International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

GDPR's impact on cybersecurity: A review focusing on USA and European practices

Olukunle Oladipupo Amoo [1], Akoh Atadoga [2], Femi Osasona [3], Temitayo Oluwaseun Abrahams [4,*], Benjamin Samson Ayinla [5] and Oluwatoyin Ajoke Farayola [6]

[1] *Department of Cybersecurity, University of Nebraska at Omaha, United States of America.*
[2] *Independent Researcher, San Francisco, USA.*
[3] *Scottish Water, UK.*
[4] *Independent Researcher, Adelaide, Australia.*
[5] *University of Law Business School, Manchester, United Kingdom.*
[6] *Financial Technology and Analytics Department, Naveen Jindal School of Management. Dallas, Texas, USA.*

International Journal of Science and Research Archive, 2024, 11(01), 1338–1347

Publication history: Received on 27 December 2023; revised on 03 February 2024; accepted on 05 February 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.11.1.0220

Abstract

The General Data Protection Regulation (GDPR) has emerged as a landmark legislation reshaping the global landscape of data privacy and cybersecurity. Enforced in May 2018, the GDPR has had a profound impact on organizations worldwide, prompting a reevaluation of cybersecurity practices to ensure compliance with stringent data protection standards. This paper provides a comprehensive review of GDPR's influence on cybersecurity, with a particular emphasis on the contrasting approaches and practices adopted in the United States (USA) and Europe. The GDPR introduces a set of robust principles designed to protect the rights and privacy of individuals, emphasizing the need for transparency, accountability, and proactive measures to safeguard personal data. Its extraterritorial scope extends its impact beyond European borders, compelling businesses operating globally to adhere to its regulations. This paper explores the challenges and opportunities arising from GDPR compliance, examining how organizations in the USA and Europe have navigated the evolving cybersecurity landscape. In the USA, where privacy regulations historically differed across states, the GDPR has prompted discussions around the development of federal privacy laws. The review delves into the varying approaches adopted by American businesses, considering the interplay between state and federal regulations in shaping cybersecurity strategies. Conversely, European practices reflect a proactive response to the GDPR, as organizations have embraced the principles embedded in the regulation to fortify cybersecurity frameworks. The paper investigates the evolution of cybersecurity standards in Europe, highlighting successful strategies and potential areas for improvement. By synthesizing experiences from both sides of the Atlantic, this review contributes to a deeper understanding of the GDPR's impact on cybersecurity. It sheds light on the evolving dynamics of data protection, offering insights for organizations seeking to enhance their cybersecurity resilience in the face of a rapidly changing regulatory landscape.

Keywords: GDPR; Cybersecurity; USA; Europe; Data Protection; Review

1. Introduction

The General Data Protection Regulation (GDPR), enacted in May 2018, stands as a transformative force reshaping the global landscape of data protection and cybersecurity. As the most comprehensive data privacy regulation to date, the GDPR has far-reaching implications for organizations worldwide, compelling them to reevaluate and fortify their cybersecurity practices (Alic, 2021, Dowd & Dowd, 2022). This paper undertakes a comprehensive review of the GDPR's impact on cybersecurity, with a specific focus on the divergent approaches and practices observed in the United States (USA) and Europe.

* Corresponding author: Temitayo Oluwaseun Abrahams

Copyright © 2024 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

In an era where digital transactions and data-driven technologies are ubiquitous, the GDPR addresses the critical need for safeguarding individuals' rights and privacy. Grounded in principles of transparency, accountability, and proactive data protection, the regulation introduces a new standard for organizations that handle personal data. Its extraterritorial reach extends its influence beyond the borders of the European Union, impacting businesses operating on a global scale (Politou, et. al., 2022, Van de Waerdt, 2020).

This review aims to dissect the multifaceted effects of the GDPR on cybersecurity, with particular attention to the contrasting responses witnessed in the USA and Europe. While the USA has historically grappled with a patchwork of state-level privacy regulations, the GDPR has stimulated discussions on the necessity for federal privacy laws and prompted a paradigm shift in cybersecurity strategies. Conversely, Europe has demonstrated a proactive embrace of the GDPR's principles, influencing a paradigmatic shift in organizational cybersecurity frameworks.

As organizations on both sides of the Atlantic navigate the complexities of GDPR compliance, this review seeks to unravel the nuances, challenges, and success stories that have emerged. By providing a comparative analysis of USA and European practices, the paper aims to contribute valuable insights for businesses, policymakers, and cybersecurity professionals seeking to adapt to the evolving regulatory landscape and bolster their defenses in an era of heightened data protection expectations.

2. GDPR Principles and Framework

The General Data Protection Regulation (GDPR) represents a paradigm shift in the realm of data protection, introducing a comprehensive set of principles designed to safeguard individuals' privacy in an increasingly digitized world (Andrew & Baker, 2021, Reinhardt, 2022). At its core, GDPR seeks to empower individuals with greater control over their personal data while imposing significant responsibilities on organizations that collect, process, and store such information. The key principles that underpin the GDPR framework are here discussed. GDPR mandates that the processing of personal data must be lawful, fair, and transparent. Organizations are required to communicate clearly with individuals about the purposes of data processing, ensuring they have a full understanding of how their information will be used. Organizations are obligated to collect personal data for specified, explicit, and legitimate purposes. Any subsequent processing must be compatible with these original purposes, discouraging the indiscriminate use of collected data. The GDPR encourages the minimization of personal data processing. Organizations should only collect and process data that is strictly necessary for the intended purpose, reducing the risk of data breaches and unauthorized access. Organizations are required to ensure the accuracy of the personal data they process and take steps to rectify inaccuracies promptly (Ke & Sudhir, 2023, Štarchoň & Pikulík, 2019). This principle underscores the importance of maintaining reliable and up-to-date information. GDPR imposes constraints on the retention of personal data. Organizations must establish predefined retention periods, and data should not be kept longer than necessary for the intended purpose. Organizations are obligated to implement appropriate technical and organizational measures to ensure the security of personal data. This includes protecting against unauthorized access, disclosure, alteration, and destruction. Perhaps one of the most significant principles, accountability requires organizations to demonstrate compliance with GDPR. This involves maintaining detailed records of data processing activities, conducting privacy impact assessments, and appointing a Data Protection Officer in certain cases.

One of the most distinctive features of the GDPR is its extraterritorial reach, transcending the boundaries of the European Union to impact businesses operating globally. Regardless of their physical location, organizations that process personal data of EU residents are subject to the regulation. This has far-reaching implications for multinational corporations, requiring them to navigate a complex web of compliance obligations. The extraterritorial scope of GDPR has stimulated a global conversation on data protection standards, prompting countries outside the EU to reevaluate and strengthen their own privacy regulations. Non-compliance can result in substantial fines, making it imperative for businesses worldwide to align their practices with GDPR requirements. This not only reflects a legal obligation but also a growing expectation from consumers for a higher standard of data protection (Burri, 2021, Daniel, 2022).

Transparency, accountability, and data protection lie at the heart of the GDPR, reflecting a commitment to fostering a culture of trust between individuals and the entities that handle their data. GDPR places a strong emphasis on transparency in data processing. Individuals have the right to be informed about how their data is used, who processes it, and for what purposes. This transparency requirement is intended to empower individuals to make informed decisions about the use of their personal information. The accountability principle holds organizations responsible for their data processing activities (Lamoureux, 2020, Polanco, 2020, Schade, 2023). This involves implementing measures to ensure compliance, such as conducting privacy impact assessments, maintaining records of processing activities, and appointing a Data Protection Officer when necessary. Accountability not only strengthens data protection but also builds confidence among stakeholders. GDPR's overarching goal is to enhance the protection of personal data. By establishing

robust security measures, organizations can mitigate the risk of data breaches and unauthorized access. The regulation encourages a proactive approach to data protection, urging organizations to prioritize the security and integrity of the information they handle.

In conclusion, the GDPR principles and framework represent a groundbreaking effort to address the evolving challenges of data protection in the digital age. By fostering transparency, accountability, and a heightened focus on data protection, the GDPR sets a global standard for privacy regulations, compelling organizations worldwide to reevaluate their practices and prioritize the rights and privacy of individuals in an interconnected and data-driven world.

2.1. Evolution of Cybersecurity Practices in the USA

The United States has navigated a complex and fragmented landscape of privacy regulations throughout its history. Unlike the European Union, which embraced comprehensive data protection legislation early on, the USA traditionally relied on a patchwork of sector-specific laws and regulations. The absence of a federal privacy law created a dynamic environment where different industries adhered to disparate rules, often resulting in varying standards for the protection of personal information (Debbarma, 2023, Getrich, et. al., 2019, Tullis & Kar, 2021).

Historically, privacy regulations in the USA have been reactive, responding to specific incidents or emerging technologies rather than adopting a holistic approach. Legislation such as the Privacy Act of 1974 and the Electronic Communications Privacy Act of 1986 provided some protections, but the absence of a comprehensive framework left gaps in addressing the challenges posed by the rapid evolution of technology.

The introduction of the General Data Protection Regulation (GDPR) in Europe marked a watershed moment that reverberated across the Atlantic, prompting discussions on the need for federal privacy laws in the USA (Borges Monroy, 2023, Rubinstein & Petkova, 2019). The GDPR's comprehensive and rights-focused approach set a new standard for data protection, pushing the USA to reevaluate its regulatory landscape.

In response to GDPR, there was a noticeable shift in the discourse surrounding privacy in the USA. Lawmakers, industry leaders, and privacy advocates engaged in conversations about the necessity of a federal privacy framework that could provide a unified and robust approach to data protection. The GDPR served as a catalyst for rethinking the adequacy of existing laws and recognizing the importance of harmonizing privacy regulations at the national level.

The USA's regulatory environment is further complicated by the interplay between state and federal regulations. Unlike the centralized approach of the GDPR, the American regulatory landscape is characterized by a federal system where individual states retain significant autonomy in shaping their privacy laws. This decentralized structure has led to a patchwork of state-level regulations, creating compliance challenges for businesses operating across multiple jurisdictions (Cairney & Wellstead, 2021, Wu, Hao & Ren, 2020).

While some states, such as California with its California Consumer Privacy Act (CCPA), have taken steps to enact comprehensive privacy legislation, the absence of a federal standard has resulted in inconsistencies. The interplay between state and federal regulations has created a complex compliance landscape, where businesses must navigate varying requirements and standards depending on their geographic reach.

The extraterritorial reach of the GDPR has posed considerable challenges for American businesses aiming to achieve compliance with European data protection standards. Some of the key challenges include; the disparity between US privacy regulations and the stringent requirements of the GDPR presents a compliance dilemma for American businesses. Adapting to a new and comprehensive framework requires significant adjustments to data processing practices, often necessitating substantial investments in technology and personnel training (Jovanovic, 2020, Voss & Houser, 2019). The patchwork of state and federal regulations in the USA adds a layer of complexity for businesses striving to meet GDPR standards. Achieving compliance with varying and sometimes conflicting requirements across jurisdictions requires a nuanced understanding of the regulatory landscape. Smaller businesses, in particular, may face resource constraints when attempting to align with the GDPR. Implementing robust cybersecurity practices and ensuring compliance demands financial investments, skilled personnel, and a thorough understanding of the intricacies of the regulation. American businesses that handle data transfers between the USA and the EU must grapple with GDPR's strict guidelines on international data transfers. Ensuring lawful data flows while maintaining compliance with GDPR poses a significant hurdle.

In conclusion, the evolution of cybersecurity practices in the USA has been marked by a historical context of decentralized and sector-specific regulations. The influence of the GDPR has sparked conversations about the need for

a comprehensive federal privacy law, yet the interplay between state and federal regulations continues to present challenges for businesses. Navigating these complexities requires a strategic and adaptable approach to cybersecurity, as organizations strive to meet the evolving expectations of data protection in a globally interconnected digital landscape.

2.2. European Response to GDPR

The European response to the General Data Protection Regulation (GDPR) has been characterized by a proactive embrace of its principles, setting the stage for a paradigm shift in the region's approach to data protection. The GDPR, with its stringent requirements and emphasis on individual rights, prompted European nations to reevaluate and fortify their cybersecurity frameworks. This proactive adoption is rooted in a commitment to safeguarding the privacy and rights of individuals in an era of unprecedented data-driven advancements (Arner, Castellano & Selga, 2022, Bauer & Erixon, 2020).

European countries recognized the need for a comprehensive and standardized approach to data protection, leading to the incorporation of GDPR principles into national legal frameworks. The GDPR's emphasis on transparency, accountability, and data minimization resonated across industries, influencing not only legal and compliance teams but also shaping the mindset of organizations and individuals involved in handling personal data.

The impact of the GDPR on organizational strategies and practices in Europe has been transformative, influencing how businesses collect, process, and manage personal data. Key aspects of this impact include; the GDPR prompted organizations to establish robust data governance structures, ensuring accountability and transparency in data processing activities. This shift involved the appointment of Data Protection Officers (DPOs), conducting privacy impact assessments, and developing comprehensive records of processing activities. The GDPR's emphasis on the security and integrity of personal data led to the implementation of advanced cybersecurity measures. European organizations invested in state-of-the-art technologies, encryption protocols, and employee training programs to mitigate the risk of data breaches and unauthorized access (de Carvalho, et. al., 2020, Jafari-Sadeghi, et. al., 2021, Labadie & Legner, 2019). The GDPR places a strong emphasis on empowering individuals with greater control over their personal data. This has translated into organizations providing clearer and more accessible privacy notices, facilitating easier data access requests, and respecting individuals' rights to erasure and data portability. European organizations, cognizant of the GDPR's extraterritorial reach, established global compliance standards. This involved aligning data protection practices not only with European regulations but also with the evolving privacy landscape worldwide. Such foresight positioned European companies as leaders in navigating the complexities of international data transfers.

The European experience with GDPR compliance has yielded success stories and valuable lessons that resonate globally; Organizations that successfully implemented GDPR compliance measures experienced an increase in customer trust. Transparent data practices, coupled with robust security measures, reassured individuals about the responsible handling of their personal information, fostering long-term customer loyalty. GDPR compliance has spurred innovation in privacy-enhancing technologies. European companies have been at the forefront of developing solutions that prioritize privacy by design, offering individuals greater control over their data while enabling organizations to meet regulatory requirements seamlessly. Successful GDPR compliance in Europe often involved collaborative efforts and knowledge sharing. Organizations learned from each other's experiences, sharing best practices and contributing to the development of a community dedicated to advancing data protection standards. European nations have played a leading role in advocating for robust data protection regulations globally. GDPR's influence has extended beyond the European borders, inspiring other jurisdictions to consider similar principles in their privacy frameworks (Buckley, Caulfield & Becker, 2022, Li, 2020, Sandin & Sjöholm, 2023).

In conclusion, the European response to the GDPR reflects a proactive and innovative approach to data protection. The region's commitment to embracing and implementing the regulation's principles has not only strengthened cybersecurity practices but has also positioned European organizations as pioneers in the global landscape of data privacy. The success stories and lessons learned from GDPR compliance in Europe serve as a blueprint for organizations worldwide, emphasizing the transformative potential of a comprehensive and principled approach to data protection.

2.3. Comparative Analysis between USA and Europe

The United States and Europe, while both grappling with the challenges of data protection in the digital age, have approached the issue from distinct perspectives. These differences are evident in their regulatory frameworks, historical contexts, and cultural attitudes towards privacy; The USA, historically reliant on sector-specific regulations, lacks a comprehensive federal privacy law. Instead, it operates within a fragmented system of state and industry-specific regulations, resulting in varying standards for data protection across sectors. In contrast, Europe has embraced the

General Data Protection Regulation (GDPR), a unified and comprehensive framework that sets stringent standards for the processing of personal data (Lynskey, 2019, Wu, Vitak & Zimmer, 2020, Zarsky, 2019). Europe has long held a more privacy-centric cultural stance compared to the USA. The GDPR reflects a commitment to safeguarding individual privacy rights and has been shaped by a cultural ethos that values data protection as a fundamental right. In the USA, the cultural perspective on privacy has often been more pragmatic, with a historical emphasis on sector-specific laws responding to specific issues or incidents. The GDPR's extraterritorial reach has had a profound impact on global businesses, irrespective of their physical location. American companies operating in Europe or handling European citizens' data must adhere to GDPR standards, bridging the regulatory gap between the two continents. This contrasts with the USA, where businesses are subject to a patchwork of state-level regulations, and discussions around federal privacy laws are ongoing.

Despite the contrasting approaches, the USA and Europe share common challenges in navigating the complex landscape of data protection. Identifying these challenges has led to the development of shared strategies to address them; both the USA and Europe grapple with the challenges posed by fragmented regulatory environments. The diversity of regulations within the USA and the interplay between state and federal laws mirror the complexities faced by European organizations operating across different jurisdictions. Achieving a balance between fostering innovation and implementing robust data protection measures is a shared challenge. Organizations on both sides of the Atlantic are tasked with adapting to evolving technologies while ensuring compliance with stringent regulatory standards. Small and medium-sized enterprises (SMEs) face resource constraints when navigating the complexities of data protection regulations. Adequate resource allocation for implementing cybersecurity measures and achieving compliance remains a shared challenge for businesses in both regions (Höglund, 2019, Ryngaert & Taylor, 2020). The GDPR's restrictions on international data transfers impact businesses on a global scale. American companies, in particular, face challenges in ensuring lawful data flows between the USA and Europe, navigating the GDPR's strict guidelines for cross-border data processing. The effectiveness of the GDPR in shaping cybersecurity practices is a multifaceted evaluation, considering both its positive impacts and areas that warrant further attention:

The GDPR has raised awareness about the importance of data protection and instilled a sense of accountability among organizations. The appointment of Data Protection Officers and the requirement for privacy impact assessments have reinforced a culture of responsibility. GDPR's emphasis on individual rights has empowered users to have greater control over their personal data. This shift has led organizations to adopt transparent data practices, providing individuals with clearer information about how their data is processed. The GDPR's global influence is evident in the efforts of other countries to adopt similar data protection standards. It has set a benchmark for global data privacy expectations and influenced discussions around international data governance. The GDPR's comprehensive nature has also led to complexity, resulting in a significant compliance burden for businesses, especially SMEs. Streamlining compliance processes and providing clearer guidance could address these challenges. The GDPR's principles are subject to divergent interpretations, leading to variations in enforcement practices across European countries. Achieving greater consistency in interpretation and enforcement would enhance the regulation's effectiveness. While the GDPR has influenced global discussions on data protection, achieving global harmonization of privacy standards remains a challenge. Bridging the gap between the GDPR and other regulatory frameworks could promote a more cohesive approach to data governance on a global scale (Milch, et. al., 2019, Norval, et. al., 2021).

In conclusion, the comparative analysis between the USA and Europe in the realm of data protection underscores the divergent paths these regions have taken. While both face common challenges, their approaches to regulation, cultural attitudes, and strategies for addressing these challenges differ significantly. The effectiveness of the GDPR in shaping cybersecurity practices is evident in its positive impacts on awareness, accountability, and individual empowerment. However, ongoing efforts are needed to address challenges related to complexity, enforcement consistency, and global harmonization. The dynamic landscape of data protection continues to evolve, necessitating continued collaboration and adaptation on both sides of the Atlantic.

2.4. Case Studies

Facebook, a tech giant headquartered in the USA, faced intricate challenges in aligning with GDPR principles. The social media platform, used globally, had to reevaluate its data processing practices to meet the stringent requirements of the regulation. Facebook prioritized transparency, enhancing user consent mechanisms, and implementing tools for users to control their data (Cook, 2021, Nicola & Pollicino, 2020). The case highlights the tension between fostering innovation and achieving compliance, prompting Facebook to strike a delicate balance to maintain its global user base while adhering to GDPR standards.

Microsoft, a multinational technology company, exemplifies a global approach to GDPR compliance. While rooted in the USA, Microsoft has successfully aligned its practices with European data protection standards. The company proactively implemented privacy-by-design principles, invested in advanced cybersecurity measures, and collaborated with European regulatory authorities. Microsoft's case showcases the benefits of adopting a comprehensive global strategy, considering the extraterritorial impact of the GDPR on businesses operating internationally (Oldani, 2020, Petelka, et. al.,2022).

Siemens, a European multinational conglomerate, embraced GDPR compliance as a core corporate value. The company prioritized data protection by implementing robust security measures, conducting regular privacy impact assessments, and fostering a culture of awareness among employees (Dindarian, 2023, van den Hoven et al., 2022). Siemens' case illustrates how European businesses can integrate GDPR principles into their corporate DNA, turning compliance into a strategic advantage and a commitment to customer trust.

SAP, a European software corporation, serves as a prime example of a company implementing privacy by design principles in response to the GDPR. The company incorporated data protection considerations at the inception of new products and services, ensuring that privacy is a foundational element in its technological innovations. SAP's case emphasizes the importance of proactive measures in achieving and maintaining compliance, showcasing how businesses can weave privacy into the fabric of their technological advancements (Mike, 2023, Politou, et. al., 2022).

Transparent communication with users is paramount. Facebook learned that providing clear information about data processing practices, enabling users to control their data, and regularly updating privacy policies fosters trust and helps meet GDPR transparency requirements. Open and transparent communication internally and externally is crucial. Siemens demonstrated that creating a culture of awareness and educating employees about the importance of data protection contributes to overall compliance success (Jaime, et. al., 2023, James & Rabbi, 2023). Global businesses should adopt a unified approach to data protection. Microsoft's case highlights the importance of collaborating with regulatory authorities, implementing consistent standards across regions, and prioritizing a global compliance strategy. Privacy by design is an essential concept. SAP's example teaches businesses the value of integrating data protection considerations into the early stages of product development, ensuring that privacy becomes an integral part of technological innovations. Balancing innovation with compliance is challenging but crucial. Facebook learned that adapting its data processing practices to meet GDPR requirements not only ensures compliance but also aligns with evolving expectations around data protection. Innovation can be a catalyst for compliance. Microsoft demonstrated that investing in advanced cybersecurity measures and leveraging innovative technologies can strengthen data protection practices while fostering a culture of innovation.

In conclusion, these case studies provide valuable insights into how organizations in the USA and Europe have navigated the complex landscape of GDPR compliance. They underscore the importance of transparency, global collaboration, and proactive measures in achieving and maintaining compliance. By learning from these real-world examples, businesses on both sides of the Atlantic can glean valuable lessons to enhance their data protection practices, foster customer trust, and stay ahead in an ever-evolving regulatory landscape.

2.5. Future Implications and Trends

The future of data protection is intertwined with the emergence of privacy-enhancing technologies (PETs). These technologies, including encryption, homomorphic encryption, and differential privacy, are designed to protect data while still allowing for valuable insights. As the regulatory landscape evolves, businesses are expected to increasingly integrate PETs into their cybersecurity strategies to enhance both privacy and security (Becher, et. al., 2020, Hasani, et. al., 2023). A shift towards empowering individuals with greater control over their personal data is anticipated. Future data protection strategies will likely emphasize user-centric control mechanisms, enabling individuals to manage and monitor how their data is processed. This trend aligns with the principles of the GDPR and reflects a growing emphasis on respecting individual privacy rights. The intersection of artificial intelligence (AI) and data protection will become more pronounced. Ethical considerations surrounding AI and its impact on personal data will drive the development of guidelines and frameworks to ensure responsible and transparent use. Organizations will need to balance the benefits of AI with the ethical imperative of protecting individual privacy.

The absence of a comprehensive federal privacy law in the USA is likely to change in the coming years. There is a growing consensus among lawmakers, businesses, and consumers that a unified approach is necessary. The potential evolution towards federal privacy legislation would bring consistency to the regulatory landscape, aligning the USA more closely with global data protection standards. The demand for enhanced consumer privacy protections will likely drive the evolution of privacy regulations. With an increasing awareness of data privacy issues, consumers are becoming

more proactive in advocating for their rights. Future regulations in the USA may incorporate stronger safeguards for individuals, including transparency requirements, data access rights, and mechanisms for opting in or out of data processing. Recognizing the interconnectedness of the global economy, the USA may actively participate in global harmonization efforts. Collaborative initiatives to align privacy regulations with international standards, as seen with the GDPR's influence, could become a focal point for policymakers. This would facilitate smoother cross-border data flows and encourage a more cohesive approach to data protection on a global scale (Chander, Kaminski & McGeveran, 2020, Solove & Schwartz, 2020).

The GDPR's emphasis on accountability is expected to persist, influencing organizations to maintain a proactive and responsible approach to data protection. Continuous efforts to demonstrate compliance, conduct privacy impact assessments, and appoint Data Protection Officers will remain integral to cybersecurity practices. As the GDPR catalyzed discussions around ethical data use, future cybersecurity practices influenced by the regulation will likely incorporate ethical considerations. Organizations will be compelled to assess the broader societal impact of their data processing activities, ensuring alignment with ethical standards and societal values (Aseri, 2020, Hoofnagle, Van Der Sloot & Borgesius, 2019, Sivan-Sevilla, 2022).

The GDPR's extraterritorial scope has already prompted global businesses to align with its standards. Future cybersecurity practices are likely to witness enhanced cross-border collaboration as organizations adapt to evolving regulatory landscapes. This could involve increased cooperation between regulatory authorities and a shared commitment to global data protection standards. The GDPR's impact on cybersecurity practices will continue to drive innovation in privacy technologies. Organizations will explore and adopt advanced solutions to protect personal data while meeting regulatory requirements. Privacy-enhancing technologies will evolve to address new challenges, providing organizations with effective tools to secure sensitive information (Bendiek & Römer, 2019, Gstrein & Zwitter, 2021).

In conclusion, the future implications and trends in data protection and cybersecurity are marked by a shift towards user-centric control, the integration of privacy technologies, and a growing emphasis on ethical considerations. In the USA, the potential evolution of privacy regulations is expected to involve federal legislation, increased consumer privacy advocacy, and efforts towards global harmonization. The GDPR's enduring impact on cybersecurity practices will manifest in the continuous emphasis on accountability, the integration of ethical considerations, and enhanced cross-border collaboration. As the digital landscape evolves, organizations must stay agile to adapt their cybersecurity strategies and embrace emerging trends to effectively safeguard personal data in an increasingly interconnected world.

3. Recommendation

This comprehensive review of GDPR's impact on cybersecurity in the USA and Europe illuminates several critical findings. In the USA, the historical context of fragmented privacy regulations and ongoing discussions regarding federal privacy laws underscore the need for a unified approach. Europe, on the other hand, showcases a proactive adoption of GDPR principles, emphasizing transparency, accountability, and data protection as integral components of organizational strategies.

The examination of select American organizations, such as Facebook and Microsoft, navigating GDPR compliance highlights the challenges of balancing innovation with regulatory adherence. European businesses like Siemens and SAP exemplify the successful alignment with GDPR principles, showcasing the integration of data protection into corporate values and technological advancements.

For organizations operating in the USA, the evolving regulatory landscape suggests a need to prepare for potential federal privacy legislation. The emergence of privacy technologies, a user-centric control approach, and the growing focus on ethical data use signal the direction for future cybersecurity practices. American businesses are encouraged to proactively integrate these emerging trends into their strategies, ensuring alignment with global standards.

In Europe, where GDPR compliance has become ingrained in corporate values, businesses are urged to sustain their commitment to data protection. This involves continuous efforts to enhance transparency, strengthen cybersecurity measures, and foster a culture of accountability. The success stories of Siemens and SAP underscore the importance of weaving data protection into the fabric of organizational identity, ensuring long-term resilience against evolving threats.

The GDPR has ushered in a new era of data protection, influencing cybersecurity practices on a global scale. Its ongoing impact is evident in the heightened awareness, increased accountability, and focus on individual empowerment

observed in both the USA and Europe. As organizations navigate the complexities of data protection, lessons learned from real-world examples, such as those discussed in this review, serve as beacons of guidance.

Looking ahead, the review anticipates a future where privacy technologies play a pivotal role, individuals exercise greater control over their data, and organizations adopt ethical considerations in their data processing practices. The potential evolution of privacy regulations in the USA towards federal legislation aligns with the broader trend of global harmonization, emphasizing the interconnectedness of data protection standards.

4. Conclusion

In conclusion, the GDPR's influence on cybersecurity practices transcends regulatory compliance; it shapes a cultural shift towards a more privacy-aware and responsible digital landscape. Organizations are urged to view GDPR not merely as a regulatory hurdle but as a catalyst for innovation, ethical considerations, and a holistic commitment to protecting the rights and privacy of individuals. As the journey of data protection continues, staying attuned to emerging trends and global standards is paramount for organizations seeking to thrive in an era defined by heightened expectations of privacy and security.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] 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.

[2] Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. Journal of Business Ethics, 168, 565-578.

[3] Arner, D. W., Castellano, G. G., & Selga, E. K. (2022). The transnational data governance problem. Berkeley Tech. LJ, 37, 623.

[4] Aseri, D. A. M. (2020). The implication of the European union's general data protection regulation (GDPR) on the global data privacy. Journal of Theoretical and Applied Information Technology, 98(04).

[5] Bauer, M., & Erixon, F. (2020). Europe's quest for technology sovereignty: Opportunities and pitfalls (No. 02/2020). ECIPE Occasional Paper.

[6] Becher, S., Gerl, A., Meier, B., & Bölz, F. (2020). Big picture on privacy enhancing technologies in e-health: a holistic personal privacy workflow. Information, 11(7), 356.

[7] Bendiek, A., & Römer, M. (2019). Externalizing Europe: the global effects of European data protection. Digital Policy, Regulation and Governance, 21(1), 32-43.

[8] Borges Monroy, I. (2023). Immobilized or petrified? Explaining privacy concerns and the (de) mobilization against mass online surveillance in 21st-century advanced democracies.

[9] Buckley, G., Caulfield, T., & Becker, I. (2022, October). "It may be a pain in the backside but..." Insights into the resilience of business after GDPR. In Proceedings of the 2022 New Security Paradigms Workshop (pp. 21-34).

[10] Burri, M. (2021). Data flows versus data protection: Mapping existing reconciliation models in global trade law. In Law and Economics of Regulation (pp. 129-158). Cham: Springer International Publishing.

[11] Cairney, P., & Wellstead, A. (2021). COVID-19: effective policymaking depends on trust in experts, politicians, and the public. Policy Design and Practice, 4(1), 1-14.

[12] Chander, A., Kaminski, M. E., & McGeveran, W. (2020). Catalyzing privacy law. Minn. L. Rev., 105, 1733.

[13] Cook, M. M. (2021). Bringing Down Big Data: A Call for Federal Data Privacy Legislation. Okla. L. Rev., 74, 733.

[14] Daniel, N. F. (2022). EU Data Governance: Preserving Global Privacy in the Age of Surveillance (Doctoral dissertation, Johns Hopkins University).

[15] de Carvalho, R. M., Del Prete, C., Martin, Y. S., Araujo Rivero, R. M., Önen, M., Schiavo, F. P., ... & Koukovini, M. N. (2020). Protecting citizens' personal data and privacy: Joint effort from GDPR EU cluster research projects. SN Computer Science, 1, 1-16.

[16] Debbarma, R. (2023). The changing landscape of privacy laws in the age of big data and surveillance. Rivista Italiana di Filosofia Analitica Junior, 14(2), 1740-1752.

[17] Dindarian, K. (2023). The Changing Nature of Politics, Globalization and Business. In Embracing the Black Swan: How Resilient Organizations Survive and Thrive in the face of Geopolitical and Macroeconomic Risks (pp. 203-222). Cham: Springer International Publishing.

[18] Dowd, R., & Dowd, R. (2022). Digitized Data Protection as a Fundamental Human Right. The Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU, 27-69.

[19] Getrich, C. M., Rapport, K., Burdette, A., Ortez-Rivera, A., & Umanzor, D. (2019). Navigating a fragmented health care landscape: DACA recipients' shifting access to health care. Social Science & Medicine, 223, 8-15.

[20] Gstrein, O. J., & Zwitter, A. (2021). Extraterritorial application of the GDPR: promoting European values or power?. Internet Policy Review, 10(3).

[21] Hasani, T., Rezania, D., Levallet, N., O'Reilly, N., & Mohammadi, M. (2023). Privacy enhancing technology adoption and its impact on SMEs' performance. International Journal of Engineering Business Management, 15, 18479790231172874.

[22] Höglund, W. (2019). Exporting data protection law. The extraterritorial reach of the GDPR.

[23] 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.

[24] Jafari-Sadeghi, V., Garcia-Perez, A., Candelo, E., & Couturier, J. (2021). Exploring the impact of digital transformation on technology entrepreneurship and technological market expansion: The role of technology readiness, exploration and exploitation. Journal of Business Research, 124, 100-111.

[25] Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. Sensors, 23(21), 8944.

[26] James, E., & Rabbi, F. (2023). Fortifying the IoT Landscape: Strategies to Counter Security Risks in Connected Systems. Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries, 6(1), 32-46.

[27] Jovanovic, S. (2020). Governing the Internet: The Extraterritorial Effects of the General Data Protection Regulation.

[28] Ke, T. T., & Sudhir, K. (2023). Privacy rights and data security: GDPR and personal data markets. Management Science, 69(8), 4389-4412.

[29] 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).

[30] Lamoureux, S. (2020). Implementing the General Data Protection Regulation: The experiences of three Finnish organizations.

[31] Li, Z. S. (2020). Complying with the GDPR in the Context of Continuous Integration (Doctoral dissertation).

[32] Lynskey, O. (2019). Grappling with "data power": normative nudges from data protection and privacy. Theoretical Inquiries in Law, 20(1), 189-220.

[33] Mike, N. (2023). European Privacy by Design (Doctoral dissertation, Budapesti Corvinus Egyetem).

[34] Milch, R. S., Pernice, I., Romanosky, S., von Lewinski, K., Shackelford, S., Rosenzweig, P., ... & Wenger, E. (2019). Building common approaches for cybersecurity and privacy in a globalized world. Available at SSRN 3508933.

[35] Nicola, F. G., & Pollicino, O. (2020). The balkanization of data privacy regulation. W. Va. L. Rev., 123, 61.

[36] Norval, C., Janssen, H., Cobbe, J., & Singh, J. (2021). Data protection and tech startups: The need for attention, support, and scrutiny. Policy & Internet, 13(2), 278-299.

[37] Oldani, I. (2020). Exchanging and Protecting Personal Data across Borders: GDPR Restrictions on International Data Transfer.

[38] Petelka, J., Oreglia, E., Finn, M., & Srinivasan, J. (2022). Generating practices: investigations into the double embedding of GDPR and data access policies. Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2), 1-26.

[39] Polanco, K. (2020). Trimming the Fat: The GDPR as a Model for Cleaning up Our Data Usage. Touro L. Rev., 36, 603.

[40] Politou, E., Alepis, E., Virvou, M., & Patsakis, C. (2022). Privacy and Data Protection Challenges in the Distributed Era (Vol. 26, pp. 1-185). Springer.

[41] Politou, E., Alepis, E., Virvou, M., Patsakis, C., Politou, E., Alepis, E., ... & Patsakis, C. (2022). The "right to be forgotten" in the GDPR: implementation challenges and potential solutions. Privacy and Data Protection Challenges in the Distributed Era, 41-68.

[42] Reinhardt, J. (2022). Realizing the fundamental right to data protection in a digitized society. In Personality and Data Protection Rights on the Internet: Brazilian and German Approaches (pp. 55-68). Cham: Springer International Publishing.

[43] Rubinstein, I. S., & Petkova, B. (2019). Governing privacy in the datafied city. Fordham Urb. LJ, 47, 755.

[44] Ryngaert, C., & Taylor, M. (2020). The GDPR as global data protection regulation?. American Journal of International Law, 114, 5-9.

[45] Sandin, M., & Sjöholm, E. (2023). Are there two sides toevery coin; even GDPR?: A Qualitative Study on theImpact of GDPR within theHealth Tech Industry.

[46] Schade, F. (2023). Dark Sides of Data Transparency: Organized Immaturity After GDPR?. Business Ethics Quarterly, 1-29.

[47] Sivan-Sevilla, I. (2022). Varieties of Enforcement Strategies post-GDPR: A fuzzy-set qualitative comparative analysis (fsQCA) across data protection authorities. Journal of European Public Policy, 1-34.

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

[49] Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices-mobile phones. Procedia Computer Science, 151, 303-312.

[50] Tullis, J. A., & Kar, B. (2021). Where is the provenance? Ethical replicability and reproducibility in GIScience and its critical applications. Annals of the American Association of Geographers, 111(5), 1318-1328.

[51] Van de Waerdt, P. J. (2020). Information asymmetries: recognizing the limits of the GDPR on the data-driven market. Computer Law & Security Review, 38, 105436.

[52] van den Hoven, J., Pozzi, G., Stauch, M., Lishchuk, I., Musiani, F., Domingo-Ferrer, J., ... & Comandè, G. (2022). The European approach to artificial intelligence across geo-political models of digital governance. EasyChair Preprint, 8818.

[53] Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. American Business Law Journal, 56(2), 287-344.

[54] Wu, H., Hao, Y., & Ren, S. (2020). How do environmental regulation and environmental decentralization affect green total factor energy efficiency: Evidence from China. Energy Economics, 91, 104880.

[55] Wu, P. F., Vitak, J., & Zimmer, M. T. (2020). A contextual approach to information privacy research. Journal of the Association for Information Science and Technology, 71(4), 485-490.

[56] Zarsky, T. Z. (2019). Privacy and manipulation in the digital age. Theoretical Inquiries in Law, 20(1), 157-188.