World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Evaluating the Impact of Data Protection Compliance on AI Development and Deployment in the U.S. Health sector

Emmanuel Utomi [1], Adewale Samuel Osifowokan [2], Alice Ama Donkor [3] and Isaac Amornortey Yowetu [3,*]

[1] *Department of Computing and Informatics, College of Science, University of Louisiana at Lafayette, LA, USA.*
[2] *Renegeron Pharmaceuticals, New York, USA.*
[3] *Klerconsult, El Paso, TX, USA.*

World Journal of Advanced Research and Reviews, 2024, 24(02), 1100–1110

Publication history: Received on 29 September 2024; revised on 09 November 2024; accepted on 11 November 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.2.3398

Abstract

This paper evaluates the impact of data protection Compliance on artificial intelligence development and deployment in the U.S. Health sector. As AI technologies develop quickly, worries about data security and privacy have increased, especially in delicate industries like healthcare. HIPAA, or the Health Insurance Portability and Accountability Act, and CCPA, or California Consumer Privacy Act, are two important U.S. laws that are examined in this paper along with their comparison to the European Union's General Data Protection Regulation, or GDPR. The intersection of AI and data protection regulations is also examined. The analysis emphasizes the necessity for privacy-by-design principles and the development of openness and accountability, and it shows how these policies affect AI developers, healthcare providers, and other stakeholders. Through an analysis of the opportunities and obstacles posed by the CCPA and HIPAA, the paper offers useful guidance for managing the regulatory environment and promoting innovation in AI development. The study reports that observing data protection rules is not only required by law but also strategically crucial for fostering public confidence and guaranteeing the moral application of AI in healthcare. The paper finally concludes that maintaining a sustainable growth of AI applications in the U.S. healthcare industry requires striking a balance between technological advancement and stringent data privacy procedures and compliance as AI continues to advance.

Keywords: Artificial intelligence; Data protection; Compliance; U.S. healthcare; HIPAA; CCPA; Privacy laws.

1. Introduction

The inclusion of AI in decision-making processes has revolutionized how various sectors of organizations operate [1]. However, given how quickly technology is advancing, privacy and data security compliance are becoming increasingly important concerns. Following the introduction of stringent data protection legislation such as the GDPR (General Data Protection Regulation) in Europe and the California Consumer Privacy Act, also known as the CCPA, in the US, the development and deployment of AI systems has encountered new opportunities as well as obstacles. According to Chander et al., [2], "The goal of the California Consumer Privacy Act (CCPA) is to provide Californian consumers more power. The CCPA, which went into effect in January 2020, signals the start of a new phase in consumer-centric data protection laws in the US. This legislation, which started in California, has stimulated discussions on the necessity of federal privacy rules and encouraged other states to look into or pass legislation along similar lines." On the other hand, European regulation known as the General Data Protection Regulation (GDPR) created safeguards for the security and privacy of personal data about people in operations situated in the European Economic Area ("EEA") as well as in some non-EEA businesses that handle personal data of people in the EEA [3]. The aforementioned policies have significant consequences for AI practitioners and stakeholders as they seek to protect personal data and uphold individuals' privacy rights in an increasingly digitalized society.

* Corresponding author: Isaac Amornortey Yowetu

Artificial Intelligence is strongly dependent on data to work; it uses large datasets to train algorithms and improve model performance [4]. There are several facets to the relationship between AI and data, and theoretical frameworks highlight the vital role that high-quality data plays in the advancement of AI [5]. Due to our reliance on data, there are some data privacy concerns that are brought up, such as the possibility of bias, misuse, and unwanted access. Subsequently, the Council of Europe underscores that "AI applications that may have an impact on people and society must be developed and adopted with the preservation of human dignity, human rights, and fundamental freedoms especially the right to the privacy of one's personal information [6]. For example, the GDPR places strict guidelines on gathering, analyzing, and storing data, highlighting the necessity of clear consent, accountability, and openness. Similarly, "the California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the CCPA regulations guide how to implement the law" [7]. Conceptually, an extensive assessment of these legal frameworks' effects on AI technologies is required. Data protection and artificial intelligence (AI) convergence is a complex and multifaceted problem that requires a thorough grasp of both technical and legal perspectives [8]. Investigating how data privacy laws affect AI research and application in the healthcare setting is crucial to navigating this terrain. This study aims to bridge this gap by providing an in-depth analysis of the Impact of Data Protection Compliance on AI Development and Deployment in the U.S. Health sector. By examining the regulatory requirements and their operational impact, we identify the challenges that AI developers face and the strategies they can employ to achieve compliance while maintaining innovation in the healthcare setting.

The relevance of this study stems from how it contributes to the current discussion of AI governance and ethics in the realm of data protection compliance. As AI systems grow more prevalent, it is critical to ensure that they follow data protection rules to foster public confidence and adoption. This study employs secondary research methodologies, including an examination of U.S. data protection legislation, such as the California Consumer Privacy Act (CCPA) and HIPAA, that are relevant to artificial intelligence (AI) and the healthcare industry. Through these reviews, we aim to showcase optimal strategies and insights gained from rules that have successfully explored regulatory compliance. Lastly, the goal of this research is to offer useful insights into the constant interactions that exist between AI development and deployment and data protection compliance. We give AI practitioners and consumers the knowledge they need to design and execute cutting-edge, legally compliant artificial intelligence systems by highlighting the potential and challenges presented by HIPAA and CCPA. The results emphasize how important it is to apply privacy-by-design guidelines and foster an open, accountable culture in the creation and application of AI. Maintaining the long-term evolution of AI technology will require finding a balance between innovation and data protection as we enter an era where AI is only becoming better.

2. Literature Review

2.1. An Overview of Data Privacy Legislation

According to the study conducted by Puri [9], "Data privacy laws are essential protectors in the digital age, where data flows like a current defining the features of contemporary life, outlining the guidelines for gathering, using, and sharing personal data". The two primary players in the global regulatory landscape that are the focus of this analysis are the General Data Protection Regulation (EU GDPR) and US data privacy legislation. The protection of data in the EU saw a radical change in 2018 with the introduction of the EU GDPR. It replaced the Data Protection Directive of 1995 to modernize and harmonize data protection laws across all EU member states. The impetus for legislation stems from an increasing acknowledgment of the need for a strong legal structure that protects people's privacy while also addressing the issues brought about by technological progress.

The EU GDPR's comprehensive approach to data protection is based on fundamental principles, as noted by Labadie & Legner [10]. People have certain rights with their personal data, such as the ability to access, correct, erase, and receive information. Data controllers are required to adhere to the legality, equity, and transparency criteria. The law also encourages firms to include privacy concerns from the outset of their operations by presenting the concept of safeguarding information by design and default. Both the federal and state governments in the United States have enacted numerous data privacy regulations, many of which are industry-specific. The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that specifically addresses the security and privacy of health information. According to Hulkower, et al., [11], HIPAA creates guidelines to safeguard private health information, guaranteeing its availability, confidentiality, and integrity. Covered businesses including health plans, healthcare clearinghouses, and healthcare providers are subject to the statute [12].

One significant state law that came into effect in 2020 was (CCPA). Residents of California have various rights under the CCPA regarding their personal information, such as the ability to seek the deletion of their information, the right to know what data is collected, and the ability to opt out of data sales [13]. Despite being unique to California, the CCPA

has a significant impact across state lines, frequently influencing national discussions about comprehensive federal privacy legislation. In addition to HIPAA and CCPA, other federal laws that cover particular areas of data privacy in the US include the Gramm-Leach-Bliley Act (GLBA) and the Children's Online Privacy Protection Act (COPPA) [13]. Additionally, states are passing more and more privacy legislation, which results in a confusing web of rules that businesses need to follow [13, 14, 15].

The data privacy legislation concludes by highlighting the broad and cohesive EU GDPR framework throughout the European Union, in contrast to the fragmented, industry- and state-specific US legal environment. Understanding and adhering to these rules is essential for both individuals and companies as AI interactions go across regional borders. The subtleties, difficulties, and complications of different data privacy frameworks and compliance will be further explored in the upcoming sections of this comparative assessment.

2.2. Fundamentals and Structures

Strong regulatory frameworks in the field of data privacy are constructed on principles. The European Union General Data Protection Regulation (EU GDPR) and US data privacy laws have similar goals but differ slightly in their guiding principles, according to a comparison of the two laws [16]. According to Sharma [16], the EU GDPR emphasizes the values of protecting equity, processing personal data properly, and maintaining transparency. Businesses are required to inform people about how personal data is handled, providing explicit explanations of the purposes and legal basis for such processing. Data processing must adhere to the purpose limitation principle as mandated by the EU GDPR. According to Hartzog & Richards [17], and other scholars, personal data should only be gathered for clear, explicit, and legal purposes. Any additional processing should be done in a way that further advances these initial goals.

Under the GDPR, companies are encouraged to gather only information that is strictly essential for the intended purpose, hence advocating for data minimization [18]. This idea discourages the acquisition of extra data and is consistent with the notion of privacy by design. It is the responsibility of organizations to guarantee the precision of the private information they handle. According to Zhang et al [19], “to ensure that the information is reliable, steps should be taken to quickly correct errors. No longer than required for the reasons for which it is processed, personal data should be kept on file”. The GDPR promotes the idea of storage limits by introducing precise timeframes for data storage. Protecting the authenticity and privacy of personal data is vital. To prevent unwanted access, alteration, or disclosure, organizations must put in place the proper organizational and technical safeguards. Accountability, a fundamental component of the EU GDPR, calls on enterprises to prove that they are adhering to its guidelines [17]. This entails keeping thorough records of all data processing operations and, if required, doing impact analyses on data protection [17].

The notice and consent principle is in place in the United States, where people have the right to be given notice of the data gathered by company activities and to provide their consent prior to the collection, processing, or sharing of personal data. Similar to the EU GDPR, the USA's data privacy framework strongly emphasizes keeping data processing within the original goals for which it was obtained. This is in line with the main objective of guaranteeing equity and avoiding unforeseen applications of personal data. By guiding organizations to gather just the information required for the intended purpose, data reduction principles reduce the possibility of misuse and unwanted access. The implementation of security measures is a top priority in the US to prevent unlawful acquisition, dissemination, modification, and destruction of personal data. Certain security needs are outlined by several laws, including sector-specific legislation. Accountability is essential to US data privacy frameworks, just like it is to the EU GDPR [18]. It is required of organizations to take appropriate precautions to protect personal information and to be responsible for the processing of their data operations.

In conclusion, while the US and EU GDPR both adhere to core principles, their differing approaches to data protection framework design are a reflection of the varied legal traditions and cultural viewpoints that inform these frameworks. Due to the increasingly linked global context in which enterprises operate, it is imperative to comprehend these concepts to effectively navigate the intricate nuances of data privacy compliance, particularly in the era of AI development and deployment.

2.3. Basis for Law and Consent

In the context of AI development and application, Murdoch [20] asserts that data privacy laws are critical to safeguarding individuals' private information. A crucial element of these policies is obtaining consent before processing personal data. This comparison study looks at the legal basis and authorization requirements under the General Data Protection Regulation (EU GDPR) and various data privacy regulations in the US. Under the EU GDPR, consent is a legal basis for handling personal data. It differentiates between implied and explicit permission [21, 22]. A definite affirmative

action, like checking a box or proactively confirming a choice, is necessary for explicit permission from the data subject. Contrarily, implied consent is more subtle and can be deduced from a person's conduct. The EU GDPR places a strong focus on people's control over personal data [23]. The law gives data subjects the freedom to change their mind at any moment. This implies that people are free to decide how their data is used, and that companies must respect and make it easier for people to withdraw their consent without harming the data subject.

Unlike the EU GDPR, the US lacks a comprehensive federal privacy law for data compliance [16]. Instead, data privacy requirements are the result of an ad hoc combination of federal and state laws. The conditions for permission can vary widely. For instance, according to Edemekong et al., [24], "the use and sharing of protected health information is subject to certain consent requirements under the Health Insurance Portability and Accountability Act (HIPAA) in the healthcare industry". Consent is a concept that is deeply ingrained in healthcare laws like HIPAA. Before any use or disclosure of their health information, patients must give their informed consent. This includes the provision of healthcare services, payment, and treatment [24].

The complexity and context-dependency of consent in the United States underscore the fragmented and sector-specific structure of the nation's data privacy regulations and compliance. The unified consent framework of the EU GDPR encourages harmonization between member states [25]. The absence of a comprehensive federal statute in the United States leads to a fragmented landscape with disparate consent requirements. Businesses that operate in many states have difficulties as a result, as they must navigate various legal systems [26]. The EU GDPR emphasizes specific, affirmative actions and establishes high standards for consent. Transparency and personal liberty are given priority in this method. Achieving a uniform norm across sectors could be difficult in the United States since consent regulations differ, but it could result in improved data protection [27, 28].

While acknowledging the significance of consent, the EU GDPR and US data privacy laws take different methods. The EU GDPR gives people a strong right to withdraw and lays a significant focus on express consent. The legal system in the United States, on the other hand, is more dispersed because it combines federal and state laws. The ongoing discourse about federal privacy law in the United States presents a chance to tackle these discrepancies and progress towards a complete structure that conforms to the rapidly changing global privacy norms, particularly in the realm of AI development and deployment.

2.4. Rights of Individuals in the AI era

A key component of data privacy legislation across the globe is safeguarding people's rights in the digital age. Comparatively speaking, this study looks at the rights given to data subjects under the EU GDPR and the various data privacy laws that exist in the US [17]. People have the right to know whether or if their private information has been used and, if so, to access such data, according to the EU GDPR. Transparency is guaranteed, and people are empowered to know about and confirm the legality of the processing according to this right.

Individuals who provide their data have the right to have any errors corrected. This contributes to the confidentiality of people's data by ensuring that they can keep information correct and up to date. Another name for this right is the "right to be forgotten," which gives people the ability to ask for the erasure of their personal information in certain situations. It gives people the power to decide when their data should be deleted when it is no longer needed for the intended use [18, 29]. People can now obtain their data in an organized, widely used, and machine-readable manner thanks to this right. They can then send this information to an additional controller. There is no thorough federal data privacy law in the United States. Individuals' rights are instead provided via a patchwork of state-level rules and other sector-specific statutes. For example, Californian consumers have rights under the California Consumer Privacy Act (CCPA), such as the right to access and the right to be deleted. Transparency and control are prioritized heavily under U.S. data privacy rules, even though specific rights may differ [30]. People frequently have the right to understand what personal data is gathered and how it is utilized. They can also choose not to participate in specific data processing activities according to several rules [23]. The extensive list of individual rights the EU GDPR provides offers a uniform foundation for the European Union. To remedy the current fragmentation, efforts are being made in the United States to create a federal privacy law that might standardize rights across states and sectors [31].

By giving people control over their data, these frameworks seek to empower individuals by making sure people understand these rights and can use them effectively is the difficult part. In this context, education and awareness-raising initiatives are essential. The United States takes a sector-specific and state-driven strategy, whereas the EU GDPR establishes high standards for individual rights. The United States' changing environment, including debates about federal privacy laws, offers a chance to bring standards closer to those of other countries. While creating fair and effective data privacy laws, keeping the interests of corporations and individual rights in balance is still crucial.

2.5. Disclosure of Data Breach

Data breaches represent serious risks to people's security and privacy in today's fast-paced digital environment. This research compares the various frameworks of data breach rules in the United States with the requirements for reporting data breaches under the General Data Protection Regulation (EU GDPR). Per the EU GDPR, "Organizations must notify the appropriate supervisory body of a data breach as soon as possible and, if possible, within 72 hours once they become aware of it" [23]. Information about the breach's nature, its expected effects, and the steps taken or suggested to rectify it must all be included in the notification [32].

According to Talesh [33], "All data breaches must be internally documented by enterprises, regardless of whether notification is necessary". The handling of data breaches is made transparent and accountable to this documentation. Organizations including those in the healthcare landscape must notify the impacted data subjects of a data breach as soon as possible if there is a reasonable suspicion that the breach will pose a danger to their rights and liberties [34]. This correspondence ought to furnish lucid and comprehensible details on the type of breach and suggest actions that people might take to reduce any possible hazards. Organizations in the healthcare domain must collaborate with the supervisory authority concurrently throughout the inquiry and reaction. Building confidence and making sure regulators and data subjects are informed immediately depend on transparent communication.

The United States does not have a federal breach of data notification law, in contrast to the uniform approach of the EU GDPR. Rather, the regulatory framework is state-specific, creating a disjointed and intricate data privacy environment. Certain states have special rules for alerting those affected by a data breach, such as California, which has the California Consumer Privacy Act (CCPA). In this context, notification must be sent to affected parties promptly. The United States federal government has regulations for notifying data breaches in specific areas, including the healthcare sector. For example, after a breach is discovered, covered entities are required by the Health Insurance Portability and Accountability Act (HIPAA) to notify the affected people, the Department of Health and Human Services (HHS), and, in certain cases, the media [13].

The U.S. lacks a comprehensive data breach notification statute, which has made harmonization difficult [35]. According to the literature by Nagi [35], "There are plans to enact federal legislation that would standardize the process and make it easier for companies that operate in many states to comply". Diverse notification requirements present a difficulty for organizations with global operations. A customized response plan and a thorough comprehension of the relevant legislation are necessary to achieve compliance. While the U.S. struggles with a decentralized system, the EU GDPR establishes a standard for prompt and transparent data breach notification. The continuous endeavors in the United States to enact federal legislation offer a chance for more efficient and uniform procedures for notifying data breaches, in accordance with the worldwide movement for strict privacy laws [28, 36, 37].

3. Enforcement and Consequences

In the era of AI development and deployment, data privacy rules are essential for protecting people's personal information. This comparative review explores the various data privacy laws in the United States as well as the enforcement mechanisms and penalties under the General Data Protection Regulation (EU GDPR) [21, 22]. Supervisory authorities have the right to penalize companies found to be in breach of the EU GDPR with significant fines. There are two different levels of fines: the primary level is up to €20 million or 4% of the global annual revenue, whichever is larger, and the secondary level is up to €10 million or 2% of the global annual turnover [38]. These penalties highlight the significance of compliance by being commensurate with the seriousness of the infraction. Notably, a variety of infractions are susceptible to sanctions, such as inadequate data protection protocols, a lack of openness, and failure to abide by the rights of data subjects. Enforcing the GDPR is the responsibility of the supervisory authorities in each EU member state. They can do audits, give warnings, mandate compliance actions, and levy fines as part of their investigative and corrective authorities. According to [28, 39] the cooperative character of supervisory authorities enables uniform enforcement throughout the European Union.

Even though the concept for the agency was first proposed in the US in the 1970s, the US remains one of the few countries in the entire globe lacking a federal privacy law [40]. The US was previously a privacy leader in the world [16]. As a reaction to the increasing computerization of personal data in the US, the Fair Credit Reporting Act was passed in 1970 and is seen as the first contemporary privacy law. But in terms of protecting customer data, Europe has now overtaken the USA. Customers' ownership over their data is reinstated and their fundamental rights are safeguarded by the General Data Protection Regulation. It gives European data subjects the following rights: data portability (the ability for a data subject to receive and transmit personal data about them to another controller), access (the right to know whether or not personal data about them is being processed, where, and for what purpose), and breach notification

(within 72 hours of a breach). None of these rights apply to American data subjects [41]. This implies that American businesses will have to grant these rights to Europeans but not to Americans, creating an underclass of digital citizens. American businesses lead the world in technology, and the government ought to set the standard for technology policy as well, particularly in the era of AI development and deployment in the healthcare sector.

Conceptually, the absence of a thorough federal data privacy regulation in the United States makes it difficult to enforce the law consistently and clearly. This thus, calls for federal legislation to provide a cohesive framework for more robust and consistent enforcement in the U.S. Companies that operate internationally must navigate a variety of enforcement methods, which can be challenging. Complying with U.S. and EU GDPR requirements necessitates customized data compliance methods and a deep comprehension of the legal environment. The EU GDPR implements a cohesive and strong enforcement framework, whereas the United States faces challenges related to complex jurisdiction and industry-specific legislation. The United States' ongoing efforts to pass federal legislation offer a chance to modernize global privacy standards and expedite enforcement. To reduce the danger of significant fines, both areas emphasize how important it is for businesses to prioritize data protection and compliance [42].

4. Global Impact and Transnational Scope

The data privacy policies of the United States and the European Union, particularly the General Data Protection Regulation (EU GDPR), are crucial components of the global digital economy. This comparative analysis examines the regulations' extraterritorial reach and worldwide ramifications, providing insight into how they affect global trade and the difficulties multinational firms encounter. Despite having its roots in the European Union, the EU GDPR has a significant impact outside of its member states. Compliance applies to any entity, regardless of location, that handles the personal data of EU citizens. This has significant ramifications for foreign companies operating in the EU or providing services to their nationals [43].

According to Bakare et al. [40], the GDPR's broad description of personal data and strong data protection rules need a multifaceted approach to compliance. To comply with GDPR rules, organizations must implement privacy by design, conduct data protection impact evaluations, and designate data protection officers. The GDPR's extraterritorial reach creates jurisdictional issues. Non-EU companies that process EU residents' data may be subject to the regulation's compliance procedures, including fines. To handle these jurisdictional complexities, businesses around the world have reassessed their data-handling processes and implemented GDPR-compliant frameworks [44, 18]. The United States lacks a comprehensive federal data privacy regulation that is widely enforced, like the GDPR. On the other hand, extraterritorial reach is indicated by certain laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA), as well as industry-specific regulations. For example, CCPA applies to enterprises outside of California that process personal information from California citizens and meet specified qualifications. HIPAA, a federal statute, applies to non-US companies that handle protected health information about US citizens.

Multinational firms face difficulties in negotiating the complex landscape of US data privacy legislation. The lack of a single federal legislation results in disparities in compliance requirements between states and industry. This decentralized approach complicates corporations' efforts to maintain consistent global data protection standards [45]. The disparity in data privacy requirements between the EU GDPR and US legislation presents compliance issues for worldwide businesses. Harmonizing methods to comply with both sets of legislation requires meticulous preparation and a thorough grasp of their respective requirements [46, 47].

Looking at inferences from the literature, the growing complexity of data privacy regulations in both regions leads to a changing regulatory environment. Businesses have to stay agile in adjusting to new compliance requirements in light of ongoing changes, such as potential federal laws in the United States and GDPR amendments. The global impact and extraterritorial reach of data privacy rules highlight the digital world's interconnected nature. Businesses operating on a global scale must take proactive steps to meet the problems provided by different legislative frameworks, highlighting the significance of a strategic, internationally aware strategy for data protection and compliance.

5. Obstacles and Concerns

Businesses trying to meet compliance while maintaining data protection with commercial interests face challenges and concerns due to the dynamic landscape of data privacy laws, which is exemplified by the General Data Protection Regulation (EU GDPR) and data privacy regulations in the US. Several important topics are covered in this comparative analysis, such as possible contradictions between EU GDPR and US rules, compliance concerns, and the fine balance

between business interests and data protection. A major obstacle that organizations encounter is the sophisticated and complex nature of data privacy legislation. The EU GDPR lays out a complete framework with strict guidelines, such as mandated breach notifications, data minimization standards, and rights for data subjects. The lack of a single federal legislation in the United States leads to a patchwork of state and industry-specific laws, like the Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA) [48]. Comprehending this complex web of laws requires a sophisticated grasp of their legal systems.

According to Li et al [49], making sure that U.S. and EU GDPR requirements are followed by multinational companies that operate internationally poses a big challenge. Due to the rules of extraterritorial reach, organizations that process the personal data of citizens of the United States or residents of the European Union must ensure that their operations comply with specific legal standards. Organizing data protection procedures across many legal and logistical frameworks becomes difficult [50]. Finding a balance between business interests and data protection is an ongoing problem specifically in this era of AI development and deployment. Although strong data privacy regulations and compliance are necessary to protect people's rights, companies frequently struggle with the need to innovate and use data to make strategic decisions. Organizations must enforce ethical data practices and privacy-by-design principles to resolve the conflict between safeguarding personal data and encouraging innovation [27, 51].

There are significant costs associated with achieving and upholding compliance with data privacy legislation. To comply with regulations, industries in the healthcare sector must set aside funds for data protection officers, legal counsel, and the adoption of technical solutions. Combining the capital investments required for compliance with larger business goals involves strategic decision-making. Potential disputes arise from the disparities in requirements and norms between the EU GDPR and U.S. legislation. The right to data portability and the right to be forgotten, for example, are prioritized under the GDPR, although similar provisions may not exist under U.S. rules. To ensure complete compliance, navigating these disparities necessitates a close review of legal requirements.

The sharing of personal data across the EU and the U.S. confronts obstacles due to disparities in legislative regulations and compliance. The tight data protection laws in the EU, which are frequently thought to be stronger than those in the US, make it difficult for data to travel freely. Businesses engaging in transatlantic data transfers must establish procedures such as Standard Contractual Clauses (SCCs) to solve these problems [18]. The difficulties and worries related to compliance with data privacy rules are a reflection of how quickly the digital landscape is changing especially in AI development and deployment.

Companies managing these intricacies need to place a high priority on adopting a proactive, flexible approach to compliance, understanding the necessity of striking a balance between data security and the demands of innovation and international operations. Addressing these difficulties establishes the basis for ethical, accountable, and legally sound data management in an increasingly linked world.

6. Prospective Patterns and Advancements

The data privacy legal landscape is always changing as a result of rules continuously adjusted to meet new issues that arise in the digital age like AI development and deployment [52]. The European Union General Data Protection Regulation (EU GDPR) and data privacy laws in the United States are the main subjects of this comparative analysis, which evaluates the Impact of Data Protection Compliance on AI Development and Deployment in the U.S. Health sector. Global data protection standards are expected to continue to rise in the future. With its strong framework, the EU GDPR has established a standard for all-encompassing data protection laws. Inspired by the concepts of the GDPR, other jurisdictions will probably amend or implement their laws to offer more robust protections for people's data. This change is indicative of a growing understanding of the value of privacy in the digital era.

The rights granted to individuals by data privacy legislation are expected to expand as awareness of data privacy increases. Future laws might strengthen already existing rights for data subjects or add new ones. The growth of individual rights within data privacy regulations and compliance is anticipated to center on the right to own one's data and the capacity to hold organizations accountable for its usage [53]. The swift progression of technology demands that current regulations be updated regularly. Future modifications may cover cutting-edge technology like biometrics, artificial intelligence, and the Internet of Things (IoT), making sure that data privacy regulations continue to be applicable and efficient in protecting personal data in the face of AI development and deployment.

Regulators will probably implement clauses that demonstrate adaptation and flexibility in response to evolving situations. This covers procedures for quickly responding to data breaches, revisions to breach notification laws, and clauses that support cutting-edge business models while upholding strict data protection compliance. Recognizing the

interrelated nature of global data flows, there is an increasing drive for cross-border collaboration in designing data privacy rules. The goal of harmonization efforts is to establish a unified framework that supports high and uniform standards of data protection while enabling cross-border data exchanges. For international corporations attempting to adhere to many regulatory environments, this kind of cooperation is essential. Prospective developments could involve endeavors to harmonize data protection guidelines among legal systems. Although every location might still have its own set of regulations, efforts to standardize could concentrate on fundamental ideas to make compliance easier for healthcare corporations. This can entail a common focus on individual rights, data minimization, and transparency.

Future advancements and trends in data privacy regulations point to a commitment to strengthening people's online control over their data. The development of these regulations is influenced by changes in society's expectations, technical improvements, and the need to create a uniform global data protection strategy. To maintain continuous compliance and moral data practices, businesses working in the healthcare sector or environment need to foresee these developments and cultivate a proactive and flexible approach, particularly in the era of AI development and deployment.

7. Conclusion

An analysis of the differences between the US and EU data privacy laws highlights how crucial data privacy and compliance are for companies doing business in the U.S. healthcare landscape in AI development and deployment. The EU GDPR and the US data privacy laws are compared in this study. The comparison analysis highlighted the subtle distinctions and commonalities between the US and EU data privacy laws and compliance. In contrast to the EU GDPR, which promotes a holistic, rights-based approach, the US uses a sectoral model with a variety of federal and state laws, including the CCPA and HIPAA. In all regulatory regimes, the assessment emphasized the importance of permission, individual rights, data breach notifications, and enforcement measures. One cannot stress how crucial it is to comply with data privacy laws and adhere to data privacy compliance in the digital era where AI development and deployment have become everyday things. Ensuring the privacy of people's personal information becomes both a strategic and moral requirement for corporations as they negotiate the intricate web of legislation. Beyond meeting legal requirements, adhering to data privacy laws increases consumer/patients' trust, improves sectorial reputation, and lowers the possibility of negative legal and financial outcomes. Respecting the rights and expectations of data subjects is what data privacy compliance is all about; it's not just a box to be checked. The fundamental values of data privacy legislation support a culture of responsible data stewardship that is well-received by partners and customers in the healthcare setting and beyond. These values form the basis of moral business practices. This comparative review's conclusion is a call to action for companies working in the U.S. healthcare sector to take a proactive approach to data protection as they explore AI in their operations. It is becoming more and more necessary to be informed as the regulatory environment changes, both legally and strategically. Companies need to make it a priority to regularly review how they handle data and stay up to date on any changes to laws and industry standards. In the face of AI development and deployment, shifting consumer/patient demands, and international harmonization initiatives, adaptability is essential for data privacy compliance. Businesses should include privacy-by-design principles into their daily operations to ingrain a dedication to data security at every stage of the data processing activity's lifespan.

In conclusion, organizations in the U.S. healthcare landscape have a huge obligation to respect and safeguard people's privacy because they are the guardians of a great deal of personal data. By taking on this obligation, they help to build a digital ecosystem based on ethics, openness, and trust, in addition to adhering to legal requirements. Healthcare institutions are asked to approach the ongoing transition to strong data privacy with caution, devotion, and a commitment to the highest ethical standards.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed

References

[1] Saba, D., Sahli, Y., & Hadidi, A. (2021). The role of artificial intelligence in a company's decision-making. Enabling AI Applications in Data Science, 287-314.

[2] Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). Achieving privacy: Costs of compliance and enforcement of Data Protection Regulation. Policy Research Working Paper, 9594.

[3] GDPR, G. D. P. R. (2016). General data protection regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[4] Topol, E. J. (2019). High-performance medicine: the convergence of human and artificial intelligence. Nature medicine, 25(1), 44-56.

[5] Gangwal, A., Ansari, A., Ahmad, I., Azad, A. K., & Sulaiman, W. M. A. W. (2024). Current strategies to address data scarcity in artificial intelligence-based drug discovery: A comprehensive review. Computers in Biology and Medicine, 179, 108734.

[6] Ruppert, A., & Wendt, D. H. (2021). Data protection and EU-regulation for artificial intelligence. In Connected Living: international and interdisciplinary conference (2021), Frankfurt am Main.

[7] Illman, E., & Temple, P. (2019). California Consumer Privacy Act. The Business Lawyer, 75(1), 1637-1646.

[8] Yanamala, A. K. Y., Suryadevara, S., & Kalli, V. D. R. (2024). Balancing Innovation and Privacy: The Intersection of Data Protection and Artificial Intelligence. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 15(1), 1-43.

[9] Puri, A. (2022). The group's right to privacy (Doctoral dissertation, University of St Andrews).

[10] Labadie, C., & Legner, C. (2019, February). Understanding data protection regulations from a data management perspective: a capability-based approach to EU-GDPR. In Proceedings of the 14th International Conference on Wirtschaftsinformatik (2019).

[11] Hulkower, R., Penn, M., & Schmit, C. (2020). Privacy and confidentiality of public health information. Public Health Informatics and Information Systems, 147-166.

[12] Krzyzanowski, B., & Manson, S. M. (2022). Twenty years of the health insurance portability and accountability act safe harbor provision: unsolved challenges and ways forward. JMIR medical informatics, 10(8), e37756.

[13] Harding, E. L., Vanto, J. J., Clark, R., Hannah Ji, L., & Ainsworth, S. C. (2019). Understanding the scope and impact of the California consumer privacy act of 2018. Journal of Data Protection & Privacy, 2(3), 234-253.

[14] Putman, C. G. J. (2020). Assessing the Impact of the Implementation of the California Consumer Privacy Act on the United States through Policy Evaluation (Master's thesis, University of Twente).

[15] Li, Y. (2019). The California Consumer Privacy Act of 2018: Toughest US Data Privacy Law with Teeth? Loy. Consumer L. Rev., 32, 177.

[16] Sharma, S. (2019). Data privacy and GDPR handbook. John Wiley & Sons.

[17] Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. BCL Rev., 61, 1687.

[18] Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65-98.

[19] Zhang, H., Yu, Y., Jiao, J., Xing, E., El Ghaoui, L., & Jordan, M. (2019, May). Theoretically principled trade-off between robustness and accuracy. In International conference on machine learning (pp. 7472-7482). PMLR.

[20] Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Medical Ethics, 22, 1-5.

[21] Fabbrini, F., & Celeste, E. (2020). The right to be forgotten in the digital age: The challenges of data protection beyond borders. German Law Journal, 21(S1), 55-65.

[22] Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online. Technology, 58(2), 157-65.

[23] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.

[24] Edemekong, P. F., Annamaraju, P., & Haydel, M. J. (2018). Health insurance portability and accountability act.

[25] Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). Human genetics, 137, 575-582.

[26] Hagemann, R., Huddleston Skees, J., & Thierer, A. (2018). Soft law for hard problems: The governance of emerging technologies in an uncertain future. Colo. Tech. LJ, 17, 37.

[27] Hu, I. Y. (2019). The Global Diffusion of the 'General Data Protection Regulation'(GDPR). Edited by KH Stapelbroek and S. Grand. Erasmus School of Social and Behavioural Sciences.

[28] Voss, W. G., & Bouthinon-Dumas, H. (2021). EU general data protection regulation sanctions in theory and practice. Santa Clara High Tech. LJ, 37, 1.

[29] Van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. Journal of consumer policy, 42, 91-107.

[30] Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. Big Data & Society, 6(1), 2053951719860542.

[31] Safari, B. A. (2016). Intangible privacy rights: How Europe's gdpr will set a new global standard for personal data protection. Seton Hall L. Rev., 47, 809.

[32] Peppet, S. R. (2014). Regulating the internet of things: first steps toward managing discrimination, privacy, security, and consent. Tex. L. Rev., 93, 85.

[33] Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. Law & Social Inquiry, 43(2), 417-440.

[34] Marcus, D. J. (2018). THE DATA BREACH DILEMMA. Duke Law Journal, 68(3), 555-593.

[35] Nagi, A. (2024). Comparing GDPR Against the United States' Approach to Data Breach Notification by Examining Texas and California and the Feasibility of a Universal Standard. Cybaris®, 15(2), 14.

[36] Vlahou, A., Hallinan, D., Apweiler, R., Argiles, A., Beige, J., Benigni, A., ... & Vanholder, R. (2021). Data sharing under the General Data Protection Regulation: time to harmonize law and research ethics?. Hypertension, 77(4), 1029-1035.

[37] Winter, J. S., & Davidson, E. (2022). Harmonizing regulatory regimes for the governance of patient-generated health data. Telecommunications Policy, 46(5), 102285.

[38] Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. Journal of Information Policy, 11, 63-103.

[39] Schreiber, A. (2019). Feeling fine! Harmonization and inconsistency in EU supervisory authority administrative fines. Journal of Data Protection & Privacy, 2(4), 375-388.

[40] Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations. Computer Science & IT Research Journal, 5(3), 528-543.

[41] Tsesis, A. (2019). Data subjects' privacy rights: regulation of personal data retention and erasure. U. Colo. L. Rev., 90, 593.

[42] Abraha, H. H. (2020). Regulating law enforcement access to electronic evidence across borders: the United States approach. Information & Communications Technology Law, 29(3), 324-353.

[43] Alic, D. (2021). The role of data protection and cybersecurity regulations in artificial intelligence global governance: a comparative analysis of the European Union, the United States, and China Regulatory Framework. Search in.

[44] Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. Computer Law & Security Review, 44, 105640.

[45] Jacob Nix, C. I. S. A., & CCSFP, C. (2020). US Data Privacy Law: A Disparate Landscape in Need of Consolidation.

[46] Ahlstrom, D., Arregle, J. L., Hitt, M. A., Qian, G., Ma, X., & Faems, D. (2020). Managing technological, sociopolitical, and institutional change in the new normal. Journal of Management Studies, 57(3), 411-437.

[47] Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299-1323.

[48] Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. Business & Society, 58(1), 3-19.

[49] Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. Journal of Global Information Technology Management, 22(1), 1-6.

[50] Sarangi, U. (2018). Information Economy and Data Protection Laws: A Global Perspective. International Journal of Business and Management Research, 6(2), 15-35.

[51] Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. Journal of Competition Law & Economics, 16(3), 349-391.

[52] Acquisti, A., Brandimarte, L., & Hancock, J. (2022). How privacy's past may shape its future. Science, 375(6578), 270-272.

[53] Solove, D. J., & Schwartz, P. M. (2020). Information privacy law. Aspen Publishing.