Challenges Faced by the EU and US Technology Companies Before and After GDPR Implementation: A Systematic Literature Review

[1] Victoriano Travieso Morales, [2] Yelena V. Smirnova
[1] Geneva Business School, [2] GBSB Global Business School
[1] vtravieso@gbsge.com,[2] elena.smirnova.sd@gmail.com

Abstract — This paper aims to explore the influence and the key challenges of GDPR implementation on EU and US technology companies before and after coming into force. A systematic literature review was conducted by following a strict protocol, where 47 documents were found relevant to perform the review and to answer to the proposed research questions. The key challenges of GDPR implementation on EU and US companies before and after coming into force include the complexity, extension and subjectivity of the regulation, the costs for the implementation and for the running of the company, the organization's lack of awareness and or expertise on data privacy, the little support from authorities and the lack of practical guidelines. On the other hand, the influence of GDPR has a more negative effect on start-ups and SMEs than on large enterprises. In this research the enablers and benefits of being GDPR compliant were not considered as well as the practical outcomes. An international study might give insights into the topic. Further research is needed to study not only the negative effect on key challenges, but also the positive effects of the GDPR on EU and US companies of all sizes. Based on the literature, the identified key challenges and effect of GDPR implementation on EU and US companies before and after coming into force may be useful for the governments to take measures to support companies with challenges of implementing GDPR and for the organisations to be careful to avoid mistakes and pitfalls throughout the implementation process.

Index Terms— ***challenges, GDPR implementation, tech start-ups, SMEs, EU, USA.***

I. INTRODUCTION

The evolution of technology has enabled the increase of collection, process and storage of large amounts of personal data [1]. The right to the protection of personal data is a fundamental human right recognized under the Charter of Fundamental Rights of the European Union [2].

The digital revolution and the increasing collection of personal data by organisations have acquired security challenges and risks [3]. As described in the AI Index 2019 Annual Report [4], artificial intelligence ("AI") has advanced rapidly over the past decade. Many scholars believe that AI has the potential to boost human productivity and economic growth [5]. Scholars also worry that these gains may come at a cost, potentially including labour displacement, income inequality and loss of privacy. AI algorithms rely on lots of data, often including data on individuals. To protect consumers' privacy, the European Union's General Data Protection Regulation ("GDPR") has been adopted [6].

Poritskiy et al. (2019) states that the protection of personal data, whether in its physical or digital dimension, will require organisations to reinforce protection measures [7]. This will impose a significant effort on organisations, independently of their size, in monitoring and controlling the flow of personal data and in increasing the level of alert to potential privacy risks. Tikkinen-Piri et al. (2018) claim that GDPR will demand substantial financial and human resources, and it will also be necessary to offer adequate training to employees to deal with the GDPR requirements [8].

Other studies carried out by [9; 10] indicate that the GDPR implementation process and the challenges faced by companies are different depending on the size of the companies, particularly for small and medium enterprises (SMEs). For SMEs with limited resources and information management system, this means a great deal of work, so there is a need for a structured approach to make sure they do not miss anything [11; 12].

Study carried out by [7] indicate that there is no doubt that all sectors of activity need to know and apply the GDPR. However, the technological companies are one of the most affected one since they must apply not only the rules set out in the GDPR in the processing of personal data but also develop technological solutions that comply with the rules stated by the GDPR. Despite the importance of the GDPR for technological companies specially SMEs and tech start-ups no previous studies were done, and this is something that needs to be explored.

It is important to consider that this research focuses on the implementation of GDPR in organisations in general, but with an emphasis on tech companies in the EU and the US. A systematic literature review was conducted to identify the key challenges of GDPR implementation on EU and US companies before and after coming into force as well as the influence of GDPR implementation on EU and US companies after coming into force.

II. RESEARCH METHODOLOGY

A systematic literature review (SLR) is employed to identify, analyse, and interpret all available evidence regarding a specific topic or question, to use a trustworthy, rigorous and auditable methodology, to synthesize the existing work in a systematic, comprehensive and unbiased manner [13]. The research methodology is based on [13], complemented by [14], and it contains the following steps:

Planning: identify the need and motivation for the review, specify the research questions that will be addressed and answered by the review and design a review protocol by defining the necessary review procedures.

Conducting: apply the review protocol previously designed to obtain studies which will be the object of the review; and

Reporting: summarize the extracted data from the selected studies to report the findings.

The SLR as the research methodology was chosen to summarize the existing evidence regarding GDPR management key challenges, and the influence of the implementation of the GDPR on EU and US companies with emphasis on tech start-ups and SMEs, to answer to the proposed research questions.

III. Theoretical background

A. General Data Protection Regulation

The GDPR intends to establish uniform criteria for all the EU member states on data protection and introduces major changes regarding personal data and privacy, replacing a repealing the EU's 1995 Data Protection Directive [15].

GDPR became mandatory on the 25th May 2018 after a two year transitional period [16]. The evolution of technology has favoured the increasing collection of personal data and a balance must be found between economic and customer data privacy. The globalization and rapid technological change have enabled citizens to easily share, sometimes without having their explicit prior consent, data about their behaviour and preferences and often this information becomes globally accessible to other organizations [7]. The studies conducted by [17] and [18] indicate that the increase of big data tools allows a cross-analysis of personal data and most mobile applications require access to a considerably high amount of personal data. Being many of those mobile applications free to download users may still be paying with their personal data.

GDPR aims to provide more control to citizens over their data, strengthening their rights, to reform how organizations view and control these data and to remove obstacles to cross-border trades, enabling more natural expansion of businesses across Europe, as well as ensuring the free movement of personal data between EU member states [19]. The GDPR aims to provide trust in the digital economy and harmonize data protection throughout the EU, according to the Digital Single Market strategy [20].

B. General Data Protection Regulation Implementation

GDPR gives rise to many discussions and controversy in many businesses. Studies conducted by [21] indicate that organisations especially were frightened about the consequences – large fines – if they will not follow the GDRP procedures. Further GDRP regulation made a kind of irritation and negative motivation to be requested to do more procedures. It was felt by managers and employees like extra frictions to the business and its business models – especially on value chain function dimensions. As indicated by [21], the business's most significant challenge might be implementing the GDPR in practice – especially for the SMEs and that the implementation of the GDPR requires comprehensive changes to the businesses practice – especially for businesses that had not implemented a comparable level of privacy before the regulation. Several businesses lacked privacy experts and knowledge and new requirements on personal data protection and handling. Therefore, more of the business studied a strong need for education in data protection and privacy. However, many businesses did not have extra resources to use on this issue – although they saw it as a critical factor for meeting the new GDPR demands. A different interpretation of the GDPR inside the businesses (managers and employees) and outside the businesses (customers, network- partners, e.g.) lead to very different levels of GDPR solutions and privacy handling.

Studies carried out by [9; 10] indicate that the GDPR implementation process and the challenges faced by companies are different depending on the size of the companies, particularly for SMEs.

IV. Planning the Review

This section corresponds to the first step of the SLR methodology. It begins by providing the motivation of this paper, followed by the research questions aim to address and answer with the research. Finally, a review protocol is proposed.

A. Motivation

The GDPR has come to stay and has brought an important set of legal, technological and functional changes which have a major effect on all organisations [1] since in order to comply with the regulation they have to carry out major management changes [22].

However, GDPR is a complex and extensive regulation that does not provide specific and clear guidelines regarding the technologies to be used to comply with what is required [19]. Moreover, there is little support from authorities and a lack of practical guidelines.

Therefore, this research aims to obtain information regarding GDPR implementation key challenges and their influence.

B. Research Questions

The research and analysis are based on RQ1 and RQ2, as presented below:

RQ1. What are the key challenges of GDPR implementation on EU and US companies?

RQ2. What is the influence of GDPR implementation on EU and US companies after coming into force?

Moreover, RQ1 can be further detailed into two sub-questions:

RQ1.1. What are the key challenges of GDPR implementation on EU and US companies before coming into force?

RQ1.2. What are the key challenges of GDPR implementation on EU and US companies after coming into force?

C. Review Protocol

A review protocol was carried out, starting with the literature research, with the definition of the search string that will be used in the chosen data sets to retrieve the maximum number studies that may address the proposed research questions. The used search string and the data sets are listed below:

Search string: GDPR AND (Challenge OR

Implementation OR Impact OR Effect OR Compliance OR Adoption OR Implications OR Business OR SMEs OR tech Start-ups)

Data sets: Google and Google Scholar, ResearchGate, Mendeley, Journal Storage, Social Science Research Network, Unpaywall.

After that, inclusion and exclusion criteria must be applied to filter the obtained documents. Our criteria are presented in Table 1. The publication date chosen was from 2016 so that the literature already reflects the final approved GDPR.

Table 1. Inclusion and Exclusion Criteria

Inclusion criteria	*Exclusion criteria*
Written in English or Spanish	Not written in English or Spanish
Publication date after 2016 to 2020, inclusive	Publication date before 2016
Scientific papers in conferences or journals	Non-free documents nor master thesis
Title relevance regarding GDPR	No title relevance regarding GDPR

Afterwards, the first set of documents is obtained. Then, in the first phase, the abstracts must be screened to decide their relevance to the research. Finally, these documents are read to obtain the final selection of studies to perform the review.

V. Conducting the Review

This section corresponds to the second step of the SLR methodology. We start by applying the review protocol previously defined and perform an analysis to the extracted data.

Based on the work carried out by [1] after applying the defined search string in the listed data sets, 2720 documents were obtained. With the inclusion and exclusion criteria presented in Table 1, 306 papers were obtained, excluding duplicates.

Afterward, the abstracts were read to further decide the documents' relevance, gathering 50 documents. Each one of these documents was read, obtaining 45 relevant studies for our research. This information is synthesized in Table 2, as presented below.

Table 2. Selection of studies

Review protocol phase	*No. of studies*
Data set searching with string	2720
Inclusion and exclusion criteria	306
Abstracts screened	215
Full-text document	47

VI. Reporting the Review

This section corresponds to the third and last step of the SLR methodology, where we will summarize the extracted data from the selected studies. We have identified two main topics, which are the following sub-sections: GDPR implementation challenges and the influence of GDPR on EU and US technological companies with emphasis on tech start-ups and SMEs.

A. General Data Protection Regulation Implementation Challenges

To comply with GDPR and avoid fines, organisations must ensure that the processing of personal data is in accordance with GDPR. This will impose a great effort on organisations, especially the SMEs and tech start-ups, in supervising and controlling the stream of personal data and in raising the level of alert to potential privacy risks. In this sense, this study seeks to explore the implementation management challenges for the technological companies before and after of the GDPR coming into force.

The management challenges to be GDPR compliant before the GDPR coming into force. The EU companies have faced and are still facing problems to be GDPR compliant. Report research carried out between the 9th and the 15th January 2018 by Populos under the order of Senzing [23] revealed that before the entry into force of the GDPR 60 per cent of the EU companies were not ready. The report is based on a survey of 1.015 companies based in UK, Germany, France, Spain, and Italy which cover all size companies. The GDPR readiness scale was calculated based on responses to questions which are explicitly about knowledge, understanding and actions being taken concerning GDPR.

The survey questions were directed to find out the level of knowledge of where data is housed, the level of confidence about being able to account for all different databases, the actions being taken to prepare for GDPR, the level of awareness of the reputational impact of GDPR non-compliance, of the financial fines resulting from GDPR non-compliance and of confidence that the company can respond to data enquiries within the thirty-day obligation.

The findings of this report identify that 60 per cent of all the participating companies are not GDPR ready for dealing with the challenges that GDPR compliance will demand and that more than one in ten (12 per cent) of companies are not confident that they know where all their data is housed [23].

The report carried out by Senzing [23] is relevant to the present research to assess the level of GDPR compliance of companies, especially the SMEs and the tech start-ups before the GDPR implementation. Although this report is of great value on the level of GDPR compliance, mainly on data location, it does not concentrate on tech start-ups in the EU and the US, but on companies of all sizes based in UK, Germany, France, Spain, and Italy.

Research carried out by [24] before the GDPR coming into force revealed that UK tech-start-ups perceive GDPR as “vague” and “open to interpretation" and feel frustrated since there are no clear set of implementation guidelines. The Right of erasure (which provides a mechanism for data subjects to have their data deleted by the data controller) under art. 17 of the GDPR was revealed as the biggest GDPR challenge that blockchain companies face, because “you cannot remove [the data], you need to find a way to make the data unavailable”.

The research carried out by [24] is relevant to the present research to assess the GDPR challenges around the UK tech start-ups before the GDPR implementation. The findings suggest that many of the UK tech start-ups struggled and or misinterpreted how compliance could be achieved. Although this research is of great value on the level of GDPR challenges around the UK tech start-ups before the GDPR implementation, it does not concentrate on tech start-ups in the rest of the EU and the US.

The independent report research carried out in May 2017 to IT and Legal professionals for the US companies and in

August 2017 to IT, and Legal professionals for the EU companies by Dimensional Research under the order of TrustArc [25] which concentrated on the level of GDPR compliance on UK and US companies before the GDPR coming into force revealed that for US and UK privacy professionals they needed the most help complying with data privacy requirements. For US and UK respondents, developing a GDPR plan topped the list and that in terms of costs to find a solution to their GDPR challenges they will invest in resources such as consultants, new hires and technology to prepare for meeting the GDPR deadline [25].

The identified challenges before the GDPR coming into force can be summarised as the lack of technical and legal know-how in terms of data location and being able to account for all different databases, uncertainty in the actions being taken to prepare for GDPR, the level of awareness for the reputational impact and financial fines of GDPR noncompliance, the lack of confidence that the organisation can respond to data enquiry within the 30 day obligation, GDPR being vague and open to interpretation, missing a clear set of guidelines for implementation, the right to erasure, struggled and or misinterpreted how compliance could be achieved, the need of help to comply with data privacy requirements and in terms of costs to invest in resources such as consultants, new hires and technology to help prepare for meeting the GDPR deadline.

The management challenges to be GDPR compliant after the GDPR coming into force. The latest independent report research carried out by Dimensional Research under the order of TrustArc in June 2018 [26] focused on a comparative analysis of the level of GDPR compliance among companies of all sizes based in the US, UK, and EU (countries other than the UK) as well as in terms of costs expenditure, efforts, most significant challenges and motivations to become GDPR compliant by the deadline. For all the respondents, privacy represented at least 25% of their job. The participating companies included a mix of small, mid-sized and large firms, from all major industry sectors.

The report came out with some important findings: GDPR is a work in progress, companies are motivated more by values and customer and other third-party expectations than by fear of fines and litigation, companies are further ahead with updating policies and cookie management than with international data transfer and vendor risk management, and GDPR has been challenging but rewarding. Among the top challenges were GDPR complexity, lack of expertise, qualified staff and GDPR technology and tools, 65% are positive about the impact of GDPR on their business, GDPR will continue to dominate privacy efforts, achieving, maintaining, and demonstrating GDPR compliance are the top three privacy priorities over the next 6-12 months and 50 per cent of respondents will seek a third party GDPR validation rather than wait for the official GDPR certification.

Study research conducted by [21] on SMEs concludes as major challenges: the lack of privacy experts and knowledge on how to handle the new requirements on privacy data protection. Therefore, there was a strong need for education in data protection and privacy, different interpretation of the GDPR among managers and employees and customers and network partners and adapting their original business model to be GDPR compliant.

Study research conducted by [7] on the information technology sector concludes three major challenges; the process of conducting an audit to GDPR (audit systems) and data erasure, the technical challenges of implementing the right to be forgotten and limits the growth of emerging technologies. The challenges related to the increase in technical complexity and limits the growth of emergent technologies are greater for smaller companies particularly due to a lack of human resources [7]. Vranaki et al. (2016) consider on their report that micro-companies and SMEs face greater challenges in shifting to the GDPR because of the need for a cultural change in customer relations and working methods [27].

A report conducted by European Commission (2020) makes clear that there are a number of areas for improvement. The Commission acknowledges that some SMEs may face challenges in complying with the GDPR, but points to the practical tools and resources that several supervisory authorities have made available and encourages further progress in this area.

The identified challenges after the GDPR coming into force can be summarised as top challenges GDPR complexity and lack of expertise, qualified staff and GDPR technology and tools. The lack of privacy experts and knowledge on how to handle the new requirements on privacy data protection especially international data transfer and vendor risk management. The challenges related to the increase in technical complexity and limits the growth of emergent technologies are greater for smaller companies particularly due to a lack of human resources. micro-companies and SMEs face greater challenges in shifting to the GDPR because of the need for a cultural change in customer relations and working methods.

B. The Influence of GDPR on EU and US Technological Companies with Emphasis on Tech Start-ups and SMEs

GDPR brings many juridical and functional changes together with the need to educate staff and regularly train them in order to change their mindset and culture to the new model [9].

Study conducted by [1] indicate that GDPR is extensive, complex, it does not provide specific guidelines that should be used to comply with its requirements [8] and it involves subjectivity [3]. Moreover, the biggest challenge for the organisation is the lack of privacy knowledge and expertise [8], followed by the lack of budget and of human resources [8; 28] and increasing administrative work [29]. Therefore, business costs are expected to increase also because the organization may require recruiting privacy experts [21]. Contracting the services of a DPO may be also a challenge since it may be difficult to recruit and retain people with those skills [8].

Study conducted by [30] on SMEs in Germany identifies six constructs: Know-how, expenditure of time, uncertainty, costs, provision of information, and process adaption. Each construct has a negative influence on the impacts on the implementation of the GDPR in already existing business models.

Most discussions on data protection, and especially GDPR, have focused on the larger tech firms, such as Facebook and

Google, and what these laws mean for the users of such services (e.g., see [31]) other discussions have focused on SMEs [30] and on small tech start-ups, but about one country the UK (e.g., see [24]). However, tech start-ups and SMEs also require attention, especially tech start-ups, who are driven by innovation, pushing the boundaries of technologies but lacking established data protection best practices. Initial decisions taken by start-ups could well have negative long-term impacts. Making sure that the innovations and practices of tech start-ups are sound, appropriate, and acceptable should, therefore, be a high priority.

The Supervisory Authorities need to provide more support to the tech start-ups, such as increasing awareness and guidance. They also need to take an active role to prevent harm and deter so that the start-ups are given the best opportunities to innovate within the GDPR framework [24]. There is the conviction that the Supervisory Authorities are concentrating more on the larger tech firms than the small tech start-ups and SMEs if that is the case the negative long-term impact can be devastating [24].

Moreover, the GDPR costs implication for the tech start-ups and the SMEs are creating struggles in terms of innovation. Theoretical works of [32] and [33] show that compliance costs and data regulation can create barriers to entry and may negatively affect innovation. The researchers [33] indicate that although privacy regulation forces costs on all companies, the small and new companies are the most negatively affected ones, especially for goods where the price mechanisms do not mediate the effect, such as the advertising-supported internet. The researchers [32] show that as the costs of compliance by small companies increase, more innovations will be developed within established companies.

The work of [34] shows that the industrial innovations that venture capitalists help facilitate are a multiple of the ratio of venture capital to the R&D expenditures (as cited in [35]).

The researchers collected data on all technology-venture related activity in the EU and US from July 2017 to September 2018 to study the effects of the GDPR coming into force in May 2018 on venture financing in the EU [35]. For this, the researchers contrasted venture activity in the EU with the US before and after the coming into force of the GDPR. The researchers found evidence suggesting adverse and significant effects following the enforcement of the GDPR on the number of venture deals, the size of those deals, and the overall amount of dollars invested. They broke down those effects according to two venture categories (financial/healthcare and technology start-ups) and four venture age groups. They presented a rough estimate of the effect on the number of jobs for zero to three-year-old technology ventures. They estimated a job loss of between 3.604 and 29.819 in the number of individuals employed by those companies.

The report research study carried out by [35] is relevant to the present research to evaluate the effects of the GDPR in May 2018 on venture finance in the EU tech start-ups by comparing venture activity in the EU and the US before and after the GDPR coming into force.

Research carried out by [24] before the GDPR coming into force revealed that some of the UK tech-start-ups remained unable or unwilling to make a GDPR continuing compliance effort. Tech start-ups always need to take their regulatory obligations seriously. This report is of great value, primarily because it mainly deals with tech start-ups, the report could have been more relevant if also companies from the EU will have participated.

However, there is research that points that many start-ups either do not see a DPO as applicable to their firm, or they had appointed someone internally as a DPO, regardless of their data protection expertise or organisational independence [36]. A DPO should be a person with expert knowledge of data protection law and practices [36]. Article 35(5) of the GDPR states that a DPO must have ‘an expert knowledge of data protection law and practice’ but does not specify how controllers could appreciate this ‘expert knowledge’. In the researcher’s opinion a DPO should be certified to prove his or her competence in the field, that organisations do not see a DPO as applicable to their firm or that they may appoint a DPO regardless of their data protection expertise is because companies see the DPO as a new legal burden. There is a real risk that companies ensure only a minimum application of the law and since the DPO does not necessarily have to be a certified one then they are not breaching the law.

In the researcher opinion and that of Lothar Determann, a Chief Privacy Officer (CPO) should also be considered. For many companies understanding precisely what is required to become compliant has been and still is one of the biggest problems because the GDPR does not offer the practical solutions to be GDPR compliant [37].

Therefore, it all comes down to the start-ups and SMEs lack of privacy knowledge and expertise, followed by the lack of budget and of human resources and increasing administrative work together with a need for a cultural change on customer relations and working methods. On the other, hand the larger companies have the greatest difficulties in implementing the erasure data.

CONCLUSION, LIMITATIONS, AND FUTURE WORK

In this work, the authors conducted a systematic literature review to identify the key challenges and the effect of GDPR implementation on EU and US tech companies before and after coming into force. With the summarized information and analysis performed above, the authors can answer the proposed research questions.

Hence, the answer to the research questions RQ1 and RQ1.1 is the following: there are several key challenges: as the lack of technical and legal know-how, uncertainty in the actions being taken to prepare for GDPR, the level of awareness for the reputational impact and financial fines of GDPR noncompliance, the lack of confidence, GDPR being vague and open to interpretation, missing a clear set of guidelines for implementation, the right to erasure, the need of help to comply with data privacy requirements and in terms of costs to invest in resources such as consultants, new hires and technology to help prepare for meeting the GDPR deadline.

In relation to the RQ1.2, several key challenges of GDPR implementation were identified:

1.- The complexity and the extension of the regulation that also does not provide specific and clear guidelines regarding the technologies to be used to comply with what is required and the subjectivity of the regulation itself.

2.- The associated costs not only for the implementation, but for the running with the need in some cases to contract the services of a DPO because of the organization's lack of awareness and or expertise on data privacy which may also lead to the decrease organization's performance.

3.- Limited support from the authorities and the lack of practical guidelines.

Concerning the influence of GDPR implementation on EU and US companies after coming into force (RQ2), it has been revealed that the lack of know-how, the high expenditure of time, the big uncertainties, the high costs, the insufficient provision of information, and the difficult process adaption has a negative influence on the implementation of the GDPR in already existing models.

By identifying challenges, the organizations will be careful to avoid mistakes and pitfalls throughout the process of GDPR implementation.

REFERENCES

[1] G. A. Teixeira, M. Mira da Silva, and R. Pereira, "The critical success factors of GDPR implementation: a systematic literature review," Digital Policy, Regulation and Governance, 21(4), pp. 402–418, 2019.

[2] S. Rodotà, "Data Protection as a Fundamental Right," In Reinventing Data Protection? (pp. 77–82), 2009.

[3] S. Agarwal, "Towards dealing with GDPR uncertainty," IFIP Summer School in Privacy and Identity Management, 2016.

[4] R. Perrault, Y. Shoham, E. Brynjolfsson, J. Clark, J. Etchemendy, B. Grosz Harvard, … J. C. Niebles, "The AI Index 2019 Annual Report," In AI Index Steering Committee, Human-Centered AI Institute, 2019.

[5] J. Furman and R. Seamans, "AI and the Economy," Innovation Policy and the Economy, 19, pp. 161–191, 2019.

[6] J. E. Bessen, S. Impink, L. Reichensperger, and R. Seamans, "GDPR and the Importance of Data to AI Startups," SSRN Electronic Journal, 2020.

[7] N. Poritskiy, F. Oliveira, and F. Almeida, "The benefits and challenges of general data protection regulation for the information technology sector." Digital Policy, Regulation and Governance, 21(5), pp. 510–524, 2019.

[8] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," Computer Law and Security Review, 2018.

[9] M. da C., Freitas, and M. Mira da Silva, "GDPR Compliance in SMEs: There is much to be done." Journal of Information Systems Engineering & Management, 3(4), pp. 1–7, 2018.

[10] K. Kapoor, K. Renaud, and J. Archibald, "Preparing for GDPR: Helping EU SMEs to manage data breaches," Proceedings of AISB Annual Convention 2018.

[11] V. Supyuenyong, N. Islam, and U. Kulkarni, "Influence of SME characteristics on knowledge management processes," Journal of Enterprise Information Management, 22(1/2), pp. 63–80, 2009.

[12] M. Brodin, "A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises," European Journal for Security Research, 4(2), pp. 243–264, 2019.

[13] B. Kitchenham, "Procedures for Performing Systematic Reviews," In Department of Computer Science, Keele University, Keele. 2004.v

[14] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," MIS Quarterly, 26(2), pp. 13–23, 2002.

[15] P. De Hert and V. Papakonstantinou, (2016). "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" Computer Law and Security Review, 2016.

[16] European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da. Official Journal of the European Union, 59, pp. 1–88. 2016.

[17] Y. McDermott, "Conceptualising the right to data protection in an era of Big Data," Big Data & Society, 4(1), 2017.

[18] S. E. Polykalas and G. N. Prezerakos, "When the mobile app is free, the product is your personal data." Digital Policy, Regulation and Governance, 21(2), pp. 89–101, 2019.

[19] S. Sirur, J. R. C. Nurse, and H. Webb, "Are We There Yet?" Proceedings of the 2nd International Workshop on Multimedia Privacy and Security, (ii), pp. 88–95, 2018.

[20] J. Seo, K. Kim, M. Park, M. Park, and K. Lee, "An analysis of economic impact on IoT industry under GDPR," 8th International Conference on ICT Convergence (ICTC), pp. 879–881. (2017).

[21] P. Lindgren, "GDPR Regulation Impact on Different Business Models and Businesses," Journal of Multi Business Model Innovation and Technology, 4(3), pp. 241–254, 2018.

[22] M. Boban, "Protection of personal data and public and private sector provisions in the implementation of the general eu directive on personal data (GDPR)," In 27th International Scientific Conference on Economic and Social Development, 2018.

[23] J. Jonas, "Finding the Missing Link in GDPR Compliance," Research Report Conducted by Populos, 2018.

[24] C. Norval, H. Janssen, J. Cobbe, and J. Singh, "Data protection and tech startups: The need for attention, support, and scrutiny," 2019.

[25] TrustArc. "Privacy and the EU GDPR. US and UK Privacy Professional", 2017.

[26] TrustArc. "GDPR Compliance Status: A Comparison of US, UK and EU Companies," 2018.

[27] A. Vranaki, M. Heyder, and B. Bellamy, "Implementing and Interpreting the Gdpr: Challenges and Opportunities", 2016.

[28] M. C. Addis and M. Kutar. "The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness," UKAIS, 2018.

[29] L. Magnusson, and S. Iqbal, "Implications of EU-GDPR in Low-Grade Social, Activist and NGO Settings," International Journal of Business & Technology, 6(3), pp. 1–7, 2018.

[30] R. C. Härting, R. Kaim, and D. Ruch, "Impacts of the implementation of the general data protection regulations (GDPR) in SME business models-an empirical study with a quantitative design," Smart Innovation, Systems and Technologies, 2020).

[31] K. A. Houser and W. Voss, "GDPR: The End of Google And Facebook Or A New Paradigm In Data Privacy?" Richmond Journal of Law & Technology, XXV(1), pp. 1–109, 2018.

[32] S. Krasteva, P. Sharma, and L. Wagman, "The 80/20 rule: Corporate support for innovation by employees," 38, 1–36, 2014.

[33] J. Campbell, A. Goldfarb, & C. Tucker, "Privacy Regulation and Market Structure," Journal of Economics & Management Strategy, 24(1), pp. 47–73, 2015.

[34] S. Kortum and J. Lerner, "Assessing the Contribution of Venture Capital to Innovation," The RAND Journal of Economics, 2000.

[35] J. Jia, G. Zhe Jin and L. Wagman, "The Short-Run Effects of GDPR on Technology Venture Investment", 2019.

[36] E. Lachaud, "Should the DPO be certified?" International Data Privacy Law, 4(3), 189–202, 2014.

[37] L. Determann, "Determann's Field Guide to Data Privacy Law" (4th ed.). Elgar Compliance Guides, 2020.