The Critical Success Factors of GDPR Implementation

Gonçalo Villa de Freitas de Almeida Teixeira
Instituto Superior Técnico (Taguspark)
Universidade de Lisboa
Lisboa, Portugal
goncalo.almeida.teixeira@tecnico.ulisboa.pt

Abstract

The new digital era we live in today, supported by the technology evolution in the last years, leveraged the consumption of data to a new level, being a threat to people's privacy. To prevent the misuse of personal data by organizations and to adapt to the new digital landscape, the European Union proposed the General Data Protection Regulation with a set of requirements and obligations for organizations to put in practice and to comply with regarding the processing of personal data.

In order to identify the critical success factors which contribute for implementing GDPR, a Delphi study with 10 experts was conducted, based on a list of critical success factors previously identified in the literature through a systematic literature review. This list was validated and further elaborated, resulting in a top10 of both enablers and barriers in GDPR implementation, with a moderate agreement among the participants.

Keywords: GDPR; Critical success factors; Enablers; Barriers; Systematic literature review; Delphi.

1. Introduction

The evolution of technology over the years enabled the increasing collection of personal data by organizations, which have inherent security challenges and risks. To protect citizens' personal data and privacy, regulators are adapting regulations to the present digital economy [1].

To prevent the misuse of personal data by organizations and to address the privacy issues emerging from this new digital era [2], the European Commission proposed the General Data Protection Regulation (GDPR), with a set of obligations regarding the storing, processing, collecting and disclosing of data [3].

GDPR replaces and repeals the European Union Data Protection Directive (DPD), which was adopted in 1995 and no longer meets the privacy requirements of the new digital landscape [4], and introduces significant changes regarding personal data and privacy, aiming to give more control to citizens over their personal data to ensure a harmonized, unified and sustainable approach to data protection [5].

Enforced from May 25, 2018, the regulation applies to any organization that processes European citizens' data and may impose hefty fines when non-compliance is detected [6]. To comply with GDPR requirements and avoid fines, organizations need to review their processes and procedures, which will impact their businesses and impose a lot of changes and adaptions. Although many organizations understand the importance of complying with the new regulation, the uncertainty around GDPR has led to some divided approaches [7] because GDPR is not prescriptive regarding solutions to achieve compliance, not providing specific guidelines to implement its requirements [4].

Therefore, and to help organizations and ease the compliance process, a systematic literature review (SLR) was conducted to identify the critical success factors (CSFs) that contribute for GDPR implementation by identifying the enablers and barriers in the compliance process. Furthermore, this list of CSFs was further validated and elaborated through a Delphi study, where 10 experts identified the critical success factors of GDPR implementation, achieving a moderate consensus.

The systematic literature review was published in the Digital Policy, Regulation and Governance journal (Q2), and the Delphi study was submitted in the Law, Innovation and Technology journal (Q1).

This document is structured as follows. Section 2 introduces the Theoretical Background, including both the regulation and critical success factors. Section 3 presents the chosen research methodologies. After that, both methodologies are explained in detail, including its results and discussion. First, in Section 4, the SLR results are revealed. Then, in Section 5, Delphi results are presented as well, with further analysis and discussion. Finally, Section 6 concludes the document.

2. Theoretical Background

In this section, we will introduce the two core concepts of this work: the General Data Protection Regulation (GDPR) and critical success factors (CSFs).

2.1. General Data Protection Regulation (GDPR)

GDPR was enforced on 25 May 2018 [6] and introduced several changes to the current data protection laws, updating the regulatory framework to face the challenges of the information age [8], thus replacing and repealing the Data Protection Directive [6]. Besides that, it is a regulation, meaning that it does not require additional national legislation to be implemented, having already binding legal force [6] and being applied directly and universally in all Member States, which provides a unified and harmonized set of data protection policies [9].

The aim of the regulation is to improve the level of personal data protection, by strengthening data protection rights of individuals and imposing stricter obligations to organizations, and to facilitate the free flow of personal data [10]. Furthermore, it offers a more modern and wide-reaching approach to protection personal data [11].

The regulation introduces a lot of changes and a number of new obligations and data protection principles [12], from data minimization and limitation to data protection by design and by default [4]. These requirements also include the appointment of a qualified Data Protection Officer (DPO), which must have a comprehensive overview of the data processing operations of the organization [13], the realization of Data Protection Impact Assessments (DPIA) whenever a processing of personal data may result in a high risk for the citizens, and report data breaches within 72 hours to supervisory authorities [6].

Due to the extra territorial scope of GDPR, organizations located within the EU or holding or processing European citizens' personal data are under GDPR scope [14], and therefore subject to the respective obligations and requirements [15], meaning that these data protection rules may apply to non-European organizations as well if these provide services to European citizens [8].

Failing to comply with GDPR may impose hefty fines to organizations, which can lead up to €20 million or 4% of the annual turnover, whichever is higher [6]. In order to be compliant, organizations need to review their policies and processes, and adopt new practices and procedures by combining technical solutions with organizational controls [16], to ensure they process, hold and collect data in a GDPR-manner [6].

2.2. Critical Success Factors (CSFs)

Introduced by Rockart in a Harvard Business Review article in 1979 [17], critical success factors (CSFs) are the key areas in which satisfactory results are necessary to ensure a successful performance and for the organization to achieve its goals [18].

CSFs represent a conceptualization of critical subjects and help ensure that organizations' needs are addressed, helping the business in prioritizing information system projects [19]. Therefore, by identifying CSFs, organizations can assess the threats and identify the opportunities in a specific project, including characteristics, conditions and variables [20], to develop a robust strategic plan for that project implementation [19].

In this work, we distinguish critical success factors between enablers and barriers.

2.2.1. Enablers

Often called facilitators, enablers are the factors that help a project development and progress [21], enabling its successful and effective implementation [22,23], being therefore critical to the project's success. Enablers can also help to prevent or even overcome potential barriers [24,25]. Thus, organizations must enhance and prioritize the existing enablers to implement a project in the most effective way.

2.2.2. Barriers

Barriers, also called inhibitors, are the factors that do not necessarily conduct to a project failure but hinder a project implementation [24], inhibiting an effective and successful project implementation [22, 24]. Therefore, organizations should make an effort in order to avoid, minimize or mitigate the identified barriers [22, 25].

3. Research Methodologies

This work was conducted using a combination of two research methods, systematic literature review and Delphi, mixing these two different methods into a single study.

3.1. Systematic Literature Review (SLR)

A systematic literature review (SLR) is a form of study used to identify, analyze and interpret all the available evidence in the literature regarding a specific topic or question, using a trustworthy, rigorous and auditable methodology, to synthesize the existing work in a systematic, comprehensive, reproducible and unbiased manner [26].

SLRs provide a context and background for subsequent research, creating a starting point and shaping the directions for future research [27] in order to develop new theories [28]. The applied SLR methodology structure is based on Kitchenham [26], complemented by Webster and Watson [29].

The SLR was chosen as one of the research methodologies since it was our intention to summarize the existing evidence regarding GDPR implementation, to identify the critical success factors of GDPR implementation present in the literature, and to use it as a starting point for the Delphi method. The SLR results are presented in Section 4.

3.2. The Delphi Method

The Delphi method is an iterative group communication process that collects and refines the anonymous opinions of the experts, by using a series of questionnaires, with the aim to reach convergence and consensus [30,31], enabling a group interaction without the need of face to face meetings [30].

As mentioned above, anonymity is one of the important features of Delphi, in order to encourage a true and controlled debate [32], allowing the participants to freely express their opinions without any kind of pressure or dominance from other participants [31].

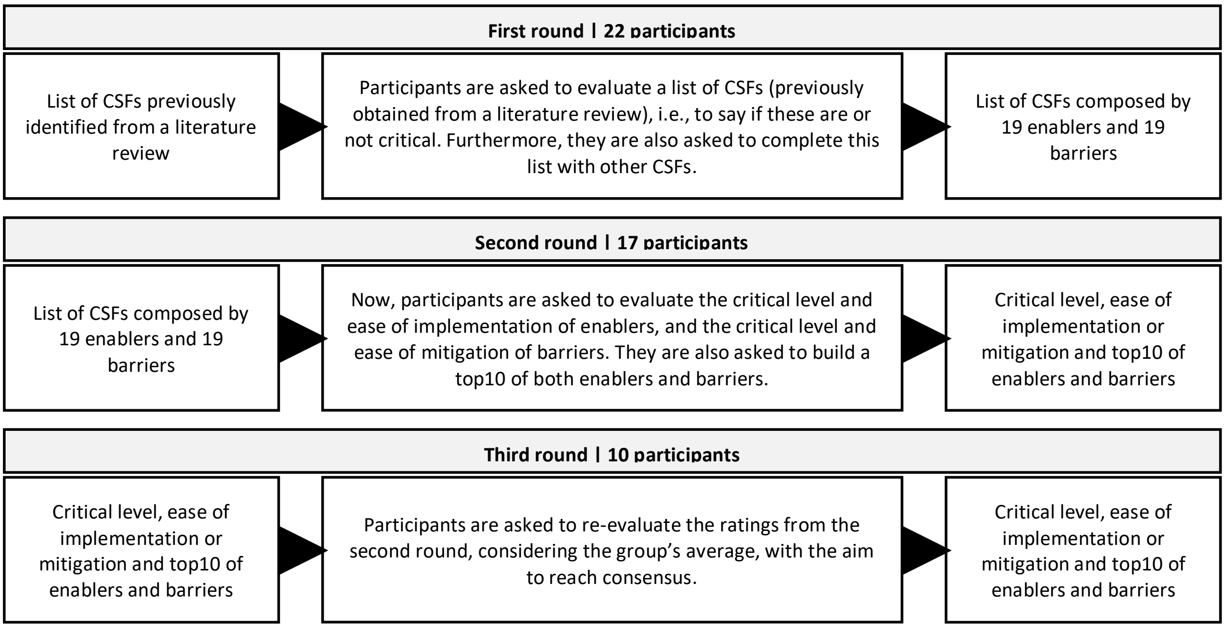
The next sections present the panel of experts and the overview of the applied. The Delphi results, as well as its discussion, are presented in Section 5.

3.2.1. Participants

The selection of participants plays a key role on a successful Delphi, because the results of the investigation depend on the knowledge and opinions of the experts [31, 32]. For this investigation, Data Protection Officers and people with privacy and data protection skills or with experience in implementing GDPR were considered eligible as experts. Some of the participants were provided by APDPO (a Portuguese DPOs association), while the others were contacted through LinkedIn.

3.2.2. Rounds

Below, Figure 1 describes the applied Delphi, which was performed between April 1 and May 13.



First round | 22 participants

List of CSFs previously identified from a literature review

Participants are asked to evaluate a list of CSFs (previously obtained from a literature review), i.e., to say if these are or not critical. Furthermore, they are also asked to complete this list with other CSFs.

List of CSFs composed by 19 enablers and 19 barriers

Second round | 17 participants

List of CSFs composed by 19 enablers and 19 barriers

Now, participants are asked to evaluate the critical level and ease of implementation of enablers, and the critical level and ease of mitigation of barriers. They are also asked to build a top10 of both enablers and barriers.

Critical level, ease of implementation or mitigation and top10 of enablers and barriers

Third round | 10 participants

Critical level, ease of implementation or mitigation and top10 of enablers and barriers

Participants are asked to re-evaluate the ratings from the second round, considering the group's average, with the aim to reach consensus.

Critical level, ease of implementation or mitigation and top10 of enablers and barriers

Figure 1: Delphi study

The Delphi method can be continuously iterated until consensus is achieved. However, the higher the number of rounds, the lower the response rate [31]. Three rounds are enough to collect the needed information and to achieve consensus in most cases [33], with each round being developed based on the results of the previous round [31].

Regarding the scores given by the participants in the second and thirds rounds:

- Critical level was given a score between 1 and 5, where 1 means less critical and 5 more critical;
- Ease of implementation was given a score between 1 and 5, where 1 means easy to implement and 5 hard to implement;
- Ease of mitigation was given a score between 1 and 5, where 1 means easy to mitigate and 5 hard to mitigate;
- In both top10, 1 means the most important CSF and 10 the less important one, within the 10 most important factors

The questionnaires were provided online, through Google Spreadsheets, to reduce communication delays and burdens [32], giving the participants the flexibility to answer them digitally and in their own time [34].

4. Systematic Literature Review

After applying a strict review protocol, from 959 papers identified in the literature, only 32 were considered eligible to perform the review.

From these 32 articles, we were able to identify the critical success factors present in the literature, including enablers and barriers, as is presented below in Table 1.

Table 1: Critical success factors from the literature

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

5. The Delphi Method

This section describes the results and discusses the core findings of the performed Delphi, which includes the identification of the critical success factors of GDPR implementation, including both enablers and barriers.

5.1. Participants

The Delphi started with 22 experts but only 10 concluded the whole investigation, which is a reasonable number as there are Delphis in the literature with participants ranging from 4 to 171 [31].

5.2. Rounds

As already stated, the starting point for this Delphi study was the systematic literature review previously described in Section 4, where 8 enablers and 8 barriers regarding GDPR implementation were identified.

The Delphi study was executed in three rounds.

5.2.1. Round 1

In the first round, the participants were asked to validate the critical success factors from Table 1, i.e., to say if these are or not critical regarding GDPR implementation. Considering a threshold of two-thirds (66%) of acceptance rate, the enabler Data Protection Officer (63,64%) and the barriers GDPR extension (50%), GDPR complexity (59,09%) and GDPR subjectivity (54,55%) were further eliminated from the CSFs list.

Furthermore, the participants were also asked to elaborate on this list by providing additional CSFs regarding GDPR implementation. By combining all the different inputs given by the participants from the first round, a list with 19 enablers and 19 barriers was elaborated (Table 2, below). This list will be the baseline of this Delphi study, and will be evaluated in the remaining rounds according to the parameters referred in Section 3.2.2.

Table 2: Critical success factors of GDPR implementation

Critical Success Factors		CSF ID
Enablers	Alignment of DPO with other enterprise roles	E1
	Certification	E2
	Collaboration between IT and Legal Departments	E3
	Data management	E4
	Data protection and security policies	E5
	Data Protection Impact Assessments	E6
	Enterprise engagement	E7
	GDPR analysis	E8
	Implementation by external consultant	E9
	Implementation roadmap	E10
	Information Security Management System (ISMS)	E11
	Monitorization	E12
	Organizational culture	E13
	Process documentation	E14
	Right level of technology	E15
	Risks identification	E16
	Security measures and mechanisms	E17
	Top management sponsorship and involvement	E18
	Training awareness	E19

Critical Success Factors		CSF ID
Barriers	Absence of a well-defined organizational culture	B1
	Absence of planification	B2
	Change resistance	B3
	Consider GDPR a burden instead of an advantage	B4
	Data availability/accessibility	B5
	GDPR misconception	B6
	Internal politics	B7
	Lack of budget	B8
	Lack of human resources	B9
	Lack of KPIs	B10
	Lack of management commitment and support	B11
	Lack of management knowledge	B12
	Lack of practical guides or standard procedures	B13
	Lack of privacy knowledge and expertise	B14
	Lack of required technology	B15
	Lack of security practices	B16
	Lack of training	B17
	Organizational culture	B18
	Poor compliance assessment	B19

5.2.2. Round 2

In the second round, participants were asked to evaluate the critical success factors identified from the previous round (Table 2). Enablers were evaluated by critical level and ease of implementation, while barriers were evaluated by critical level and ease of mitigation. Furthermore, participants were also asked to build a top10 of both enablers and barriers, based on the critical level and ease of implementation/mitigation values. These results are presented in Table 3 (enablers) and Table 4 (barriers), and the CSFs are ordered by rank.

Table 3: Enablers' critical level, ease of implementation and rank from rounds 2 and 3

Enablers	Critical Level			Ease of Implementation			Rank		
	Rounds		Δ	Rounds		Δ	Rounds		Δ
	2	3		2	3		2	3	
Top management sponsorship and involvement (E18)	4,41	4,40	-0,01	3,59	4,10	0,51	1	1	---
Risks identification (E16)	4,06	4,20	0,14	3,35	3,40	0,05	3	2	↑1
Data protection and security policies (E5)	4,24	4,40	0,16	3,06	3,30	0,24	4	3	↓1
Collaboration between IT and Legal Departments (E3)	4,12	3,80	-0,32	2,88	2,70	-0,18	2	4	↑2
Security measures and mechanisms (E17)	3,94	3,80	-0,14	3,47	3,60	0,13	5	5	---
Organizational culture (E13)	3,88	3,80	-0,08	3,76	4,00	0,24	6	6	---
Enterprise engagement (E7)	3,94	3,80	-0,14	3,59	3,90	0,31	7	7	---
Data Protection Impact Assessments (E6)	4,18	4,20	0,02	3,18	3,40	0,22	8	8	---
Training awareness (E19)	4,24	4,00	-0,24	2,76	2,80	0,04	9	9	---
Right level of technology (E15)	3,59	3,60	0,01	3,47	3,60	0,13	10	10	---
GDPR analysis (E8)	3,35	2,90	-0,45	2,71	2,60	-0,11	16	11	↑5
Process documentation (E14)	3,65	3,50	-0,15	2,47	2,60	0,13	14	12	↑2
Information Security Management System (ISMS) (E11)	3,71	3,50	-0,21	3,47	3,50	0,03	11	13	↓2
Alignment of DPO with other enterprise roles (E1)	3,41	3,00	-0,41	2,76	2,80	0,04	15	14	↑1
Monitorization (E12)	4,06	4,00	-0,06	3,00	3,10	0,10	13	15	↓2
Implementation by external consultant (E9)	2,94	2,40	-0,54	2,41	2,20	-0,21	17	16	↑1
Implementation roadmap (E10)	3,41	3,30	-0,11	2,65	2,70	0,05	12	17	↓5
Data management (E4)	3,94	3,70	-0,24	3,06	3,10	0,04	18	18	---
Certification (E2)	2,59	2,50	-0,09	2,94	3,00	0,06	19	19	---

5.2.3. Round 3

In the third round, participants were asked to re-evaluate their second round ratings, considering the groups' average. These results are also presented in Tables 3 (enablers) and 4 (barriers), and are also ordered by rank.

Table 4: Barriers' critical level, ease of mitigation and rank from rounds 2 and 3

Barriers	Critical Level			Ease of Mitigation			Rank		
	Rounds		Δ	Rounds		Δ	Rounds		Δ
	2	3		2	3		2	3	
Lack of management commitment and support (B11)	4,29	4,40	0,11	3,82	4,10	0,28	1	1	---
Change resistance (B3)	3,88	3,80	-0,08	3,47	3,80	0,33	2	2	---
Lack of security practices (B16)	4,12	4,00	-0,12	3,35	3,40	0,05	3	3	---
Lack of budget (B8)	3,76	3,90	0,14	3,65	3,80	0,15	5	4	↑1
Lack of privacy knowledge and expertise (B14)	4,00	4,00	0,00	2,94	2,90	-0,04	4	5	↓1
Organizational culture (B18)	3,82	3,80	-0,02	3,76	3,90	0,14	6	6	---
Data availability/accessibility (B5)	4,00	4,00	0,00	3,29	3,30	0,01	7	7	---
Lack of required technology (B15)	3,76	3,80	0,04	3,41	3,40	-0,01	8	8	---
Lack of human resources (B9)	3,76	3,90	0,14	3,71	3,60	-0,11	9	9	---
Poor compliance assessment (B19)	3,59	3,30	-0,29	3,00	3,10	0,10	10	10	---
Internal politics (B7)	3,29	3,20	-0,09	2,76	2,60	-0,16	16	11	↑5
Absence of a well-defined organizational culture (B1)	3,76	3,70	-0,06	3,35	3,30	-0,05	11	12	↓1
Lack of management knowledge (B12)	3,44	3,30	-0,14	3,06	3,00	-0,06	17	13	↑4
Consider GDPR a burden instead of an advantage (B4)	3,41	3,00	-0,41	3,24	3,00	-0,24	13	14	↓1
Lack of practical guides or standard procedures (B13)	3,88	3,70	-0,18	2,71	2,70	-0,01	15	15	---
Lack of training (B17)	3,88	3,60	-0,28	2,53	2,60	0,07	12	16	↓4
Lack of KPIs (B10)	3,35	3,30	-0,05	2,94	2,80	-0,14	18	17	↑1
Absence of planification (B2)	3,71	3,50	-0,21	3,00	3,10	0,10	14	18	↓4
GDPR misconception (B6)	2,76	2,70	-0,06	2,41	2,10	-0,31	19	19	---

5.3. Discussion

Starting with the first round results (Appendix A), from the 16 critical success factors identified in the literature, only 4 of them were excluded from the list according to the defined threshold (one enabler and three barriers).

5.3.1. Enablers

We will now discuss the results from second and third rounds, regarding the enablers, by analysing their critical level, ease of implementation and rank values.

Critical Level

The critical level values do not differ much between the two rounds, with a mean of deltas of -0,15.

It is possible to observe that there are two different scenarios in and out of the top10. The critical level values of the best positioned enablers have a small variation from round two to round three, with a mean of -0,06.

However, it is possible to find, out of the top10, a big discrepancy regarding critical level values between the two rounds in almost all the enablers, with a mean of -0,25, showing that there is more convergence on the most important enablers (within the top10).

Moreover, almost all the enablers with the highest critical values are on the top 10, with two exceptions: Monitorization has one of highest critical level values (4,00) but is ranked in the 15th position; Data management (18th) has a higher critical level value than Right level of technology (10th).

The enablers' average critical level value is 3,62.

Ease of Implementation

The ease of implementation values follows the same tendency, with low variations between rounds two and three, with a mean of deltas of 0,10.

Contrary to what happens with the critical level values, most of the enablers (16 out of 19) have positive deltas, meaning that the ease of implementation values increased from round two to round three.

Eight of the ten enablers with the highest ease of implementation values are within the top 10, with the following exceptions: Information Security Management Systems (ISMS) has one of the highest ease of implementation values but is ranked in the 13th position; Training awareness and Collaboration between IT and Legal Departments are within the enablers' top10 (9th and 4th, respectively) but have some of the lower ease of implementation values.

The enablers' ease of implementation average value is 3,18.

Rank

Below, in Figure 2, is represented the relationship between the enablers' critical level and ease of implementation values from round 3. The blue dots are the enablers' top10.

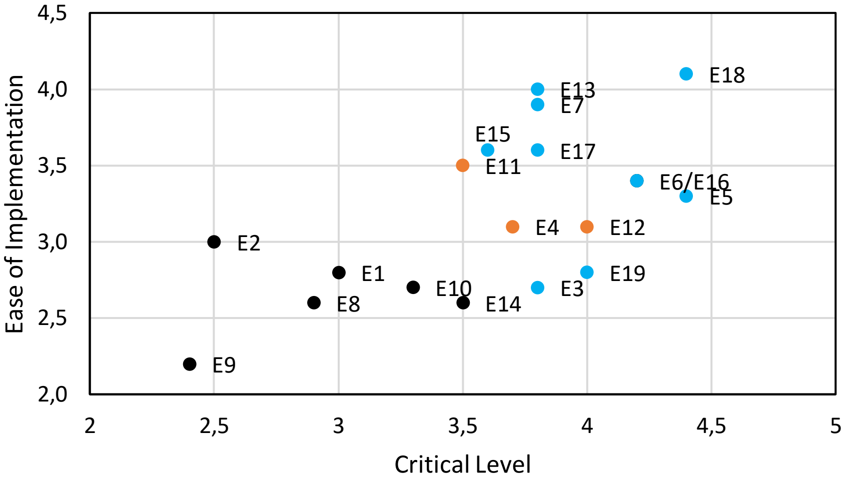


Figure 2: Critical level and ease of implementation of GDPR implementation enablers

As it is possible to see, almost all the top10 enablers have the higher critical level x ease of implementation scores. However, there are some exceptions, namely E3 (Collaboration between IT and Legal Departments) and E19 (Training awareness), which are outliers.

The orange dots, which are the enablers E4 (Data management), E12 (Monitorization) and E11 (Information Security Managements Systems (ISMS)) have a best score than the outliers, but are not on the top10.

In fact, E4 (Data management) is one of the worse enablers concerning the rank, being placed in the 18th position, even though it has critical level and ease of implementation values near the enablers' average values.

The variations within the enablers' rank are presented in Figure 3.

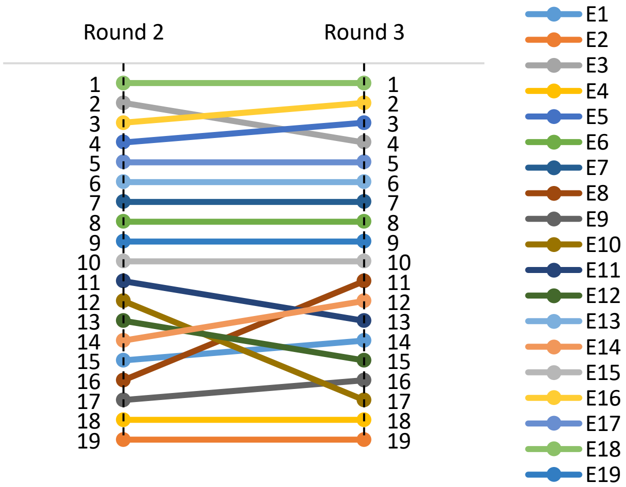


Figure 3: Enablers' rank variations between round 2 and 3

Indeed, there are some variations, but mainly out of the top10. The top10 remained with the same enablers through the second and third rounds.

Moreover, from the enablers identified in the literature which were considered critical by the experts, only three are placed within the top10: E16 (Risks identification), E17 (Security measures and mechanisms) and E19 (Training awareness).

5.3.2. Barriers

Regarding the barriers, we will now discuss the results from second and third rounds, by analyzing their critical level, ease of mitigation and rank values.

Critical Level

Once again, the critical values did not differ much between the second and third rounds as well, with a mean of deltas of -0,08. Similar to what happened with the enablers' critical level values, it is also possible to observe two scenarios, in and out of the top10. The critical level values of the barriers' top10 have a small variation between second and third rounds, with a mean of -0,01.

However, there is a big variation within the barriers out of the top10, with a mean of -0,17, showing once again that there is more convergence on the most important barriers (within the top10).

Furthermore, almost all the barriers in the top10 have the highest critical level values, except for Poor compliance assessment (10th position), which has one of the lowest critical level values.

The barriers' critical level average value is 3,63, which is very similar to the enablers' average.

Ease of Mitigation

The ease of mitigation values follows the same pattern as well, with low variations between rounds two and three, with a minimal delta of 0,005.

Eight of the ten barriers with the highest ease of mitigation values are indeed on the top10 rank. There are, therefore, two exceptions: Lack of privacy knowledge and expertise has one of the lowest values regarding ease of mitigation but is ranked in the 5th position; Poor compliance assessment (11th position) is tied with Absence of planification (10th position). However, the second one had a lower standard deviation.

The barriers' ease of mitigation average value is 3,18.

Rank

Below, in Figure 4, is represented the relationship between the barriers' critical level and ease of mitigation results from round 3. The highlighted blue dots are the barriers' top10.

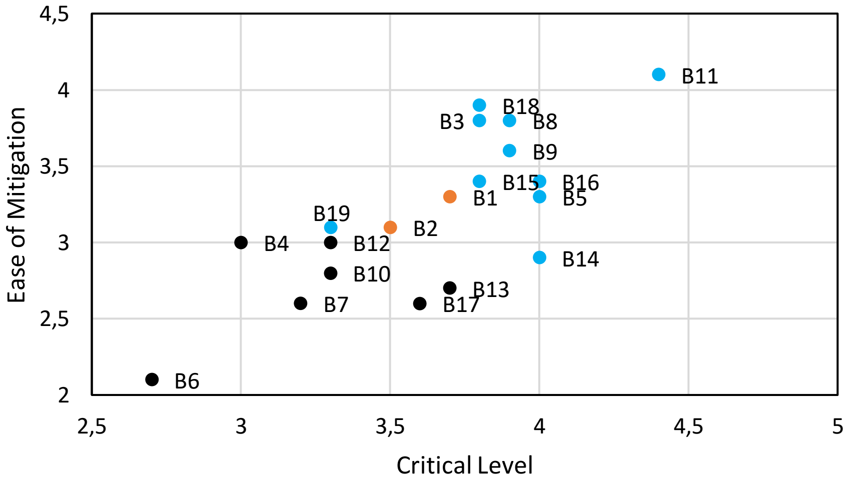


Figure 4: Critical level and ease of mitigation of GDPR implementation barriers

As it is possible to see, almost all the top10 barriers have the higher critical level x ease of mitigation rates. However, B19 (Poor compliance assessment) is an outlier.

The orange dots, representing the barriers B1 (Absence of a well-defined organization culture) and B2 (Absence of planification), have a best combined score than B19, but are not on the top10.

In fact, B2 is almost the worst barrier regarding the rank, being placed in the 18th position, even though its critical level and ease of mitigation values are near the barriers' average values. This also happens with one enabler, as already reported.

The variations within the barriers' top10 are presented in Figure 5.

There are some variations out of the top10. However, the barriers' top10 was identical between the second and third round, with only one shift between B8 and B14. Moreover, from the barriers identified in the literature which were considered critical by the experts, only B13 (Lack of practical guides or standard procedures) is not placed within the top10.

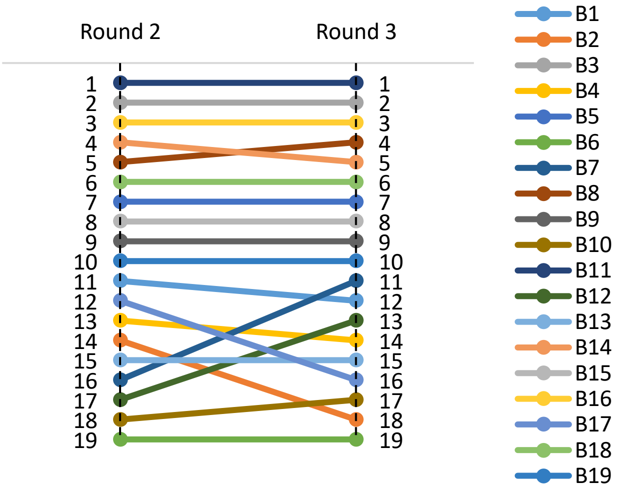


Figure 5: Barriers' rank variations between round 2 and 3

5.3. Consensus

The Kendall's W coefficient of concordance is used to measure the consensus between the participants. Its values range between 0 and 1, where 0 stands for no consensus and 1 indicates perfect consensus [35]. The enablers have a W value of 0.6, while the barriers have a W value of 0.5, which can be considered a moderate agreement [35] in both parameters.

6. Conclusion

With the information summarized above and further analysis and discussion, it is possible to identify the ten most important enablers in implementing GDPR regarding its critical level and ease of implementation, and the ten most important barriers in GDPR implementation regarding its critical level and ease of mitigation, in Table 5.

Table 5: Enablers of GDPR implementation

Rank	Enablers	Barriers
1	Top management sponsorship and involvement	Lack of management commitment and support
2	Risks identification	Change resistance
3	Data protection and security policies	Lack of security practices
4	Collaboration between IT and Legal Departments	Lack of budget
5	Security measures and mechanisms	Lack of privacy knowledge and expertise
6	Organizational culture	Organizational culture
7	Enterprise engagement	Data availability/accessibility
8	Data Protection Impact Assessments	Lack of required technology
9	Training awareness	Lack of human resources
10	Right level of technology	Poor compliance assessment

These final lists of critical success factors provide to organizations a small sample of what to focus on the most when implementing GDPR. Nevertheless, the identified enablers and barriers throughout the Delphi study provide a broader picture regarding what is critical, according to the panel of experts, in the compliance process.

By identifying these CSFs, organizations can prioritize the enablers, while being careful regarding the barriers to avoid mistakes and pitfalls throughout the compliance process, being better prepared to achieve compliance in the most efficient way.

References

[1] S. Agarwal, "Towards dealing with GDPR uncertainty", in *11th IFIP Summer School on Privacy and Identity Management*, 2016.

[2] E. Politou, A. Michota, E. Alepis, M. Pocs, and C. Patsakis, "Backups and the right to be forgotten in the GDPR: An unease relationship", *Computer Law & Security Review*, vol. 34, no. 6, pp. 1247-1257, 2018.

[3] G. Gabriela, S. E. Cerasela, and C. M. Alina, "The EU General Data Protection Regulation Implications for Romanian Small and Medium-Sized Enterprises", *Ovidius University Annals (Economic Science Series)*, vol. 18, no. 1, pp. 88-91, 2018.

[4] C. Tikkinen-piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer Law & Security Review*, vol. 34, pp. 134-153, 2018.

[5] 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*, pp. 161-169, 2018.

[6] 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 Data Protection Regulation)”, *Official Journal of the European Union*, vol. 59, pp. 1-88, 2016.

[7] S. Sirur, J. Nurse, and H. Webb, “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*, 2018.

[8] R. Ducato, “Cloud computing for s-Health and the data protection challenge”, in *IEEE International Smart Cities Conference (ISC2)*, 2016.

[9] C. McAllister, “What About Small Businesses? The GDPR and its Consequences for Small U.S.-Based Companies”, *Brooklyn Journal of Corporate, Financial & Commercial Law*, vol. 12, no. 1, pp. 187-211, 2017.

[10] R. Rodrigues, D. Barnard-Wills, P. De Hert, and V. Papakonstantinou, “The future of privacy certification in Europe: an exploratory of options under article 42 of the GDPR”, *International Review of Law, Computers & Technology*, vol. 30, no. 3, pp. 248-270, 2016.

[11] L. Ryz and L. Grest, “A new era in data protection”, *Computer Fraud & Security*, vol. 2016, no. 3, pp. 18-20, 2016.

[12] R. O’Brien, “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, 2016.

[13] D. Drewer and V. Miladinova, “The canary in the data mine”, *Computer Law & Security Review*, vol. 34, pp. 806-815, 2018.

[14] N. Fraser, Challenges old and new: Analysis of the impacts of the General Data Protection Regulation. Master Thesis, Royal Holloway University of London, 2018.

[15] V. Gocheva, Challenges for the business when complying with the General Data Protection Regulation. Master Thesis, Tilburg University, 2017.

[16] M. Geko and S. Tjoa, “An ontology capturing the interdependence of the general data protection regulation (GDPR) and information security”, in *Proceedings of the Central European Cybersecurity Conference*, 2018.

[17] J. F. Rockart, “Chief Executives Define Their Own Needs”, *Harvard Business Review*, vol. 57, no. 2, pp. 81-93, 1979.

[18] C. V. Bullen and J. F. Rockart, A Primer on Critical Success Factors. Center for Information Systems Research, Sloan School of Management, Massachusetts Institute of Technology, 1981.

[19] A. C. Boynton and R. W. Zmud, “An Assessment of Critical Success Factors”, *Sloan Management Review*, vol. 25, no. 4, pp. 17-27, 1984.

[20] J. K. Leidecker and A. V. Bruno, “Identifying and Using Critical Success Factors”, *Long Range Planning*, vol. 17, no. 1, pp. 23-32, 1984.

[21] S. Staniszewska, N. Jones, M. Newburn, and S. Marshall, “User involvement in the development of a research bid: barriers, enablers and impacts”, *Health Expectations*, vol. 10, no. 2, pp. 173-183, 2007.

[22] H. J. Devries, “Performance-based Logistics – Barriers and Enablers to Effective Implementation”, *Defense Acquisition Review Journal*, vol. 11, no. 3, pp. 243-254, 2005.

[23] A. Kaushik, S. Kumar, S. Luthra, and A. Haleem, “Technology transfer: enablers and barriers – a review”, *International Journal of Technology Policy and Management*, vol. 14, no. 2, pp. 133-159, 2014.

[24] D. Gichoya, “Factors Affecting the Successful Implementation of ICT Projects in Government”, *The Electronic Journal of E-Government*, vol. 3, no. 4, pp. 175-184, 2005.

[25] D. Miller, B. Merrilees, and R. Yakimova, “Corporate Rebranding: An Integrative Review of Major Enablers and Barriers to the Rebranding Process”, *International Journal of Management Reviews*, vol. 16, pp. 265-289, 2014.

[26] B. Kitchenham, Procedures for Performing Systematic Reviews. Department of Computer Science, Keele University, 2004.

[27] C. Okoli and K. Schabram, “A Guide to Conducting a Systematic Literature Review of Information Systems Research”, *Sprouts: Working Papers on Information Systems*, vol. 10, no. 26, 2010.

[28] Y. Xiao and M. Watson, “Guidance on Conducting a Systematic Literature Review”, *Journal of Planning Education and Research*, vol. 39, no. 1, pp. 1-20, 2017.

[29] J. Webster and R. T. Watson, “Writing a literature review”, *MIS Quarterly*, vol. 26, no. 2, pp. 13-23, 2002.

[30] U. G. Gupta and R. E. Clarke, “Theory and Applications of the Delphi Technique: A Bibliography (1975-1994)”, *Technological Forecasting and Social Change*, vol. 53, no. 2, pp. 185-211, 1996.

[31] G. J. Skulmoski, F. T. Hartman, and J. Krahn, “The Delphi Method for Graduate Research”, *Journal of Information Technology Education*, vol. 6, no. 1, pp. 1-21, 2007.

[32] T. J. Gordon, The Delphi Method. *Future Research Methodology*, 1994.

[33] C. Hsu and B. A. Sandford, “The Delphi Technique: Making Sense of Consensus”, *Practical Assessment, Research & Evaluation*, vol. 12, no. 10, pp. 1-8, 2007.

[34] S. Schwerin, “Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study, *The Journal of the British Blockchain Association*, vol. 1, no. 1, pp. 1-76, 2018.

[35] R. C. Schmidt, “Managing Delphi Surveys Using Nonparametric Statistical Techniques”, *Decision Sciences*, vol. 28, no. 3, pp. 763-774, 1997.