data Protection Supervisor (EDPS)	An independent government agency that monitors and ensures that European institutions and bodies respect the right to privacy and data protection when processing personal data.
European Parliament (EP)	The European Parliament is the European Union's law-making body and the only EU institution directly elected by European citizens.
European Union (EU)	The European Union is a political and economic union of 27 European countries that governs common social, economic, and security practices.
Federal Commissioner for Data Protection and Freedom of Information (BfDI)	Referring to either a person or the agency they lead, tasked with supervising data protection as well as acting in an ombudsman function in freedom of information. Operates in Germany.
Federal Data Protection Act (BDSG)	A German law that governs the collection, processing, and storage of personal data by public and private entities.
General Data Protection Regulation (GDPR)	A law that sets guidelines for how personal information is collected and processed from individuals.
Member State	A Member State is a sovereign state that is a member of an international organization or federation. (e.g., The European Union)
New Federal Data Protection Act (BDSG-New)	A German law that went into effect on May 25, 2018, replacing the previous BDSG.
Organization for Economic Co-operation and Development (OECD)	An international organization that works with 38 democracies from Europe, North America, the Pacific Rim, and Latin America to promote economic growth, prosperity, and sustainable development.
Working Party (WP)	The Working Party on the Protection of individuals with regard to the Processing of Personal Data

X. Citations

1. *The History of the General Data Protection Regulation | European Data Protection Supervisor*. 25 May 2018,
2. "Charter of Fundamental Rights of the European Union." *OJ C*, vol. 326, 26 Oct. 2012, http://data.europa.eu/eli/treaty/char_2012/oj/eng.
3. *HUDOC - European Court of Human Rights*. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-120%22.
4. "Press Corner." *European Commission - European Commission*,
5. *The History of the General Data Protection Regulation | European Data Protection Supervisor*. 25 May 2018, https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
6. *Legacy: Art. 29 Working Party | European Data Protection Board*. https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en.
7. *Legacy: Art. 29 Working Party | European Data Protection Board*. https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en.
8. *What Is Personal Data? - European Commission*. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.
9. *What Is Personal Data? - European Commission*. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.
10. *The History of the General Data Protection Regulation | European Data Protection Supervisor*. 25 May 2018, https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
11. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
12. *The History of the General Data Protection Regulation | European Data Protection Supervisor*. 25 May 2018, https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
13. Bundesministerium der Justiz und für Verbraucherschutz. "Telemediengesetz (TMG)." *Gesetze im Internet*, n.d., https://web.archive.org/web/20240510021914/https://www.gesetze-im-internet.de/tmg/BJNR017910007.html.
14. *Types of Legislation | European Union*. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en.

15. International Telecommunication Union. "Telecommunications Act." *ITU-D Regulatory and Market Environment*, n.d., https://www.itu.int/ITU-D/treg/Legislation/Germany/TelecomAct.pdf.
16. *Comprehensive Approach on Personal Data Protection in the European Union | European Data Protection Supervisor*. 22 May 2024, https://www.edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_en.
17. *The History of the General Data Protection Regulation | European Data Protection Supervisor*. 25 May 2018, https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
18. *Legacy: Art. 29 Working Party | European Data Protection Board*. https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en.
19. *EP Adopts GDPR | European Data Protection Supervisor*. 12 Mar. 2014, https://www.edps.europa.eu/ep-adopts-gdpr_en.
20. "Press Corner." *European Commission - European Commission*, https://ec.europa.eu/commission/presscorner/home/en.
21. "Press Corner." *European Commission - European Commission*, https://ec.europa.eu/commission/presscorner/home/en.
22. "Press Corner." *European Commission - European Commission*, https://ec.europa.eu/commission/presscorner/home/en.
23. "Press Corner." *European Commission - European Commission*, https://ec.europa.eu/commission/presscorner/home/en..
24. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020. academic.oup.com, https://doi.org/10.1093/oso/9780198826491.001.0001.
25. Becher, Samuel, and Uri Benoliel. *Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR*. 3334095, 13 Feb. 2019. Social Science Research Network, https://papers.ssrn.com/abstract=3334095.
26. Gentile, Giulia, and Orla Lynskey. "*DEFICIENT BY DESIGN? THE TRANSNATIONAL ENFORCEMENT OF THE GDPR.*" International & Comparative Law Quarterly, vol. 71, no. 4, Oct. 2022, pp. 799–830. Cambridge University Press, https://doi.org/10.1017/S0020589322000355.
27. Molnár-Gábor, Fruzsina, et al. "*Harmonization after the GDPR? Divergences in the Rules for Genetic and Health Data Sharing in Four Member States and Ways to Overcome Them by EU Measures: Insights from Germany, Greece, Latvia and Sweden.*" Seminars in Cancer Biology, vol. 84, Sept. 2022, pp. 271–83. ScienceDirect, https://doi.org/10.1016/j.semcancer.2021.12.001.
28. *GenDG - Law on Genetic Testing of Humans*. https://www.gesetze-im-internet.de/gendg/BJNR252900009.html. Accessed 26 May 2024.

29. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex.* https://eur-lex.europa.eu/eli/reg/2016/679/oj.
30. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex.* https://eur-lex.europa.eu/eli/reg/2016/679/oj.
31. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex.* https://eur-lex.europa.eu/eli/reg/2016/679/oj.
32. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex.* https://eur-lex.europa.eu/eli/reg/2016/679/oj.
33. *GenDG - Gesetz Über Genetische Untersuchungen Bei Menschen.* https://www.gesetze-im-internet.de/gendg/BJNR252900009.html#BJNR252900009BJNG000800000. Accessed 26 May 2024.
34. Todt, Kiersten E. "Data Privacy and Protection: What Businesses Should Do." The Cyber Defense Review, vol. 4, no. 2, 2019, pp. 39–46. JSTOR, https://www.jstor.org/stable/26843891. Accessed 27 May 2024.
35. Chase, Peter H. Perspectives on the General Data Protection Regulation Of the European Union. German Marshall Fund of the United States, 2019. JSTOR, http://www.jstor.org/stable/resrep21227. Accessed 27 May 2024.
36. Kulhari, Shraddha. "Data Protection, Privacy and Identity: A Complex Triad." Building-Blocks of a Data Protection Revolution, 1st ed., Nomos Verlagsgesellschaft mbH, 2018, pp. 23–37. JSTOR, https://www.jstor.org/stable/j.ctv941qz6.7.
37. De Busser, Els, et al. "Big Data: The Conflict Between Protecting Privacy and Securing Nations." BIG DATA: A Twenty-First Century Arms Race, Atlantic Council, 2017, pp. 5–16. JSTOR, http://www.jstor.org/stable/resrep03719.5. Accessed 27 May 2024.
38. Rep. Sensenbrenner, F. James. H.R.1428 - 114th Congress (2015-2016): Judicial Redress Act of 2015. 24 Feb. 2016, https://www.congress.gov/bill/114th-congress/house-bill/1428. 2015-03-18.
39. *IAPP*. https://iapp.org/news/a/most-member-states-wont-be-ready-for-gdpr/.
40. *IAPP*. https://iapp.org/news/a/2013-03-01-privacy-law-and-history-wwii-forward/.
41. Bundesverfassungsgericht, 1 Senat. *Bundesverfassungsgericht - Decisions - Decision on the Constitutionality of the 1983 Census Act*. 15 Dec. 1983, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.
42. *Basic Law for the Federal Republic of Germany*. https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html.
43. Bundesverfassungsgericht, 1 Senat. *Bundesverfassungsgericht - Decisions - Decision on the Constitutionality of the 1983 Census Act*. 15 Dec. 1983, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.
44. *TMG - Telemedia Act*. https://www.gesetze-im-internet.de/tmg/BJNR017910007.html.

45. International Telecommunication Union. "Telecommunications Act." *ITU-D Regulatory and Market Environment*, n.d., https://www.itu.int/ITU-D/treg/Legislation/Germany/TelecomAct.pdf.
46. *Federal Data Protection Act (BDSG)*. https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0014.
47. *Federal Data Protection Act (BDSG)*. https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0361.
48. Book (eISB), electronic Irish Statute. *Electronic Irish Statute Book (eISB)*. https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print#part6-chap6:~:text=the%20further%20investigation.-,Chapter%206,Administrative%20Fines,-Power%20of%20Commission.
49. *RIS Dokument*. https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html.
50. *Bürgerservice - VGH München, Beschluss v. 29.06.2023 – 6 ZB 23.530*. https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2023-N-17253?hl=true.
51. *§ 112 BBG - Einzelnorm*. https://www.gesetze-im-internet.de/bbg_2009/__112.html.
52. *Code of Administrative Court Procedure*. https://www.gesetze-im-internet.de/englisch_vwgo/englisch_vwgo.html#:~:text=Section%20124,claimed%20and%20applies%20on%20which%20the%20ruling%20can%20be%20based.
53. *§ 112 BBG - Einzelnorm*. https://www.gesetze-im-internet.de/bbg_2009/__112.html#:~:text=(1)%20Documents%20about,the%20official%2C%20or.
54. *§ 1004 BGB - Einzelnorm*. https://www.gesetze-im-internet.de/bgb/__1004.html.
55. OpenJur. "Judgment U 2470822." *OpenJur*, n.d., https://openjur.de/u/2470822.ppdf.
56. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
57. "Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (Text with EEA Relevance)." *OJ L*, vol. 119, 27 Apr. 2016, http://data.europa.eu/eli/reg/2016/679/oj/eng.
58. Bundesarbeitsgericht. "Urteil vom 13. Oktober 2023 – 9 AZR 383/19." *Bundesarbeitsgericht*, 13. Oct. 2023, https://www.bundesarbeitsgericht.de/wp-content/uploads/2023/10/9-AZR-383-19.pdf.
59. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

60. *Federal Data Protection Act (BDSG)*. https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0057:~:text=table%20of%20contents-,Section%206%0APosition,-(1)%20The%20public.
61. *RIS Dokument*. https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html.
62. *CURIA - Documents*. https://curia.europa.eu/juris/document/document.jsf?text=&docid=198764&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=111014.
63. "Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters." *OJ L*, vol. 012, 22 Dec. 2000, http://data.europa.eu/eli/reg/2001/44/oj/eng.
64. "Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters." *OJ L*, vol. 012, 22 Dec. 2000, http://data.europa.eu/eli/reg/2001/44/oj/eng.
65. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
66. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
67. Verfassungsgerichtshof. "Erkenntnis G 287/2022, G 288/2022 vom 14. Dezember 2022." *Verfassungsgerichtshof*, 14 Dec. 2022, https://www.vfgh.gv.at/downloads/VfGH-Erkenntnis_G_287_2022-_G_288_2022_vom_14._Dezember_2022.pdf.
68. *RIS Dokument*. https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html#:~:text=MedienG)%20zu%20beachten.-,%C2%A7%C2%A09.,Paragraph%209%2C,-(1)%20The%20provisions.
69. *RIS - 2022-0.858.901 - Entscheidungstext - Datenschutzbehörde*. https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=b4b3fe31-61ea-4b14-a922-22d519a912a5&Position=1&SkipToDocumentPage=True&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=EinerWoche&ImRisSeitForRemotion=EinerWoche&ResultPageSize=100&Suchworte=DSGVO&Dokumentnummer=DSBT_20230906_2022_0_858_901_00.
70. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
71. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
72. Book (eISB), electronic Irish Statute. *Electronic Irish Statute Book (eISB)*. https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print#sec56.

73. Data Protection Commission. "Final Decision IN-20-7-2 Bank of Ireland (BOI)." *Data Protection Commission*, Mar. 2023, https://www.dataprotection.ie/sites/default/files/uploads/2023-03/Final%20Decision%20IN-20-7-2%20Bank%20of%20Ireland%20%28BOI%29%20365.pdf.
74. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
75. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
76. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
77. Data Protection Commission. "WhatsApp Final Decision (adoption version) Redacted." *Data Protection Commission*, Apr. 2023, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/WhatsApp%20FINAL%20DECISION%20%28adoption%20version%29%20Redacted.pdf.
78. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
79. "Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (Text with EEA Relevance)." *OJ L*, vol. 119, 27 Apr. 2016, http://data.europa.eu/eli/reg/2016/679/oj/eng.
80. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
81. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
82. *Regulation - 2016/679 - EN - Gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
83. "Press Corner." *European Commission - European Commission*, https://ec.europa.eu/commission/presscorner/home/en.
84. "Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (Text with EEA Relevance)." *OJ L*, vol. 119, 27 Apr. 2016, http://data.europa.eu/eli/reg/2016/679/oj/eng.