The Critical Success Factors of GDPR Implementation: a Systematic Literature Review

Gonçalo Almeida Teixeira[1] goncalo.almeida.teixeira@tecnico.ulisboa.pt
Miguel Mira da Silva[1] mms@tecnico.ulisboa.pt
Ruben Pereira[2] ruben.filipe.pereira@iscte-iul.pt

[1] Instituto Superior Técnico, University of Lisbon, Portugal
[2] Instituto Universitário de Lisboa (ISCTE-IUL), Portugal

Abstract

Purpose – The digital paradigm we live in today, which drastically increased the consumption of data, is a threat to people's privacy. In order to create a high level of privacy protection for its citizens, the European Union proposed the General Data Protection Regulation (GDPR), which introduces obligations for organizations regarding the storing, processing, collecting and disclosing of data. This research aims to identify the critical success factors of GDPR implementation.

Design/methodology/approach – A systematic literature review was conducted by following a strict review protocol, where 32 documents were found relevant to perform the review and to answer to the proposed research questions.

Findings – The critical success factors of GDPR implementation were identified, including barriers and enablers. Furthermore, benefits of complying with GDPR were also identified.

Research limitations/implications – Since GDPR is a relatively recent subject, there are still few scientific papers about it. Therefore, the authors were not able to identify nor present a robust conclusion regarding specific topics, such as practical outcomes.

Originality/value – Based on the literature, the identified critical success factors may be useful for organizations since these can be better prepared to achieve compliance by prioritizing the enablers and avoiding the barriers.

Keywords GDPR, Implementation, Organizations, Compliance, Critical Success Factors, Enablers, Barriers.

1. Introduction

Since the foundation of the Internet and the World Wide Web, the evolution of technology has enabled the increasing collection, process and storage of large amounts of personal data (Huth, 2017).

New information tools and techniques such as Big Data, Data Mining and Machine Learning revolutionized business models through the processing of data, as well as Cloud Computing and the Internet of Things, which leveraged the consumption of data to a whole new level.

All these improvements led to the ubiquitous Information Technology society we have today, having a visible digital impact in many organizations across several sectors, which take advantage of all the possibilities provided by new technologies (Lopes and Oliveira, 2018).

However, this digital revolution and the increasing collection of personal data by organizations has inherent security challenges and risks. The significant low prices to collect, process and analyze large amounts of data lure organizations to collect more data than necessary, leading to the misuse of personal data and making them vulnerable to privacy breaches (Agarwal, 2016). Therefore, to protect citizens' personal data and privacy, regulators are adapting regulations to the present digital economy (Agarwal, 2016). On this track, the European Union proposed a new regulation, the General Data Protection Regulation (GDPR), with a set of obligations regarding the storing, processing, collecting and disclosing of data (Gabriela *et al.*, 2018).

GDPR replaces and repeals the EU Data Protection Directive, which was adopted in 1995 and no longer meets the privacy requirements of the new digital landscape (Tikkinen-Piri *et al.*, 2018), and introduces significant changes regarding personal data and privacy, aiming to give more control to citizens over their personal data, in order to ensure a harmonized, unified and sustainable approach to data protection (Boban, 2018).

Enforced from 25th May 2018, the Regulation applies to any organization that processes EU citizens' data and may impose hefty fines when non-compliance is detected (European Commission, 2016).

To comply with GDPR, organizations need to review their internal procedures and processes, which will impose a lot of changes and adaptations that will impact organizations' businesses.

To the best of our knowledge, and since GDPR is a relatively recent subject, there are no literature reviews and few scientific papers with an in-depth study regarding GDPR implementation. Therefore, we conducted a systematic literature review in order to identify the critical success factors (CSF) which contribute for GDPR implementation, by identifying the enablers and barriers in the compliance process.

It is important to note that this research focuses on the implementation of GDPR in organizations in general, without any specific sector or industry, even though it is obvious that some may have more impact than others, such as IoT or Big Data industries.

This paper is structured as follows. Section 2 explains the chosen research methodology (systematic literature review). Section 3 presents the theoretical background with the GDPR and CSF description. Section 4 describes the motivation of our research, where the problem is revealed, along with the addressed research questions and the review protocol. Section 5 presents the review protocol application and the data extraction results. Section 6 discusses and analyzes the findings from the review. Finally, Section 7 concludes the paper.

2. Research Methodology

A systematic literature review (SLR) is a form of study used to identify, analyze and interpret all available evidence regarding a specific topic or question, using a trustworthy, rigorous and auditable methodology, to synthesize the existing work in a systematic, comprehensive and unbiased manner (Kitchenham, 2004).

Our research methodology is based on (Kitchenham, 2004), complemented by (Webster and Watson, 2002), which 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 basic review procedures.
- Conducting: apply the review protocol previously designed in order to obtain studies which will be the object of the review.
- Reporting: summarize the extracted data from the selected studies in order to report the findings.

We chose SLR as the research methodology since we wanted to summarize the existing evidence regarding GDPR implementation, with the aim to answer to the proposed research questions.

3. Theoretical Background

In this section, we will introduce the two major concepts that support this paper: the General Data Protection Regulation and Critical Success Factors.

3.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (EU 2016/679), known as GDPR, is an European Union Regulation enforced from 25th May 2018 which introduces major changes regarding personal data and privacy, replacing and repealing the EU's 1995 Data Protection Directive (DPD, also known as Directive 95/46/EC) (European Commission, 2016). It is the most important alteration in the last 20 years regarding data privacy, with far greater magnitude than any similar regulation (Freitas and Mira da Silva, 2018; Allen *et al.*, 2018), and contains obligations regarding the storing, processing, collecting and disclosing of data (Gabriela *et al.*, 2018).

With this Regulation, EU aims to give more control to citizens over their personal data, strengthening their rights, to reform how organizations view and control these data, and to remove obstacles to cross-border trades, enabling easier expansion of businesses across Europe, as well as ensuring the free movement of personal data between EU Member States (Boban, 2018; Sirur *et al.*, 2018). The ultimate goal of GDPR is to ensure a harmonized, unified and sustainable approach to EU citizens' data protection, by creating a high level of privacy protection in the European Union (Seo *et al.*, 2018).

The scope of GDPR is very broad since it applies to any organization that processes EU citizens' data. Therefore, the new Regulation applies to vastly more data than the previous Directive, shifting the scope from the location of the data processing to the location of the data subject (Allen *et al.*, 2018).

GDPR's life-cycle started in January 2012 with a proposal from the European Commission. After a long-run discussion, the Regulation was approved on 27th April 2016. However, the European Union established a two year transitional period for organizations to achieve compliance, so that these were able to implement the necessary changes in the meantime, until 25th May 2018 (Lopes and Oliveira, 2018; Sirur *et al.*, 2018).

It is important to highlight the difference between a directive and a regulation. The first one lay down a set of general guidelines but only becomes enforceable when transposed into national law by Member States. Regulations, however, have already binding legal force (Seo *et al.*, 2018). Therefore, GDPR is applicable in every Member State without the need for a national legislation implementation, unifying the European Union rules and laws (Freitas and Mira da Silva, 2018).

The Regulation has a lot of novelties, starting by the re-definition of personal data, which has been further expanded (Seo *et al.*, 2018). Article 4 from GDPR states that "personal data means any information relating to an identified or identifiable natural person" (European Commission, 2016). Regarding personal data, GDPR outlines a number of rights and responsibilities for citizens (referred as data subjects) and organizations (controllers and processors).

On one hand, citizens have seen their rights been expanded, including data access, rectification, the right to withdraw consent, erasure, data portability, the right to object and to lodge a complaint (European Commission, 2016).

With the new Regulation, organizations can only process citizens' data with their explicit and clear consent. After giving consent, data subjects have the right to rectification regarding inaccurate personal data, the right to withdraw previous consent at any time, and the right to erasure if there are no longer reasons for the processing of their data or if the data was unlawfully processed ("right to be forgotten") (European Commission, 2016).

Data subjects also have the right to data portability by obtaining a copy of their personal data in a structured format, with the possibility to transmit it to another organization, to object to decisions based only on automated processing (such as profiling), and to lodge a complaint with a Supervisory Authority if the processing of their data infringes GDPR. At any time, citizens may also request access to their data in order to know if it is being processed and how (European Commission, 2016).

On the other side, controllers and processors have stricter rules to follow and to comply with. GDPR provides a set of principles that organizations must implement relating to processing of personal data: lawfulness, fairness and transparency, purpose limitation (data should be collected for specific, explicit and legitimate purposes), data minimization (data should be the minimum necessary for the processing purposes), accuracy, storage limitation, integrity, confidentiality and accountability (European Commission, 2016).
Moreover, when processing of personal data may result in a high risk to the rights and freedoms of citizens, a Data Protection Impact Assessment (DPIA) should be performed to assess the inherent risk of such processing. When such assessment indicates a high risk regarding the processing of personal data, organizations must consult Supervisory Authorities prior to the processing (European Commission, 2016).
Besides these obligations, organizations should also designate a qualified Data Protection Officer (DPO), who should monitor compliance with GDPR and act as a point of contact between the organization and Supervisory Authorities. The Regulation also requires organizations to report data breaches to Supervisory Authorities within 72 hours, as well as to notify data subjects that may be potential victims (European Commission, 2016).
Failing to comply with GDPR may impose hefty fines to organizations, which may range up to 4% of annual turnover or 20M EUR, whichever is higher (European Commission, 2016).

3.2 GDPR Implementation

In order to comply with the Regulation and avoid fines, organizations must adopt protection policies and implement appropriate technical and organizational measures to ensure that the processing of personal data is in accordance with GDPR. This measures include pseudonymization, encryption, maintaining a record of the processing activities, and applying Privacy by Design and by Default principles. Furthermore, organizations must also be able to demonstrate compliance to Supervisory Authorities (European Commission, 2016).
Besides technological challenges, GDPR also brings a lot of juridical and functional changes, along with the necessity to educate staff and change their mindset and culture to this new paradigm (Freitas and Mira da Silva, 2018).
Since GDPR imposes a lot of changes and challenges, organizations will need to review their processes, routines and procedures, in order to ensure that they collect, hold and process personal data in accordance with the Regulation (Tikkinen-Piri *et al.*, 2018).

3.3 Critical Success Factors (CSF)

Critical success factors (CSF) are the areas in which satisfactory results will ensure successful competitive performance for the organization, in order for the business to flourish and for the organization to achieve its goals (Bullen and Rockart, 1981). Therefore, CSF represent the managerial or enterprise variables, conditions and characteristics that must be given special attention to attain high performance (Boynton and Zmud, 1984).
By identifying critical success factors, organizations can assess their threats and opportunities, and, when properly managed, CSF can have an important impact on an organization's success (Leidecker and Bruno, 1984) since they help ensure that critical organizations' needs are addressed (Boynton and Zmud, 1984).
In this paper, we will distinguish critical success factors between enablers – factors that ease projects' realization and are critical to its success – and barriers – factors which may conduct to projects' failure.

4. Planning the Review

This section corresponds to the first step of the SLR methodology. We begin by providing the motivation of this paper, followed by the research questions we aim to address and answer with our research. Finally, we propose our review protocol.

4.1 Motivation

The implementation of GDPR imposes a set of legal, technological and functional changes, having a major impact in organizations, regardless of their sector or industry (Freitas and Mira da Silva, 2018). Every organization will need to reconsider the way they collect, store and process personal data, adopt new measures and policies, and re-design internal processes to demonstrate their compliance (Boban, 2018).

However, GDPR does not provide specific guidelines regarding its implementation, not being prescriptive in the technologies to use to achieve compliance (Tankard, 2016). That's why organizations, in general, are having serious difficulties in understanding the Regulation and how to implement it (Sirur *et al.*, 2018). Specially, organizations that deal with large amounts of personal data are being greatly affected (Seo *et al.*, 2018).

Therefore, this research aims to obtain information regarding GDPR implementation and compliance, in order to identify the critical success factors which contribute to GDPR implementation, including both positive (enablers) and negative (barriers) factors.

4.2 Research Questions

Our research and analysis is based on RQ1 and RQ2, presented below.

RQ1: What are the critical success factors for GDPR implementation?
RQ2: What are the benefits of complying with GDPR?

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

RQ1.1: Which are the barriers for GDPR implementation?
RQ1.2: Which are the enablers for GDPR implementation?

4.3 Review Protocol

The review protocol starts by the literature search, with the definition of the search string that will be used in the chosen datasets in order to retrieve the maximum number of studies that may address the proposed research questions. The used search string and respective datasets are listed below.

Search String: GDPR AND (Adoption OR Impact OR Business OR Economy OR Implementation OR SME OR Implementing OR Adopting OR Compliance OR Implications).

Datasets: Google Scholar, ScienceDirect, IEEEXplore, Microsoft Academic and Scopus.

After that, inclusion and exclusion criteria must be applied in order to filter the obtained documents. Our criteria is presented in Table 1.

Table 1. Inclusion and Exclusion Criteria.

Inclusion Criteria	**Exclusion Criteria**
Written in English or Portuguese	Not written in English nor Portuguese
Publication date after 2016, 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

The publication date was limited from 2016 so that the literature already reflects the final approved Regulation.

Afterwards, the first set of documents is obtained. Then, in a first phase, the abstracts must be screened in order to decide their relevance to the research. Finally, these documents are read in order to obtain the final selection of studies to perform the review.
The review protocol is illustrated in Figure 1.

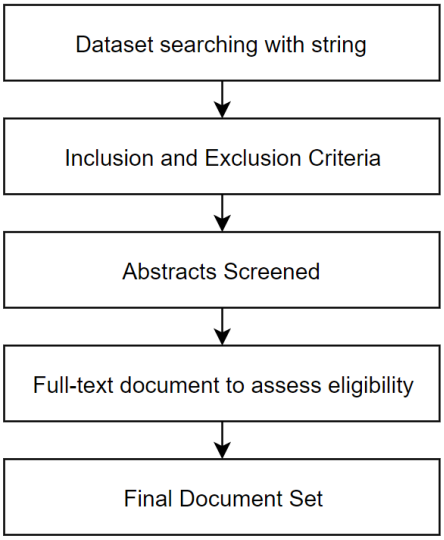

Figure 1. Review Protocol.

5. 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.

5.1 Selection of Studies

After applying the defined search string in the listed datasets, 959 documents were obtained. With the inclusion and exclusion criteria presented in Table 1, 90 papers were obtained, excluding duplicates.
Afterwards, the abstracts were read to further decide the documents' relevance, gathering 63 documents. Each one of these documents was read, obtaining 32 relevant studies for our research. This information is synthesized in Table 2, presented below.

Table 2. Selection of Studies.

Review Protocol phase	**Number of Studies**
Dataset searching with string	959
Inclusion and exclusion criteria	90
Abstracts screened	63
Full-text document	32

5.2 Data Extraction Analysis

The journal articles distribution is almost twice as the conference distribution, as it is shown in Figure 2.

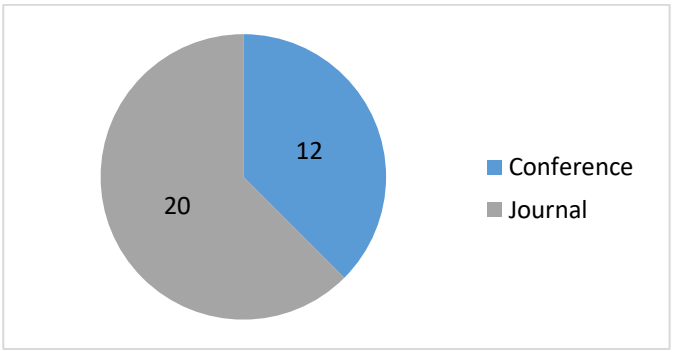

Figure 2. Conference and Journal Distribution.

It is also possible to see, in Figure 3, an increment of the number of documents over time (note that 2019 only reflects articles published until the beginning of March). This can be explained with the fact that, as already referred, GDPR was enforced in 2018. Therefore, an increase of interest over time would be expected, which is reflected in the number of published articles.

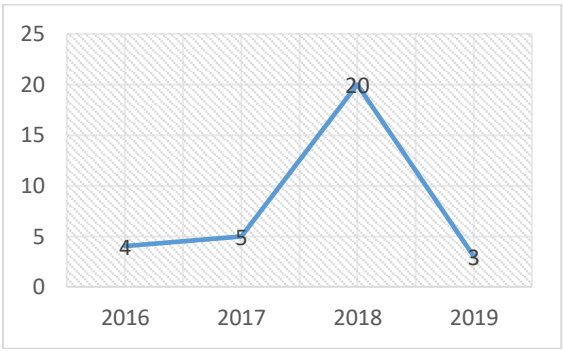

Figure 3. Number of selected documents by year.

Among the 32 selected documents, the Network Security Journal and Computer Fraud & Security Journal are the most represented sources, both with four articles, as presented in Figure 4.

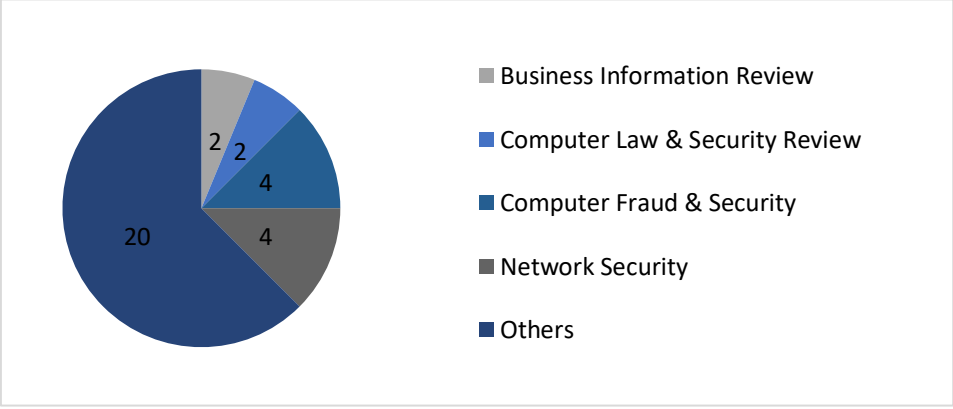

Figure 4. Most represented sources.

6. 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
- GDPR Compliance

In this section, we will start by analyzing GDPR implementation and discuss the several GDPR Roadmaps present in the literature. Moreover, we will also summarize some key points in GDPR implementation:

- GDPR Awareness and Analysis
- Data and Documentation
- Security Principles and Mechanisms
- Training Awareness
- Data Protection Officer
- Data Protection Impact Assessment

Finally, we will identify the benefits and challenges of complying with GDPR.

6.1 GDPR Implementation

The enforcement of the General Data Protection Regulation has dictated the need for organizations to comply with its requirements and obligations. Since Supervisory Authorities may impose sanctions whenever non-compliance is detected, organizations need to review their processes and procedures to ensure compliance and avoid sanctions (Tikkinen-Piri *et al.*, 2018). For organizations, this requires the implementation of complex technological solutions, as well as new organizational duties and extensive changes in the organization's business model, which may also affect resource usage (Skendzic *et al.*, 2018; Tikkinen-Piri *et al.*, 2018).

Although many organizations understand the importance of complying with the new Regulation, the uncertainty around GDPR has led to some divided approaches (Sirur *et al.*, 2018) because GDPR is not prescriptive regarding solutions to achieve compliance, not providing specific guidelines to implement its requirements (Tikkinen-Piri *et al.*, 2018).

Therefore, every organization must find and implement organizational and technological solutions to put the provisions in practice (Tikkinen-Piri *et al.*, 2018; Freitas and Mira da Silva, 2018). For that, and to achieve compliance, it is very important to design an implementation strategy and roadmap.

6.1.1 GDPR Implementation Roadmap

A detailed roadmap will help business to prioritize, as well as to demonstrate a proof of the compliance process if required by Supervisory Authorities (Garber, 2018). The literature already presents some suggestions regarding plans for implementing GDPR.

The first suggestion is an implementation plan with 4 steps. It starts by establishing an implementation step list in order to be complaint. Then, it is suggested to set realistic timelines and allocate enough resources to support the compliance process. Afterwards, compliance recommendations should be prioritized in order to make strategic decisions. Finally, when the process of compliance is in course, the organization should continue with ongoing reviews and improvements regarding the implementation program (Boban, 2018).

Even though this approach takes into account the resources allocation and the continuous evaluation of the implementation plan, with monitoring and implementing improvements, it is very superficial and low detailed and does not focus on understanding GDPR requirements, which is very important to derive a strategy for compliance, nor in data management.

Another alternative suggests an implementation roadmap, but with much more detail regarding GDPR. The first step consists in auditing the data and internal processes to understand in which extent the GDPR applies to the organization, by analyzing the owned personal data. After that, the organization should put data management into practice, by adopting transparent policies in order to show how they collect and process data. Then, security measures should be established to protect these data. Finally, appropriate tools should be used to ensure new requirements, record keeping and documentation (Gabriela *et al.*, 2018).

This approach is very complete and implicitly takes into account GDPR requirements in the first step. However, it does not specify the security measures to be applied and does not take into account the impact of the implementation plan in the organization resources, namely people.

Other approach refers the initial steps to make before implementing measures in order to achieve compliance stated by Baker & McKenzie, an international law firm. The first one consists in assessing whether or not the organization falls within the GDPR scope. Then, organizations need to understand the GDPR compliance obligations, how to comply with them and assess their impact. After that, organizations should identify new responsibilities and risks, and identify strategies to mitigate them. The final step is to devise a strategy for GDPR implementation (Tankard, 2016).

In fact, it is a very complete approach regarding steps to do before putting the compliance process into action. However, the author did not completed the roadmap suggested by Baker & McKenzie with specific implementation strategies nor security measures to put in practice.

The last roadmap found in the literature is divided in three stages. In the first stage (Gather), organizations should map all the personal data they own. In the second stage (Analyze), organizations should analyze these data in order to detect flaws. It may be necessary to carry DPIAs as well. With the flaws identified and the risks measured, a strategy plan can be traced, with solutions to achieve compliance. Finally, in the Implement stage, organizations must implement the necessary changes, including security mechanisms. In the end of the last stage, organizations must ensure the continuity of their compliance by performing periodically compliance audits (Lopes and Oliveira, 2018).

Besides being the most complete roadmap in the literature, it is the only approach that mentioned risk assessment, which is a GDPR requirement whenever processing of personal data may result in high risk to the privacy of its owners.

6.1.2 GDPR Awareness and Analysis

The first step towards GDPR compliance consists in being aware of the Regulation, regarding not only its existence but its content as well, including requirements and obligations. Even though this seems obvious, there are some surveys that show that there are a lot of organizations that were not realizing the relevance of GDPR and complying with it, lacking awareness about the European Regulation.

In September 2016, an online survey studying the perceptions and readiness of organizations regarding GDPR reported that 18% had never heard of GDPR before, and 31% didn't know any details. Furthermore, roughly one third of the enterprises affirmed that they were ready for GDPR. The study concluded that companies were not prepared for GDPR and that there were a broad lack of awareness (Dell, 2016).

Later on, in March 2017, another study was performed in the United Kingdom, and a general lack of awareness and knowledge regarding GDPR also emerged. UK organizations were, in general, not well informed or aware of GDPR, even though large organizations tended to be better informed (Addis and Kutar, 2018).

In the same month, another survey with 101 organizations, this time in Portugal, reported that 65% consider to have at least a medium level of awareness (KPMG, 2017), which is already reasonable since they still had one year until the deadline.

Last but not least, in the beginning of 2018, an online survey with 62 Norwegian companies concluded that the majority of the respondents was well informed about the new Regulation, with 45% claiming to have a great knowledge about it (Presthus *et al.*, 2018).
It is possible to conclude that the GDPR awareness raised over time, as would be expected, due to the proximity of the deadline as time went by. However, all the numbers evidenced in the surveys above are somehow alarming since they show that there were a lot organizations that didn't identify GDPR compliance as a priority.
GDPR awareness is very important because the sooner organizations start the preparation for GDPR, the better prepared they will be to achieve compliance, minimizing risks and reducing the likelihood of being fined. Organizations must get acquainted with the Regulation as soon as possible in order to improve the probability to be among the early adopters in the market, which will drive them to be in a better position than competitors to gain customers' trust (Lopes and Oliveira, 2018; Garber, 2018).
Therefore, the starting point of implementing GDPR is to acquire knowledge about the Regulation in order to understand its requirements and obligations, so that these are taken into account when developing strategies to achieve compliance (Tikkinen-Piri *et al.*, 2018). This can be done internally, by studying the Regulation, or by hiring experts who understand GDPR and are already trained in planning, implementing and maintaining compliance (Boban, 2018).

6.1.3 Data and Documentation

GDPR can be seen as a data governance framework, which encourages organizations to have an overview of the personal data they own, including having plans regarding the collection, use and destruction of data (Hoofnagle *et al.*, 2019). So, every organization must know what personal data do they have, the reason for collection, origin, how was the collection performed and location (Magnusson and Iqbal, 2017). Moreover, it is also important to know how the data is processed (Freitas and Mira da Silva, 2018).
Therefore, an audit of the organizations' information must be performed in order to identify the existing personal data, which will help to implement a good Data Management (Laybats and Davies, 2018).
The literature already presents a list with steps in order to perform this audit. It starts with listing all systems and databases containing personal data, followed by the identification of all data sources and associated communications. Afterwards, a classification matrix should be implemented in order to classify existing data (Magnusson and Iqbal, 2017). However, it does not assess the reason behind the collection of data nor how it was collected. Furthermore, the documentation process is also not referred in this list.
In fact, organizations must document not only the existing data but the processing operations as well (Lopes and Oliveira, 2018). Regarding data flow mapping, in order to know the behaviour of existing data and increase their control over it, organizations can use graphical representations such as Business Process Management Notation (BPMN) (Presthus *et al.*, 2018).
It is also important to review documents such as contracts, privacy policies and consent forms, among others (Lopes and Oliveira, 2018).
Organizations must also adopt the data minimization principle, required by GDPR, which ensures that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (European Commission, 2016).
After having a good data management in place, organizations will be able to answer to deletion and access requests by their customers, as well as Supervisory Authorities requests for compliance demonstration.
By practising high-quality data and document management, which provides a comprehensive and holistic view of all the existing data, organizations can go a step further and implement data analytics (Garber, 2018), in order to maximize the potential and value of their data.

6.1.4 Security Principles and Mechanisms

Privacy and security must be top priorities for every organization, and be embedded in every process and procedure, in order to be one step ahead and achieve compliance (Cavoukian, 2018).

Specifically, the Regulation refers that organizations must implement appropriate privacy protection measures, including technological and operational safeguards, in order to ensure adequate personal data security. Furthermore, this measures must meet the principles of data protection by design and by default (European Commission, 2016).

Privacy by Design (PbD) means that privacy and data protection are embedded throughout the whole life cycle of technologies and applications, since the early design stage until their deployment, use and disposal (Romanou, 2018).

Pseudonymization is one of the measures which meet the principles of PbD. According to GDPR, pseudonymization means the "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information" (European Commission, 2016).

An example of pseudonymization is encryption, which is specifically mentioned in the Regulation and should be the default option in order to protect all stored data (Tankard, 2016). Internal applications should also communicate over encrypted lines (Magnusson and Iqbal, 2017), by using secure transmission protocols to secure the internal network and respective communications (Geko and Tjoa, 2018). Encryption is very important since, if leaked, encrypted data will not be accessible by non-authorized third parties (Krystlik, 2017), ensuring the confidentiality of data.

Organizations should also implement access controls in order to prevent access to data from unauthorized people within the organization itself (Tankard, 2016; Romanou, 2018). This can be achieved with Authentication and Authorization mechanisms.

The adoption of internationally recognized information security standards is also essential (Bindley, 2019). Standards such as ISO 27001 and ISO 27002 may help the organizations to ensure that they have appropriate security measures in place to protect information, enabling best practices to be embedded in their procedures (Tankard, 2016).

Nevertheless, it is important to refer that no security measure guarantees 100% security, so organizations must be ready to deal with the inevitability of a breach (O'Brien, 2016).

6.1.5 Training Awareness

In order to increase the organization's familiarity to GDPR, training sessions should be carried to ensure that everyone follows the internally determined rules and pose no risk to the client's data (Magnusson and Iqbal, 2017). In fact, most of the data breaches are internal and not due to external hacks (Addis and Kutar, 2018). Therefore, data protection training awareness, whether through online courses or face-to-face, is a must for all staff in order to sustain the right levels of compliance (Perry, 2019).

6.1.6 Data Protection Officer

Organizations must designate a Data Protection Officer in case of being a public authority, or when the processing operations require regular and systematic monitoring of data subjects or processing of sensitive data on a large scale.

The DPO will bring expertise regarding information privacy and security, and will help the organization to achieve compliance by giving advice and recommendations, including monitoring compliance with the Regulation (European Commission, 2016).

However, the designation itself is not enough, since a DPO can only help organizations when functionally independent (Drewer and Miladinova, 2018). Furthermore, all the employees must be aware of this new role and responsibilities in order to maximize its contribution (Presthus *et al.*, 2018).

Even though it is not mandatory, the appointment of a DPO can facilitate compliance and become a competitive advantage (Drewer and Miladinova, 2018), and demonstrates that the organization recognizes data as its main asset and the fact that it is crucial to their success (Zerlang, 2017).

6.1.7 Data Protection Impact Assessment

According to the Regulation, Data Protection Impact Assessments must be conducted when "a type of processing is likely to result in high risk to the rights and freedoms of natural persons". Furthermore, Supervisory Authorities must be consulted prior to the processing if the assessment results in a high risk (European Commission, 2016).
Therefore, risk management supports the execution of Data Protection Impact Assessments. It starts by identifying the need for and scope of the DPIA. After that, the threats are identified and risks estimated. Afterwards, risks are evaluated and prioritized in order to identify data protection solutions and countermeasures to mitigate the risks (Tikkinen-Piri *et al.*, 2018; Martín and Kung, 2018). Finally, these measures are communicated to the Supervisory Authorities in order to obtain approval, the so called "prior consultation".

6.2 GDPR Compliance

Complying with GDPR has inherent consequences. It may bring some benefits, but may also impose challenges that organizations need to take into account during the compliance process.

6.2.1 Benefits

Overall, the literature reflects on the following benefits that organizations may achieve by implementing GDPR:

- Proper data management
- Use of data analytics
- Cost reduction
- Increase of reputation and competitiveness

Starting with data management, GDPR is an opportunity for organizations to document processes and procedures (Lopes and Oliveira, 2018), including cleaning and gaining control over their personal data (Presthus *et al.*, 2018), which will contribute to the prevention of personal data abuse and to make data consistent across the organization (Skendzic *et al.*, 2018).
With proper data management, it is also possible to implement data analytics which will produce more accurate and useful insights such as predict future activities, inform changes to business processes or identify new business opportunities (Garber, 2018). Moreover, with an effective data management in place, organizations can reduce data management costs due to the fall in the costs for data storage (Miglicco, 2018; Beckett, 2017), since it facilitates the elimination of redundant data (Perry, 2019). Beyond that, the European Commission estimates a reduction of costs up to 2.3B EUR per year (O'Brien, 2016).
Other potential benefit from being GDPR compliant is to develop a reputation as a trustworthy organization, due to the capability of guaranteeing the safe governance of data, which may lead to attract further businesses and even new customers (Beckett, 2017). The adoption of GDPR requirements may also bring competitive advantage to organizations (Tikkinen-Piri *et al.*, 2018). Finally, compliance may also boost organizations' performance (Garber, 2018) by improving operational efficiency (Miglicco, 2018).

6.2.2 Challenges

GDPR is a very complex and extensive regulation, which is a challenge by itself (Freitas and Mira da Silva, 2018). Additionally, it does not provide specific guidelines regarding technologies that should be used to comply with its requirements (Tikkinen-Piri *et al.*, 2018) and involves

subjectivity (Agarwal, 2016). Thus, the biggest challenge is for organizations to find specific solutions by themselves (Tikkinen-Piri *et al.*, 2018).
Moreover, GDPR compliance may be expensive and time consuming since it requires substantial financial and human resources (Tikkinen-Piri *et al.*, 2018; Addis and Kutar, 2018), increasing administrative work as well (Magnusson and Iqbal, 2017). Therefore, business costs are expected to increase (Lindgren, 2018).
The lack of privacy knowledge and expertise inside organizations, which translates in lack of awareness or in difficulties to understand the Regulation, may also require extra budget in order to recruit privacy experts (Lindgren, 2018). Designating an inside DPO is also a challenge since it is difficult to recruit and retain people with these skills (Tikkinen-Piri *et al.*, 2018; Khan, 2018).
In an online survey, 23% of the respondents referred lack of budget as one of the main challenges in complying with GDPR. 18% also referred lack of required technology to meet the requirements. Regarding requirements, and according to the same survey, the right to erasure is the top challenge for organizations (42%), followed by recording of processing activities (31%) and data protection by design and by default (29%) (Presthus *et al.*, 2018).
Another online survey with 210 Romanian organizations reported that 16% of the respondents referred lack of practical guides or standard procedures and increased bureaucratic effort as encountered challenges during GDPR implementation. 14% also mentioned the complexity of the Regulation. However, and contrary to what would be expected, only 5% referred increased costs (Gabriela *et al.*, 2018).
Due to all the regulatory restrictions of GDPR, compliance may also decrease organization's performance (Marel *et al.*, 2016), which, along with the fact that it is a costly process, may lead some organizations to reduce their product offering to European citizens, in order to step away from the Regulation (Allen *et al.*, 2018).

7. Conclusion, Limitations and Future Work

In this work, we conducted a systematic literature review in order to identify the critical success factors which contribute for GDPR implementation. With the summarized information and analysis performed above, we are able to answer to the proposed research questions, by mapping the topics discussed above with the research questions proposed before.
This mapping is presented below, in Table 3.

Table 3. Mapping between Topics and Research Questions.

	RQ1		RQ2
	RQ1.1	RQ1.2	
6.1 GDPR Implementation		X	
6.2 GDPR Compliance	X		X

With section 6.1 (GDPR Implementation), by describing some implementation roadmaps and key points in GDPR implementation, we were able to identify which are the enablers which may ease the compliance process, which answers RQ1 (RQ1.2, specifically).
With section 6.2 (GDPR Compliance), by identifying the challenges in complying with the Regulation, we were able to identify which are the barriers that may difficult the compliance process, which answers RQ1 as well (RQ1.1, specifically). Furthermore, we also identified the benefits of complying with GDPR, which answers to RQ2.

Hence, answering the proposed research questions:

- RQ1.1 - Which are the barriers for GDPR implementation?

The Regulation itself. It is complex, extensive and involves subjectivity. The compliance process is also extensive, time consuming and requires substantial financial and human resources.

The lack of privacy knowledge and expertise, required technology, and practical guides or standard procedures are also barriers.
The most challenging requirements to comply with are the right to erasure, recording of processing activities, implement data protection by design and by default and designate a DPO.

- RQ1.2 - Which are the enablers for GDPR implementation?

Design an implementation roadmap, perform GDPR analysis, identify risks, document processing operations, apply a robust data management, implement appropriate privacy security measures, carry training sessions, designate a DPO and conduct DPIAs.

- RQ2 - What are the benefits of complying with GDPR?

Proper Data Management, use of data analytics, increase of reputation and competitiveness, and increase of transparency and awareness.

The summarization of the identified critical success factors, which is the answer to RQ1, is presented below, in Table 4.

Table 4. The Critical Success Factors of GDPR Implementation.

Barriers	**Enablers**
GDPR extension	Implementation roadmap
GDPR complexity	GDPR analysis
GDPR subjectivity	Risks identification
Lack of privacy knowledge and expertise	Data management
Lack of budget	Process documentation
Lack of human resources	Data Protection Officer
Lack of required technology	Security measures and mechanisms
Lack of practical guides or standard procedures	Training awareness

By identifying the critical success factors, organizations are better prepared to achieve compliance, by prioritizing the GDPR implementation enablers, while being careful regarding the barriers in order to avoid mistakes and pitfalls throughout the compliance process.
Regarding limitations, we were not able to gather sufficient information and present a robust conclusion regarding specific topics, such as practical outcomes, due to the fact that GDPR is a recent subject and there are few case studies presenting real GDPR implementations. Additionally, we did not take into account the references of the selected documents as eligible documents to the review due to scalability issues.
In the future, we will validate and deepen the identified critical success factors using proper research methods such as interviews and surveys, among others. It would also be interesting to determine the relevance of each critical success factor in implementing GDPR. Furthermore, future research may also focus on defining a robust implementation roadmap, for organizations to use as a guideline in order to ease GDPR implementation.

References

Addis, M.C. and Kutar, M. (2018), "The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness", in *UK Academy for Information Systems Conference*, United Kingdom, pp. 1-23.

Agarwal, S. (2016), "Towards dealing with GDPR uncertainty", in *11th IFIP Summer School on Privacy and Identity Management*, Sweden, pp. 1-7.

Allen, D. *et al.* (2018), "Some Economic Consequences of the GDPR", *SSRN Electronic Journal*, pp. 1-9.

Beckett, P. (2017), "GDPR compliance: your tech department's next big opportunity", *Computer Fraud & Security*, Vol. 2017 No. 5, pp. 9-13.

Bindley, P. (2019), "Joining the dots: how to approach compliance and data governance", *Network Security*, Vol. 2019 No. 2, pp. 14-16.

Boban, M. (2018), "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*, Rome, pp. 161-169.

Boynton, A.C. and Zmud, R.W. (1984), "An Assessment of Critical Success Factors", *Sloan Management Review*, Vol. 25 No. 4, pp. 17-27.

Bullen, C.V. and Rockart, J.F. (1981), "A Primer on Critical Success Factors", working paper 69, Sloan School of Management, Massachusetts Institute of Technology, Massachusetts, USA, June 1981.

Cavoukian, A. (2018), "Staying one step ahead of the GDPR: Embed privacy and security by design", *Cyber Security: A Peer-Reviewed Journal*, Vol. 2 No. 2, pp. 172-180.

Dell (2016), "GDPR: Perceptions and Readiness. A Global Survey of Data Privacy Professionals at companies with European Customers", available at: https://www.eurocloud.fr/wp-content/uploads/2016/10/gdpr.pdf (accessed 19 January 2019).

Drewer, D. and Miladinova, V. (2018), "The canary in the data mine", *Computer Law & Security Review*, Vol. 34, pp. 806-8015.

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

Freitas, M.C. and Mira da Silva, M. (2018), "GDPR Compliance in SMEs: There is much to be done", *Journal of Information Systems Engineering & Management*, Vol. 34 No. 4, pp. 30.

Gabriela, G., Cerasela, S.E. and Alina, C.A. (2018), "The EU General Data Protection Regulation Implications for Romanian Small and Medium-Sized Enterprises", *Ovidius University Annals (Economic Sciences Series)*, Vol. 18 No. 1, pp. 88-91.

Garber, J. (2018), "GDPR – compliance nightmare or business opportunity?", *Computer Fraud & Security*, Vol. 2018 No. 6, pp. 14-15.

Geko, M. and Tjoa, S. (2018), "An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security", in *Proceedings of the Central European Cybersecurity Conference*, Slovenia.

Hoofnagle, C.J., Sloot, B. and Borgesius, F.Z. (2019), "The European Union general data protection regulation: what it is and what it means", *Information & Communications Technology Law*, Vol. 28 No. 1, pp. 65-98.

Huth, D. (2017), "A Pattern Catalog for GDPR Compliant Data Protection", in *Practice of Enterprise Modelling (PoEM*), Belgium, pp. 34-40.

Khan, J. (2018), "The need for continuous compliance", *Network Security*, Vol. 2018 No. 6, pp. 14-15.

Kitchenham, B. (2004), "Procedures for Performing Systematic Reviews", Department of Computer Science, Keele University, United Kingdom.

KPMG (2017), "O Impacto do Regulamento Geral de Protecção de Dados em Portugal", available at: https://assets.kpmg/content/dam/kpmg/pt/pdf/pt-2017-rgpd.pdf (accessed 19 January 2019).

Krystlik, J. (2017), "With GDPR, preparation is everything", *Computer Fraud & Security*, Vol. 2017 No. 6, pp. 5-8.

Laybats, C. and Davies, J. (2018), "GDPR: Implementing the regulations", *Business Information Review*, Vol. 35 No. 2, pp. 81-83.

Leidecker, J.K. and Bruno, A.V. (1984), "Identifying and Using Critical Success Factors", *Long Range Planning*, Vol. 17 No. 1, pp. 23-32.

Lindgren, P. (2018), "GDPR Regulation Impact on Different Business Models and Businesses", *Journal of Multi Business Model Innovation and Technology*, Vol. 4 No. 3, pp. 241-254.

Lopes, I.M. and Oliveira, P. (2018), "Implementation of the General Data Protection Regulation: A Survey in Health Clinics", in *13th Iberian Conference on Information Systems and Technologies*, Spain, pp. 1-6.

Magnusson, L. and Iqbal, S. (2017), "Implications of EU-GDPR in Low-Grade Social, Activist and NGO Settings", in *International Conference on Computer Science and Communication Engineering and Information Systems and Security*, Albania, pp. 91-97.

Marel, E. *et al.* (2016), "A methodology to estimate the costs of data regulations", *International Economics*, Vol. 146, pp. 12-39.

Martín, Y. and Kung, A. (2018), "Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering", in *IEEE European Symposium on Security and Privacy*, United Kingdom, pp. 108-111.

Miglicco, G. (2018), "GDPR is here and it is time to get serious", *Computer Fraud & Security*, Vol. 2018 No. 9, pp. 9-12.

O'Brien, R. (2016), "Privacy and security: The new European data protection regulation and it's data breach notification requirements", *Business Information Review*, Vol. 33 No. 2, pp. 81-84.

Perry, R. (2019), "GDPR – project or permanent reality?", *Computer Fraud & Security,* Vol. 2019 No. 1, pp. 9-11.

Presthus, W., Sørum, H. and Andersen, L.R. (2018), "GDPR Compliance in Norwegian Companies", in *Norwegian Conference for IT Use in Organisations (NOKOBIT)*, Norway, pp. 1-15.

Romanou, A. (2018), "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise", *Computer Law & Security Review*, Vol. 34, pp. 99-110.

Seo, J. *et al.* (2018), "An Analysis of Economic Impact on IoT under GDPR", in *8th International Conference on ICT Convergence (ICTC)*, Korea, pp. 879-881.

Sirur S., Nurse, J. and Webb H. (2018), "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)", in *25th ACM Conference on Computer and Communication Security*, Canada, pp. 1-8.

Skendzic, A., Kovacic, B. and Tijan, E. (2018), "General Data Protection Regulation - Protection of Personal Data in an Organisation", in *International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Croatia, pp. 1370-1375.

Tankard, C. (2016), "What the GDPR means for businesses", *Network Security*, Vol. 2016 No. 6, pp. 5-8.

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

Webster, J. and Watson, R.T. (2002), "Writing a Literature Review", *MIS Quarterly*, Vol. 26 No. 2, pp. 13-23.

Zerlang, J. (2017), "GDPR: a milestone in convergence for cyber-security and compliance", *Network Security*, Vol. 2017 No. 6, pp. 8-11.