Journal of Theoretical and Applied Information Technology
29th February 2020. Vol.98. No 04

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE IMPLICATION OF THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION (GDPR) ON THE GLOBAL DATA PRIVACY

DR. ABDULAH M. ASERI

Management Information Systems department, College of Business Administration, Imam Abdulrahman Bin Faisal university, P.O Box 1982, Dammam, Saudi Arabia

E-mail: amaseri@iau.edu.sa

ABSTRACT

The study examined the implications of the European Union's General Data Protection Regulations on Global Data Privacy. Based on a qualitative technique, primary data were collected using semi-structured interviews. The thematic method was used in the analysis of the interview transcripts collected from 10 interviewees. The results indicate that the new data protection is effective and could negatively impact companies that fail to comply especially those located outside the EU. The policy in promoting data privacy necessitates a practical methodology in seeking data consent from participants while enforcing the viability of information acquisition and usage through affirmative action. As part of the user-centric initiative, GDPR has developed a sense of tailored accountability while reducing security breaches that impact on business potentials. The requirement for enhancing content-sensitive information by global firms and organizations increases responsibility on organizational compliance with GDPR data policies thereby with the realization of a considerable improvement in data security and privacy. The finding also shows that the GDPR is likely to address most of the privacy issues associated with the development of digital technology in the world. The policy controls the key privacy issues associated with the data collection and management such as the privacy, security, integrity and access among many others. Through the GDPR, the companies will embrace strategies to enhance the rights to be forgotten and the access aspects, hence, addressing the privacy issues.

Keywords: *Data Protection, Privacy, Global, Regulations, Compliance*

1. INTRODUCTION

In recent years, data privacy and security regulations have expanded unprecedentedly across the world as regulators make significant efforts to meet the demands and expectations of the technological advancements. Some jurisdictions are focused on fairness or consumer protection while others are geared toward the concept of privacy as a fundamental right [28]. Therefore, it becomes difficult to apply and interpret the divergent global security regulations and data privacy. Organizations are required to address the issue of data privacy with more seriousness by considering interests of employees, consumers and business necessity and lastly, likelihood and severity of the risk. Majority of countries are making fundamental changes to long-established data privacy laws. Businesses with insufficient data protection practices face high penalties as data privacy regulators continue to step up enforcement [3]. [29] state that major considerations include data residency requirements, excessive collection and processing of perusal data obtained online, requirements for online consent practices and transparency, and data security or incident response practices. As a result, more expansive data breach notification requirements will continue to be adopted by various jurisdictions.

Significant breaches from numerous cybersecurity attacks led to a recent focus on privacy concerns. Countries across the world developed regulations for strengthening consumer privacy protection and the globally recognized is the European Union's (EU's) General Data Protection Regulation (GDPR) [22]. GDPR supersedes the Data Protection Directive 95/46/EC and was implemented to address personal data transfer by giving control of individual citizens over their personal information along with simplification of the international business regulatory environment. According to [30], regulation within the EU was therefore unified.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Data privacy is important to both consumers and organizations. Fundamental rights and freedoms can be damaged due to a breach of personal information. Multiple risks can be experienced due to inadequate protection of personal data, careless processing of information, and any unauthorized collection [18]. Based on GDPR, companies that are failing to comply with the data privacy requirements are at risk of penalties such as fines and lawsuits. Authorities can ban the business from future personal data processing, and the fines can reach 20 million Euros. Therefore, rising global privacy awareness among business enterprises is attributed to severe consequences of non-compliance. According to [19], the number of nations that enacted data privacy laws in 2018 rose to 132 from 120 in 2017 and these regulations cover both the public and private sector. Many countries are endlessly trying to enforce the GDPR together with replacing or updating the existing laws. GDPR is considered the most complex data privacy law that was established in this era whereby the world is experiencing a shift towards more comprehensive legislations. However, there are questions raised on whether GDPR can yield the anticipated outcomes that relate to the regulatory fines as well as actions. Regulators still record an increased number of privacy breaches, issues and complaints [27]. The regulation continues to be implemented in all local privacy laws and since it applies to organizations that sell and store personal information of European citizens, there is a significant impact on global data privacy that need to be addressed adequately. Personal data includes information relating to an individual such as computer IP address, medical information, location details, updates on social networking websites, bank details, an email address, a photo and a name [29]. Therefore, it implies that EU and EEA citizens will have been assured that their information is protected and have greater control of it.

Research Aim and Objectives

The primary of this research is to examine the impact of the EU's GDPR on global data privacy. To achieve this aim, the following study objectives are considered:

1. To explore the business effect of GDPR on international and global organizations
2. To examine whether EU GDPR can address new privacy challenges associated with the development of digital technologies.
3. To examine the effectiveness of the new data protection policy in enhancing global data privacy

Statement of the Problem

The average cost of cybercrime has increased and the new government regulations seek to curb the issues related to data privacy. Companies that were already compliant will imperatively be required to develop effective strategies to ensure the new requirement of GDPR is adequately implemented. To this end, companies that deal with data are required to anonymize collected data to protect privacy, provide data breach notifications, seek the consent of subjects for data processing, safely handle the transfer of data across borders, and appoint data protection officer to oversee GDPR compliance. As noted by [26], the main reasons for the introduction of these regulations are to enhance conformity of data security law across the EU members. As a consequence, all companies that market their products and services to EU residents are subject to these policies regardless of the location. Large corporations and small and medium-sized enterprises are equally required to comply with these policies to avoid fines or penalties associated with the potential breach. Hoofnagle, [21] established that the GDPR is the most consequential regulation to have been developed in the information policy in contemporary society. As a result, there is a need for examining key aspects that will be considered by companies when developing information governance frameworks for in-house data and the one shared by customers. With the new developments, there is a need to explore strategic implications on companies both in the EU and outside Europe. To address these issues, this research focused on the effectiveness of the new regulations in enhancing global data protection and impacts on global organizations.

2. LITERATURE REVIEW

[19] note that GDPR demands companies to implement substantial data protection safeguards. These regulations could bring about new challenges as well as opportunities globally. Since most organizations are not prepared for compliance, it is paramount for companies to make changes to minimize liability. However, one of the major concerns of this research was to examine strategies that should be employed by firms to address the challenges and opportunities related to compliance with GDPR which were not provided by [19]. [4] proposed that technology companies that target

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

global markets need to develop effective strategies to secure their products and services, systems, and data for compliance with GDPR. Despite recommending that firms should improve their efforts for compliance, the findings of [4] was limited by the lack of information concerning the cost of meeting the requirements. According to [17], the main data protection principles in the new GDPR include data minimization, fairness and lawfulness, storage limitation, integrity and confidentiality, and purpose limitation. Although the regulations intended to affect EU citizens, its impacts would be experienced among companies that target UK customers regardless of their locations. High requirements are put on data processors and controllers to ensure all GDPR principles are complied with. For instance, organizations must implement appropriate technical measures that get user consent regarding their data.

The new GDPR was an extension of the previous data protection policy which was enhanced to reaffirm the protection of fundamental rights and freedom. A study by [8] revealed that the goals of GDPR are to reduce legal fragmentation, uncertainties and complexities that existed between EU members. Companies should leverage these changes to achieve sustainability of the data protection strategies. Again, compliance with GDPR will enable companies to preserve the equilibrium between protecting data subject rights and globalized world. Similar to [17,4], the study of [8] was limited by insufficient information on the challenges that will be experienced by firms while implementing these policies. [7] revealed that GDPR intends to replace the current data protection directive and would harmonize and modernize across the EU. With the consistent change in the regulatory environment, the role and use of data in the economy is also expected to be altered. Compliance with GDPR is fundamental for companies to participate in the single market. Accordingly, variations in the implementation of these legislations might affect a firm's capability to host data in the EU countries. However, [27] argued that the right to be forgotten and the right to withdraw consent has caused a prolonged controversy among scholars and human rights advocates regarding its implication on personal data. The author notes that enforcement of GDPR principles is feasible provided effective strategies are put forth by companies to enhance compliance. Therefore, the regulations will strengthen the well-established data protection principles as well as create technical difficulties for the implementation and integration of the requirements into data computing infrastructure.

GDPR has diversely impacted countries, organizations, governments and individuals in both positive and negative ways, thus increased attention from scholars to understand its impacts from a global perspective. [15] generally assessed the implications of GDPR and the progress of installing compliance measures among small to medium-sized enterprises in Romania. According to GDPR, collection and analysis of personal data must comply with the principles outlined in GDPR Art 4. Failure to do so attracts different forms of punishments such as financial damages and sanctions, including outrageous penalties up to 4% of global turnover (€ 20 million). Most firms are yet to install GDPR policy in their operations, citing challenges such as lack of practical guides, increased bureaucratic effort, GDPR complexity, increased consulting costs and lack of systematic information campaigns [15]. The study argues that the successful installation of GDPR hinges on the development of concrete application guides, conducting broad information campaigns as well as the provision of free GDPR training courses. Comparatively, [11] also conducted a study on the impacts of the EU's general data protection program, albeit from the perspective of global developing economies. She argues that supported third-party obligations will enable the EU's general data protection policy to export privacy norms. Conversely, developing economies around the world should implement a co-regulatory industry approach to protecting clients' data before implementing similar national legislation. Findings further indicate that the EU's GDPR policy may be the perfect framework for harmonizing privacy laws on a global scale, specifically for use among willing participants and economic sectors. As such, growing economies should enhance their legal systems and GDPR education programs to capture the merits of the thriving e-commerce sector which will be influenced by GDPR [11]. Similar to [15], the study of [11] notes that emerging economies should be wary of GDPR challenges such as technical inferiority, ineffective judicial regimes and risk of exploitation in their quest to adopt GDPR policy. Despite these positives, the two studies did not conduct quantitative data analyses to support their allegations.

Despite GDPR being influential in protecting the privacy of client and employee data, some researchers argue that the framework alone cannot guarantee optimal data privacy. [23]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

conducted a systematic study to reveal insights on the significance of standardization as an aspect of co-regulation from a data protection standpoint. The study argues that laws such as GDPR policy are necessary but insufficient in protection individuals' data. Consequently, it should be supplemented with other policy instruments and installed within a policy network. These policy instruments comprise privacy impact analyses, codes of conduct, privacy seals and privacy standards. For organizations to ascertain that self-regulatory strategies safeguard information rights of subjects such as shareholders, workers and customers, regulatory oversight is mandatory. Moreover, data management and supervision should not influence the independence of self- regulatory bodies but strive to ensure that self-regulatory tools facilitate the protection of individuals' data privacy. Besides instruments, institutions such as the International Federation of Library have started conducting GDPR sensitization as well as offering guidance on the adoption of the policy. In his systematic review of GDPR adoption, [12] notes that institutions such as libraries should safely store written records which describe the intentions for using personal information, types of personal data stored in their systems, stipulated time limit for deleting clients' personal information as well as technical organizational strategies for protecting client information. Global organizations, governments as well as social institutions should possess the legal obligation to collect, analyse, arrange, communicate and archive personal records for the general public interest. According to IFLA, international community and information professionals should fully understand the legacy and implications of GDPR within their respective countries apart from ensuring clienteles' data safety to create a better societal norm [12].

The investment climate for conducting high tech business is becoming difficult because of the change of the legal environment. In regards to this, [1] found that institutional and regulatory measures aimed at transforming the digital economy and moving entrepreneurship into the path of steady growth could adversely affect performance if respective organizations fail to develop and implement compliance strategies. Although [1] focused on digital transformations among companies, its results cannot be generalized across all companies because the context examined the challenges small and medium-sized firms are facing due to digital transformations. As noted by [20], digital technologies are transforming products, services, and operations in both small and large organizations. As a consequence, management is required to employ decision support guides to provide insights on how to address potential challenges. However, both the findings by [20,1] did not provide the link between challenges associated with digital transformations and implementation of GDPR. For that matter, [5] explored the extent firm uses big data analytics and internet of things to develop solutions for their business models. The results showed that digital technologies are affecting every aspect of the business which needs the development of effective regulations to prevent a breach of data.

A report by the Congressional Research Service indicates that technological convergence may present a wide range of issues that requires the government to develop effective measures to oversight actions [10]. Accordingly, network and technological convergence executes multiple functions as well as collects and use information in various formats which need to be governed by specific regulations to enhance data security. Technological convergence uses and collects personal data which raises privacy concerns. Before developing the new GDPR, there have been varied provisions regarding data and privacy among countries across the world. Nevertheless, there is a great gap in the knowledge regarding the impacts of these policies on businesses that deal with customer's customer because of the unification of the policies among the EU members. As technology continues to mediate the role of identity verification, the policies expose the business to operational challenges since they are required to develop effective infrastructure to enhance compliance with data protection and privacy issues. According to [24, 25] most businesses are currently embracing e-commerce as a method for improving their performance; hence creating the need for improving security and data privacy issues. Therefore, there is a gap regarding the impacts of the GDPR on the global organizations, the effectiveness of the policy, and measures organizations need to embrace to address new challenges.

3.0 RESEARCH METHODOLOGY

The research methodology chapter describes the assumptions considered during the collection and analysis of data. Following these strategies fundamentally helped in ensuring reliable information was collected based on the research questions and objectives. In this case, the assumptions were based on a qualitative method

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

that entails in-depth data from an individual's perceptions, opinion, and knowledge regarding the research phenomenon. Therefore, the main sections include the research method, research philosophy, data collection, data analysis, ethical concerns, and limitations.

3.1 Research Philosophy

The research philosophy involves the assumptions and strategies that are employed during the research process to ensure research objectives are accurately accomplished. For this reason, the pragmatic philosophy was used; which postulates that knowledge is inseparable from the agency within it as well as identification of the potential impacts of the regulation on global enterprises. According to [14], pragmatism philosophy centres around the concepts of inquiry and knowledge which eventually enhance the provision of a rich account of the research phenomenon. Although [6] established that pragmatism philosophy does not consider the interest of the stakeholders, the approach was preferred since it enhanced in-depth exploration of the research phenomenon. Additionally, an inductive approach was embraced which allowed identification of themes and patterns from the interview transcripts. Consequently, reliable results were developed based on the researcher perspective, existing knowledge, and opinions from the interviewees.

3.2 Research Method

The qualitative method was adopted which entails the collection of data from individuals. The qualitative technique is a naturalistic enquiry that relies on the direct experiences of people regarding the research phenomenon [9]. Therefore, the methods allowed understanding of individual's perceptions concerning the effect of GDPR on international and global organizations, the capability of the new frameworks in addressing privacy challenges attributed to the frequent change in digital technologies, and effectiveness of the new protection policy in enhancing global data policy. Since limited studies have explored this phenomenon, a qualitative method was most suitable in gaining an in-depth understanding of the potential impacts of the new policy.

3.4 Data Collection Process

A purposeful sampling method was employed to ensure individuals with a profound understanding of the previous and current data privacy regulations. According to [16], purposeful sampling allows the selection of individuals who have the knowledge and available to offer their opinion and perceptions concerning the research problem. Since purposeful sampling is susceptible to biases, priority was given to participants who met various factors, particularly willingness, availability, and understanding of the research problem. There was a challenge in identifying the quality and accuracy of the information responses provided by participants; thus, this measurement problem was addressed by ensuring only consistent data were used in the results. The participants were also requested to provide honest and accurate information to enhance quality of the data. For instance, the interviewer offered clarifications of various questions to ensure they understood appropriate responses that were expected.

Key parameters that were considered while selecting participants include their willingness to take part in the research, availability, and understanding of the data protection and privacy policy. To this end, 10 people selected based on the purposeful sampling were subjected to semi-structured interviews. Moreover, 4 people were female while 6 were male while the age for all participants ranged from 25 to 65. The level of education and other factors were considered during the selection. In overall, these factors were considered to ensure people with a deeper understanding of the research phenomenon participated in the research.

The interview questions were designed based on the research questions, objectives, and the existing studies to ensure the questioner and phenomenon was accurately designed and adequately addressed respectively. Moreover, the researcher ensured all the selected participants had substantial knowledge on implementation of GDPR standards.

The primary data were collected using a one-on-one interview. Before the interviews, participants were requested to fill consent form detailing the reasons why they were requested to participate in the research, objectives of the study, measures put forth to enhance their confidentiality, and importance of taking part in the study. Interviews were preferred against other forms because it offers the opportunity to create a strong rapport which ultimately influences interviewees to give honest and accurate information based on their knowledge and experience. A study by [31] revealed that interviews are the most suitable

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

approach for collecting qualitative data since it offers the opportunity for both interviewer and interviewee to seek clarification on any unclear issue. Consequently, more accurate and reliable information is collected regarding the research problem. For instance, the researcher severally requested to clarify their opinion and perception of the potential strategies that should be employed to enhance compliance with the new regulations. The interview consisted of 10 semi-structured questions and took between 10-15 minutes for every session. Essentially, individuals were only required to provide a short answer to the question or skip if they were not sure. During the interview process, the main answers were recorded and analysed as described in the following section.

3.5 Data Analysis

The thematic method was used to analyse the collected data. The technique entailed the identification of patterns and themes from the gathered data. According to Clarke and Braun (2013), the thematic method is most suitable in analysing the qualitative data because of flexibility which allows the researcher to base on the research questions, existing theory, and individuals opinion and perception in developing the findings. Following [2] recommendations, the flexibility aspect associated with the thematic approach inherently ensures suitable themes and patterns are selected from the interview transcripts. The main interests in the study involved exploring the effects of GDPR on international and global organizations, challenges associated with the new policies, and strategies that data handling firm's needs to embrace to address potential security and privacy issues. Considering limited information existing concerning the implications of GDPR, the selection of themes and patterns were based on the repetitiveness of the information and its relation to the research problem. Following the netx steps prevented potential anomalies that could affect the credibility of the data. Therefore, the analysis of the primary data was based on the six steps:

Step 1: Familiarization with Data

The primary activities in this step involved reading and re-reading of the notes to gain an understanding of every concept and its relatedness with the research questions. The step is crucial since it creates an earlier impression concerning the research phenomenon. Since every respondent's provided personal perception and opinion concerning the implementation of GDPR, reading of the responses provided insights on relevancy and appropriateness of the data concerning the research questions.

Step 2: Generating Initial Codes

In this stage, the data was organised systematically. For instance, all responses showing a common pattern were put in the same column, guided by research questions. Each segment of data was coded and significant to the research problem. Besides, familiarization provided some insights concerning potential codes and themes; hence, words that had some implication on the research questions were identified as codes. After all data had been coded, they were modified based on the study objectives before moving on searching for themes.

Step 3: Searching for Themes

Themes and patterns were selected based on their significance and relation with the research problem. For that matter, themes were identified from the initial codes, where terms and concepts related to GDPR were examined and modified from the step before being identified as major themes.

Step 4, 5, and 6: Review of Themes, Definition of Themes, and Writing-up

The selected themes from step 4 were reviewed and modified to ensure they accurately answer the research phenomenon. Some of the key factors considered to ensure only relevant themes were identified includes how they supported the data, meaning, overlapping, and within the data. After review and definition, only 3 themes remained and were used for the write-up as indicated in the following chapter.

3.6 Ethical Considerations

The data analysis and collection process were subject to ethical principles such as confidentiality, informed consent, and anonymity to ensure credible and reliable results were developed. Regarding confidentiality, the collected data were not shared by third parties or accessed by unauthorised individuals. After the analysis, all the primary data were destroyed to ensure it could not be accessible by any person who was not part of the research. Additionally, anonymity was enhanced through ensuring names of the interviewees or any information that could reveal their identity wasnot written anywhere. As a result, only the researcher was familiar with their identity. In this study, their

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

names were anonymized in letters including respondent R1, R2, and others. After the selection of the respondents using the non-probability method, they were provided with consent form detailing the importance and objectives of the study. As a consequence, all the participants had an understanding of the implication of the research before signing the consent form. Individuals were also informed about their right of withdrawal during the research process since participation was voluntary.

3.7 Study Limitation

Although credible and reliable results were formulated, this study is limited by relying on people perception and opinion in developing the findings. For this reason, some respondents might have provided information that best suited their expectations. To address this limitation, individuals were given clarifications on every question and were further requested not to attempt those that they had insufficient knowledge. Moreover, the interviewer created rapport with the participants; and this influenced them to provide a more honest opinion regarding the research problem.

4.0 RESEARCH ANALYSIS, DISCUSSION AND VALIDATION

This chapter describes the findings from the thematic analysis of qualitative data. The identified themes are presented in details and further related to existing studies on data protection and privacy issues.

4.1 Impact of GDPR on International and Global Organizations The GDPR demands that all the business operators within the EU must comply with the regulation. Some of the important personal information advocated for the control by the owners includes the names, photos, email address, social networking websites, bank details and location details among many others. According to R1 and 2, GDPR will increase an organization's liability in maintaining data privacy. "*Organizations will be more liable in ensuring the privacy of clients is maintained*". As such, companies will be required to develop appropriate strategies to enhance compliance with new data protection principles. Besides, R3, R6 and R 5 argued that customer trust towards organizations that fail comply with the policies will decline. Lack of trust will negatively affect the performance of companies. "*I believe compliance is imperative irrespective of the location. Lack of compliance will raise ethical issues*". Essentially, customer trust is essential in the digital economy as it is valued by clients for continued business activities. Organizations are compelled to ensure that the owners of the data have the right to access this information, right to be forgotten, correction, portability, right to be informed and notification among many others. Therefore, the results indicate that some of the global firms will focus their attention to non-EU members such as Asia, the USA, and emerging markets. In regards to this, R4 stated that companies are turning to other countries that are not members of the EU block. "*Recently, multinationals are focusing on emerging markets since the regulations are not meant to be implemented globally. However, with the EU countries being one of the economic and trading hubs in the world, companies will be forced to acquire relevant infrastructure to enhance compliance*".

The new policy will force global firms to enforce new approaches of data collection, processing, storage and distribution, ensuring that each of the steps meets the expectations of the GDPR. The companies tend to collect the information on individuals, customers, prospects, employees and the contractors among many others. In regards to this, R7 stated that organizations will be forced to change their strategy that is used towards the collection and the management of the information involved. "*There will be a change in strategy and acquire technology that promotes compliance. As a step towards the enhancing compliance with the GDPR policy, every company must employ a data protection officer, concerned with the roles of ensuring that the business complies with GDPR*". The appointed officers will review and control the workflows of the business to ascertain that collection, storage and distribution of the personal data meets the conditions of the policy.

According to R9 and R10, the policy has a strong magnitude on the operations of global firms because failure to comply with the policy leads to penalties and fines imposed on the annual revenues collected. "*The GDPR will significantly impact the customer engagement levels within the business operations, affecting the management of the marketing activities and the general strategies involved in the customer engagement activities"*. Communication with the stakeholders and partners is important for the wellbeing of every organization, hence, the GDPR will impose strong forces of the rules to the traditional running of the process because there will be a need to prove consent and other related aspects.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. GDPR in Fostering Data Privacy

The GDPR is likely to address most of the privacy issues associated with the development of digital technology in the world. Thus, R1, R3 and R5 stated that the policy controls the key privacy issues associated with the data collection and management such as the privacy, security, integrity and access among many others. As a consequence, the current challenges associated with data will be significantly reduced. "*With the change in policy, various weaknesses that led to the access to individual's data shall be addressed*". Through the GDPR, the companies will embrace strategies to enhance the rights to be forgotten and the access aspects, hence, addressing the privacy issues. Besides, R7 stated that GDPR policy is more effective because all the personal information collected through the different methods in the process of delivering goods or services to the customers is handled properly. "*Most of the privacy issues emanating from the digital technologies are closely tied to the improper handling of the data in the media*". The GDPR ensures that the technologies are designed and adopted in a way that protects the data collection process, storage, processing and distribution. According to R8, the user or data owner is closely involved in the process of data flow and usage, hence, robust in controlling the privacy challenges. "*Close involvement of the owner will fundamentally enhance compliance and effectiveness of the data protection policy. The investment into the manpower for the management of data as demanded by the GDPR ensures that the data privacy aspects are addressed because of the increased compliance*". R10 stated that the introduction of every digital technology must be accompanied by proper management of data through the expert skills, hence, the storage and processes are handled appropriately. "*Some of the key aspects include the consent of data, anonymity in data collection, notifications upon data breach, safety in data transfer and other related aspects that ensure that data is protected*". Therefore, data protection measures are enforced on new technological innovations.

4.3 Effectiveness of GDPR in enhancing Privacy

GDPR's new data protection policy has focused on initiating a continuous process of developing improvement measures across global organizations in pursuing data privacy. According to R4, the EU's GDPR is a critical initiative in promoting the sustainability of consumer data utilization across different platforms. "*The policy is sustainable and is more effective than the previous data protection regulations*". The new data policy has potentially reduced the international data protection conflicts that often arise among firms. Therefore, R7 and R8 argued that GDPR through various articles has focused on initiating a proactive perspective and approach in developing resilience towards the digital data challenges that impact on information security and privacy. "*There has been a potential of improving the rights of privacy for individuals while also promoting the cognizance of the influence of state and local actors in organizations*". As such, the EU's GDPR in its initiative to enforce data privacy has redesigned the organizational use and acquisition of redundant consumer data while restraining potentially unauthorized usage thereby reducing consumer litigation in firms relating to data privacy infringements.

Moreover, information privacy as a modern concept with the rise of digital technologies has necessitated the regulation of global and local organizational practices. In light of this R9 and 10 stated that through the EU's GDPR, there has been a consistent global standardization of procedures in organizational management of consumer digital data. "*The GDPR is a combination of various data policy practices aimed at harmonizing global data usage and transfers"*. The GDPR takes into consideration various EU directives in the provision of a multifaceted policy instrument for adoption and implementation across various organizations.

4.4 Discussion and Validation

The EU GDPR highlights the need for protecting people's data held by organizations in the global economies. While the international marketplace offers multinational firm opportunities for growth and potential success, the European's Union General Data Protection Regulation (GDPR) is set to impact the business operations. First, the EU's GDPR will impact the organizational acquisition of collection, storage, and usage of data for their growth prospects. This finding is in tandem with [4] who established that GDPR standards will affect various practices in the organisation which entail collection and sharing of information. Therefore, the finding helped to overcome the shortfall of the gap in knowledge regarding measures that need to be employed by global firms to enhance compliance as well as create customer trust and loyalty.

Global firms gather consumer and market data intending to implement and integrate the best

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

industry approaches for gaining competitive advantage [17]. GDPR's business effect implies that global and international organizations will need to seek consumer consent before obtaining private information. Second, global and international businesses will have limited control over information at their disposal while complying with the host state's laws and regulations regarding data protection. Despite the acquisition of consumer information, multinational firms will need to consistently endeavour to improve their data management and utilization for business purposes.

The digital technology revolution is necessitating the adoption of process automation and digitization of organizational information and transfer across different states. Many organizations are developing and aligning their business models in line with the EU GDPR data privacy requirements [15]. Many European authorizes have focused on implementing the data laws across their states to ensure that global and international organizations institute frameworks for handling consumer information and data while guaranteeing privacy. Data and information transfers across trans-borders in organizations have often generated the discrepancies in the data usage and potential manipulation of consumer data [20]. The GDPR data policy in its assertions attempts to harmonize privacy rules across different nations. Through similar operational standards in data management, it is possible to improve the viability and protection of data in global and international firms adopting digital technologies in their operations across the EU region. Therefore, these results are consistent with [11,5,7,23] which established that these changes will offer firms competitive advantage over global firms as well as enhance customer confidence. Therefore, these findings helped to overcome the perception that implementation of GDPR standards will have a negative impact on global companies.

The EU GDPR has considered varied perspectives in global data management thereby providing a comprehensive document for pursuant. The European Commission in their research asserts the effectiveness of GDPR towards improving consumer confidence while offering firms a competitive advantage over global firms across foreign markets [11].

5.0 CONCLUSION

The study examined the implication of the European Union General Data Protection Regulation on the global data policy. Consumers through the legislation have a right to examine the information stored by the global organizations while having the opportunity to withdraw consent relating to information held by global and international organizations. Multinational organizations will need to express interest in the collection of consumer data while highlighting their identities and rationale for possessing the information. GDPR necessitates restricted data handling and possession of people's data while highlighting the appropriate mechanisms for data protection and disposal after a specific period. Given the rising cases of cybersecurity, data privacy is a critical aspect of the GDPR implementation and adoption for global firms and organizations. Through a regulated approach in the data handling procedures, the GDPR has a business influence of necessitating a proactive approach in the management of consumer data. Besides, GDPR necessitates multinational firms to limit data transfers across different platforms while ensuring they undertake to critically design information systems as a priority in enhancing consumer protection. Therefore, GDPR has a cumulative effect of enforcing multinational business compliance with local state laws and EU consumer data and security protection in light of the digital challenges.

Limitation of the Study

The findings revealed that every organization that serves customers in the EU region must adhere to these policies to avoid breaching the GDPR policy. Although the study provides credible results, the findings are limited by the use of a small population sample. In regards to this, the primary data were collected from 10 individuals who; however, do not represent the entire UK members. Therefore, increasing the population sample would enhance the breadth of the study. Moreover, the results of the study provide insights to management and companies that process and deal with customer data; hence, limiting its scope.

7. 0 RECOMMENDATIONS

The rapid technological development and globalization require companies that collect and process customer information to develop effective strategies that enhance compliance with GDPR framework. Implementation of these policies will inherently improve data privacy of the customers; hence, increasing the trust with the company. Customer data protection and privacy are fundamental in the contemporary business environment, thus researchers need to further

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

explore the concept to unveil the role regulations need to employ to ensure businesses are not affected during the implementation process. The authorities should also develop and implement common training programs to educate organizations on the importance of compliance and measures that are needed to ensure implementation does not negatively affect their operations.

The research contributes to the existing knowledge regarding the impacts of GDPR on global organizations. This study provides insights about the potential methods GDPR will impact global organizations especially those that deal with client's data but are located outside the UK region. As a consequence, firms will leverage on the findings to enact effective strategies that enhance compliance. This study has made a greater improvement over the current knowledge that limited on the meaning of the policy and key considerations for compliance.

REFERENCES

[1] Afonasova, M.A. Digital Transformation of the Entrepreneurship: Challenges and Prospects**.** Journal of Entrepreneurship Education, 2018, 21(2):

[2] Alholjailan, M.I. Thematic Analysis: A critical review of its process and evaluation. *West East Journal of*

Social Sciences,2012, **1**(1): 39-47.

[3] Atikcan, E.Ö. and Chalmers, A.W. Choosing lobbying sides: the General Data Protection Regulation of the European Union. *Journal of Public Policy*, 2019, *39*(4): 543-564.

[4] Beacham, J. Is your practice GDPR ready? *In Practice*, 2018, 40(3):124–125.

[5] Bressanelli, G., Adrodegari, F., Perona, M., and Saccani, N. The role of digital technologies to overcome Circular Economy challenges in PSS Business Models: an exploratory case study. Procedia CIRP, 2018, 73: 216-221.

[6] Bryman, A. *Social research methods*. Oxford: Oxford university press, 2016.

[7] Burri, M., and Schar, R., 2016. The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy*, 2016, 6 (20): 479-511.

Chassang, G. The impact of the EU general data protection regulation on scientific research. Cancer Medical Science, 2017, 11: 709.

[8] Clarke, V. and Braun, V. Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist*, 2013,**26**(2): 120-123.

[9] Creswell, J.W and Plano Clark, V.L. Designing and conducting mixed methods research. Thousand Oaks, California: BMJ Publishing Group, 2011.

[10] CRS Report. Technological Convergence: Regulatory, Digital Privacy, and Data Security Issues. Congressional Research Service, 2019.

[11] Curtiss, T.Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies. *Washington Journal of Law, Technology & Arts, 2016, 12*(1), pp. 1-28.

[12] Das, A.K.European Union's General Data Protection Regulation: A brief overview. *Annals of Library and Information Studies, 2018, 65:*139-140.

[13] Dove, Edward. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law, Medicine & Ethics. 2018, **46**(4):1013-1030.

[14] Dudovskiy. Research Methodology. https://research-methodology.net/Business Economics, 2019, **8**(1): 17-25.

[15] Elena, S.C., Gabriela, G., and Alina, M.C. The EU General Data Protection Regulation Implications for Romanian Small and Medium-Sized Enterprises. *Economic Sciences Series, 2018, **18***(1): 88-91.

[16] Etikan, I., Musa, S.A. and Alkassim, R.S. Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, 2016, **5**(1):1

[17] Goddard, M. The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. International Journal of Market Research, 2017, 59(6): 703-705.

[18] Gruschka, N., Mavroeidis, V.,Vishi, K. and Jensen, M. Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. 2018.

[19] He, L, Lu Y. and Wu H. The Impact of GDPR on Global Technology Development, Journal of Global Information Technology Management, 2019**,** **22**(1): 1-6.

[20] Heavin, C. and Power, T.J. Challenges for digital transformation – towards a conceptual decision support guide for managers. Journal of Decision Systems, 2018, **27**(1): 38-45.

[21] Hoofnagle, J.C., Van der Sloot, B. and Borgesius, F.Z. The European Union general

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

data protection regulation: what it is and what it means. Information and Communication Technology Law, 2019, **28**(1): 65-98.

[22] Houser, K. and Voss, W. GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?. SSRN Electronic Journal. 2018.

[23] Kamara, I. Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation 'mandate'. *European Journal of Law and Technology, 2017,* ***8***(1): 1-24.

[24] Khrais, L.T., et al. A Readiness Evaluation of Applying e-Government inthe Society: Shall Citizens begin to Use it?, 2019, 10(9):55-59.

[25] Mahmoud, A.M et al. Privacy Issues in E-Commerce. Journal of theoretical and Applied information

Technology, 2019, **97**(13): 3718-3727.

[26] Palmer, D. GDPR: How Europe's digital privacy rules have changed everything. 2019, https://www.zdnet.com/article/gdpr-how-europes-digital-privacy-rules-have-changed-everything/

[27] Politou, E., Alepis, E., &Patsakis, C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of Cybersecurity, 2018, 4(1): tyy001.

[28] Rustad, M.L. and Koenig, T.H. Towards a Global Data Privacy Standard. *Florida Law Review*, 2018, *71*: 18-16.

[29] Tankard, C. What the GDPR means for businesses. *Network Security*, *2016*(6): 5-8.

[30] Voigt, P. and Von demBussche, A.. The EU general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing, 2017.

[31] Young, J.C., Rose, D.C., Mumby, H.S., Benitez-Capistros, F., Derrick, C.J., Finch, T., Garcia, C., Home, C., Marwaha, E., Morgans, C. and Parkinson, S. A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution*, 2018, ***9***(1):10-19.