The Critical Success Factors of GDPR Implementation: a Delphi Study

Gonçalo Almeida Teixeira
Instituto Superior Técnico, Universidade de Lisboa
Lisboa, Portugal *goncalo.almeida.teixeira@tecnico.ulisboa.pt*

Miguel Mira da Silva
Instituto Superior Técnico, Universidade de Lisboa
Lisboa, Portugal *mms@tecnico.ulisboa.pt*

Ruben Pereira
ISCTE - Instituto Universitário de Lisboa
Lisboa, Portugal *ruben.filipe.pereira@iscte-iul.pt*

Abstract

The European Union proposed the General Data Protection Regulation with a set of requirements for organizations 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 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, Delphi.

1. Introduction

To prevent the misuse of personal data by organizations and to address the privacy issues emerging from this new digital era [23], the European Commission proposed the General Data Protection Regulation (GDPR), with a set of obligations regarding the storing, processing, collecting and disclosing of data [10].

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 [33], 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 [2].

Enforced from May 25, 2018, the regulation applies to any organization that processes European citizens' data and may impose fines up to €20 million or 4% of the annual turnover, whichever is higher, when non-compliance is detected [8].

To comply with GDPR requirements, organizations need to review their processes and procedures, which will impact their businesses and impose a lot of adaptions [1].

Although many organizations understand the importance of complying with the new regulation, the uncertainty around GDPR has led to some divided approaches [30] because GDPR is not prescriptive regarding solutions to achieve compliance, not providing specific guidelines to implement its requirements [33], which turns the implementation of these obligations neither obvious nor easy [4].

Following a previous systematic literature review where the authors identified a list of enablers and barriers of GDPR implementation [1], this paper aims to validate and elaborate this list, through a Delphi study with ten DPOs, in order to identify the critical success factors (CSFs) of GDPR implementation, including both enablers and barriers.

It is important to refer that this research focuses on GDPR implementation in general, without any specific sector or industry.

This paper is structured as follows. Section 2 presents the theoretical background, including the regulation and critical success factors. Section 3 explains the chosen research methodology (Delphi). Section 4 presents the results from the Delphi study. Section 5 discusses the results from the research. Finally, Section 6 concludes the paper.

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)

After four years of negotiation between the European Commission, the Parliament and the Council [24], the General Data Protection Regulation (GDPR) was approved [19], being one of the most important legislative processes in the EU history [18].

GDPR introduces several changes to the current data protection laws, updating the regulatory framework to face the challenges of the information age [7], thus replacing and repealing the Data Protection Directive [8]).

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 [26]. Furthermore, it offers a more modern and wide-reaching approach to protection personal data [27].

The regulation introduces a lot of changes and a number of new obligations and data protection principles [21], from data minimization and limitation to data protection by design and by default [23]. 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 [6], 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 [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 [8].

In order to be compliant, organizations need to review their policies and processes, and adopt new practices and procedures by combining technical solutions with organizations controls [11], to ensure they process, hold and collect data in a GDPR-manner [33].

2.2. Critical Success Factors (CSFs)

Introduced by Rockart in a Harvard Business Review article in 1979, 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 [25].

CSFs represent a conceptualization of critical subjects and help ensure that organizations' needs are addressed, helping the business in prioritizing information system projects [3]. By identifying CSFs, organizations can assess the threats and identify the opportunities in a specific project, including characteristics, conditions and variables [17], in order to develop a robust strategic plan for that project implementation [3].

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

Enablers

Often called facilitators, enablers are the factors that help a project development and progress [32], enabling its successful and effective implementation [5], [16], being therefore critical to the project's success [1]. Enablers can also help to prevent or even overcome potential barriers [12], [20].

Thus, organizations must enhance and prioritize the existing enablers in order to implement a project in the most effective way.

Barriers

Barriers, also called inhibitors, are the factors that do not necessarily conduct to a project failure but hinder a project implementation [12], inhibiting an effective and successful project implementation [5], [12].

Therefore, organizations should make an effort to avoid, minimize or mitigate the identified barriers [5], [20].

3. Delphi Method

Firstly developed in 1948 at the RAND Corporation, the Delphi method only became popular in 1963 after the publication of the first article [22] with its description [14].

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 [14], [31], enabling a group interaction without the need of face to face meetings [14].

Even though it is a well-known research method, there is not a typical Delphi. Instead, it is a flexible method that can be modified to suit each research, including the number of rounds and participants [31].

As mentioned before, anonymity is one of the important features of Delphi, in order to encourage a true and controlled debate [13], allowing the participants to freely express their opinions without any kind of pressure or dominance from other participants [31].

Delphi already proved to be an effective and efficient research method [31] and has been used in Information Systems research for identifying and prioritizing issues regarding managerial decision-making [22].

3.1. Participants

The selection of participants plays a key role on a successful Delphi, since the results of the investigation depend on the knowledge and opinions of the experts [31], [13]. Therefore, participants should be highly competent in the respective area of expertise [15].

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. Furthermore, all the participants are Portuguese – it is important to note that Portugal had similar data protection laws prior to GDPR, such as Law 67/98, in order to transpose the Data Protection Directive requirements into the Portuguese law, which has a significant impact in their expertise.

The Delphi started with 22 experts but only 10 concluded the whole investigation, which is a reasonable number as there are Delphi studies in the literature with participants ranging from 4 to 171 [31]. These participants are described with more detail in Table 1.

Table 1. Delphi's panel of experts.

ID	Gender	Area of Expertise	Sector	Years of Experience	Contact
P1	Female	IT	Private	< 5 years	APDPO
P2	Male	Law	Private	< 5 years	APDPO
P3	Female	Law	Private	< 5 years	APDPO
P4	Male	Management	Private	< 5 years	APDPO
P5	Male	Law	Private	More than 5 years	APDPO
P6	Male	Tourism	Private	< 5 years	APDPO
P7	Male	IT	Private	< 5 years	APDPO
P8	Female	Law	Private	< 5 years	LinkedIn
P9	Male	Physics	Public	< 5 years	LinkedIn
P10	Female	Law	Private	More than 5 years	LinkedIn

3.2. Rounds

The Delphi method can be continuously iterated until consensus is achieved. However, the higher the number of rounds, the lower the response rate [31].

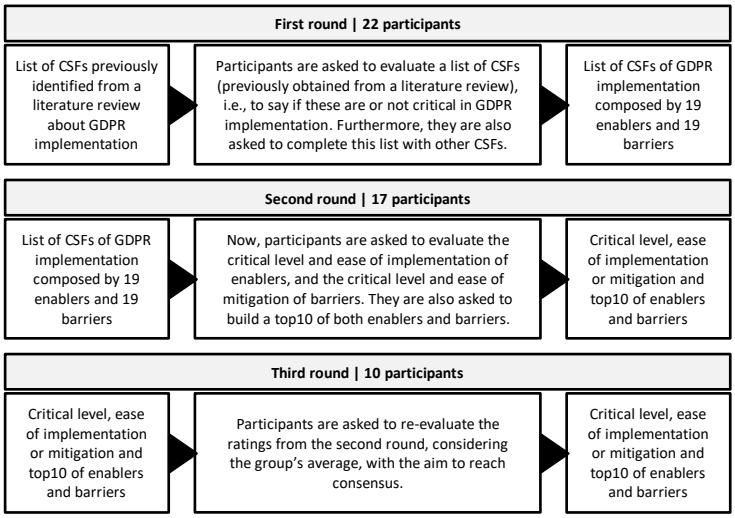

Fig. 1. Delphi study.

Three rounds are enough to collect the needed information and to achieve consensus [15], with each round being developed based on the results of the previous round [31]. Figure 1 describes the applied Delphi, performed between April 1 and May 13, 2019.

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; and

• 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, in order to reduce communication delays and burdens [13], giving the participants the flexibility to answer them digitally and in their own time [29].

4. Results

The starting point for this Delphi study was a previous systematic literature review [1], where enablers and barriers regarding GDPR implementation were identified (Table 2).

Table 2. Critical success factors from the literature [1].

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

4.1. Round 1

In the first round, the participants were asked to validate the critical success factors from Table 2, i.e., to say if these are or not critical regarding GDPR implementation. The acceptance rate of each CSF is presented in Appendix A (Table A.1).

Considering a threshold of two-thirds (66%) of acceptance rate, the enabler Data Protection Officer and the barriers GDPR extension, GDPR complexity and GDPR subjectivity were further eliminated from the critical success factors list.

Furthermore, the participants were also asked to elaborate on this list by providing additional critical success factors regarding GDPR implementation.

By combining all the inputs given by the participants from the first round and analysing their justifications, a list with 19 enablers and 19 barriers was elaborated (Table 3).

Table 3. Critical success factors of GDPR implementation.

	Critical Success Factors	ID		Critical Success Factors	ID
Enablers	Alignment of DPO with other enterprise roles	E1	Barriers	Absence of a well-defined organizational structure	B1
	Certification	E2		Absence of planification	B2
	Collaboration between IT and Legal Departments	E3		Change resistance	B3
	Data management	E4		Consider GDPR a burden instead of an advantage	B4
	Data protection and security policies	E5		Data availability/accessibility	B5
	Data Protection Impact Assessments	E6		GDPR misconception	B6
	Enterprise engagement	E7		Internal politics	B7
	GDPR analysis	E8		Lack of budget	B8
	Implementation by external consultant	E9		Lack of human resources	B9
	Implementation roadmap	E10		Lack of KPIs	B10
	Information Security Management System	E11		Lack of management commitment and support	B11
	Monitorization	E12		Lack of management knowledge	B12
	Organizational culture	E13		Lack of practical guides or standard procedures	B13
	Process documentation	E14		Lack of privacy knowledge and expertise	B14
	Right level of technology	E15		Lack of required technology	B15
	Risks identification	E16		Lack of security practices	B16
	Security measures and mechanisms	E17		Lack of training	B17
	Top management sponsorship and involvement	E18		Organizational culture	B18
	Training awareness	E19		Poor compliance assessment	B19

This list, presented in Table 3, is the baseline of this Delphi, and will be evaluated in the second and third rounds according to the parameters previously referred in Section 3.2.

4.2. Round 2

In the second round, participants were asked to evaluate the CSFs identified from the previous round (Table 3). Enablers were evaluated by critical level and ease of implementation, while barriers were evaluated by critical level and ease of mitigation.

Participants were also asked to build a top10 of enablers and barriers, based on the critical level and ease of implementation/mitigation values. These results are presented in Appendix B, in Tables B.1 (enablers) and B.2 (barriers).

4.3. Round 3

In the third and final round, participants were asked to re-evaluate their second-round ratings, considering the groups' average. These results are also presented in Appendix B, in Tables B.1 (enablers) and B.2 (barriers).

5. 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).

The barriers related with the regulation itself (GDPR extension, complexity and subjectivity) were not considered as critical, which hints that it is easy to understand the regulation and its requirements, just like any other law. However, this is not a consensual subject, since some authors say the regulation is a challenge by itself [9].

5.1. 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.

Furthermore, 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, a big discrepancy is found out of the top10 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).

Finally, 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; and "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.

Eight of the ten enablers with the highest ease of implementation values are within the top 10, with the exceptions of "Information Security Management Systems", which has one of the highest ease of implementation values but is ranked in the 13th position; and "Training awareness" and "Collaboration between IT and Legal Departments", which 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.

Dots in the top right corner of the graph have the higher critical level values and the higher ease of implementation values, meaning they represent the most critical enablers and the hardest to implement. Meanwhile, dots in the bottom left corner represent the less critical enablers and the easier to implement.

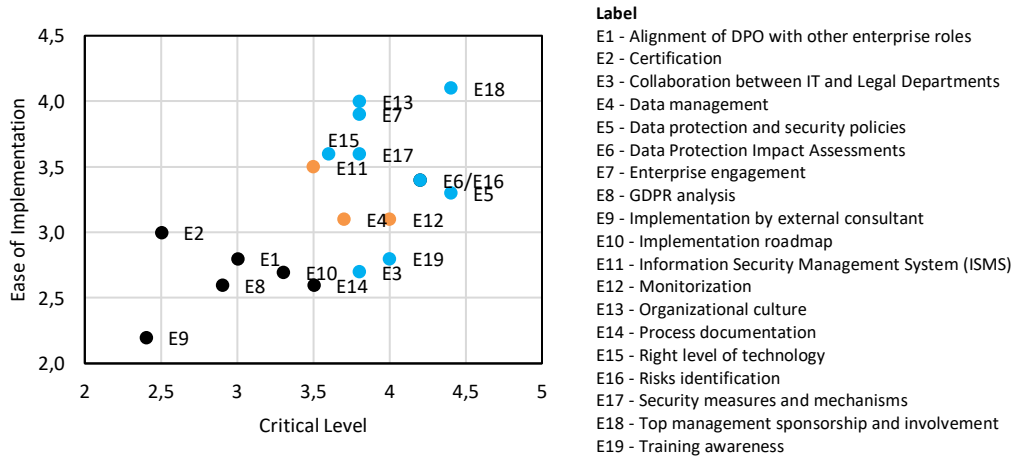

Fig. 2. Critical level and ease of implementation of GDPR implementation enablers.

As it is possible to see, almost all the top10 enablers (blue dots) have the higher critical level vs. 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) 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.

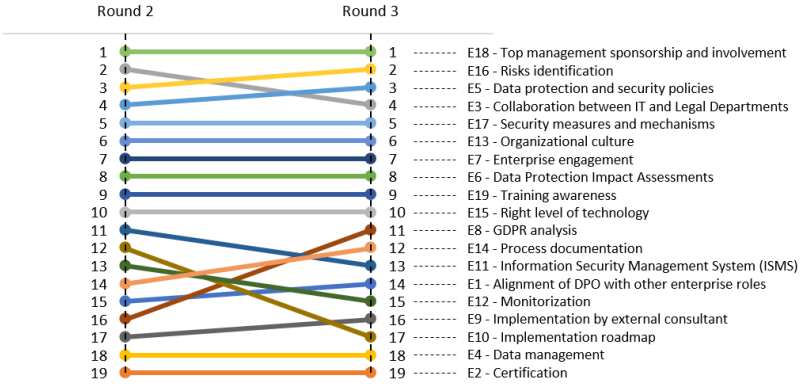

Fig. 3. Enablers' rank variations between round 2 and 3.

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

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).

5.2. Barriers

Regarding the barriers, we will now discuss the results from second and third rounds, by analysing 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.

Finally, 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 identical to the enablers' average (3,62).

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, with two exceptions: "Lack of privacy knowledge and expertise", which has one of the lowest values regarding ease of mitigation but is ranked in the 5th position; and "Poor compliance assessment" (11th position), which is tied with "Absence of

planification" (10th position) - 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.

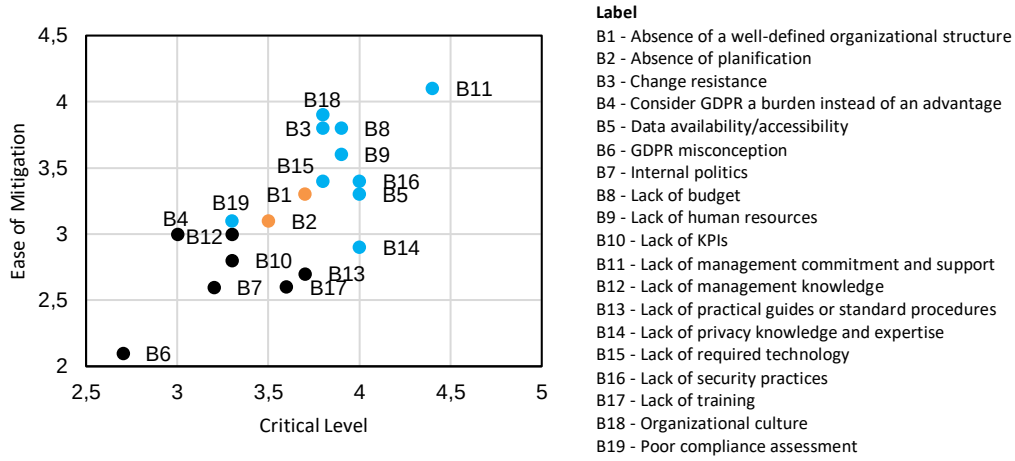

Fig. 4. Critical level and ease of mitigation of GDPR implementation barriers.

Dots in the top right corner of the graph have the higher critical level values and the higher ease of mitigation values, which means they represent the most critical barriers and the hardest to mitigate (the ones that have the biggest impact). Meanwhile, dots in the bottom left corner represent the less critical barriers and the easier to mitigate, since these have the lower critical level values as well as the lower ease of mitigation values.

Almost all the top10 barriers (blue dots) have the higher critical level vs. 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 structure) 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.

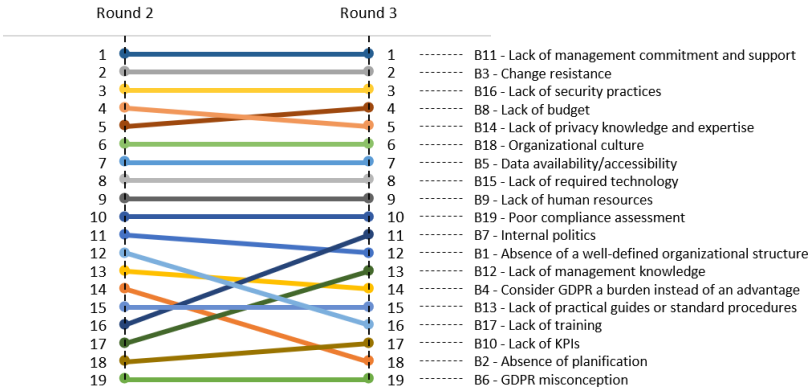

Fig. 5. Barriers' rank variations between round 2 and 3.

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 (4th and 5th).

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.

5.3. Consensus

The consensus among the panel of experts can be measured with the Kendall's W coefficient of concordance. W ranges between 0 and 1, where 0 means no consensus and 1 perfect consensus [22].

Using the Kendall's W to measure the consensus on the top10 lists, and regarding the second round, both enablers and barriers have a value of around 0,2, which suggests a weak agreement [28].

In the third and final round, where the participants had the opportunity to refine their opinions based on the groups' average ratings, with the aim to reach consensus, 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 [28] in both parameters.

6. Conclusion

In this work, a Delphi study was conducted with ten experts in order to validate and elaborate a list of CSFs, previously identified through a systematic literature review, with the aim to identify the enablers and barriers of GDPR implementation.

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 (Table 4). Furthermore, it is also possible to identify the ten most important barriers in GDPR implementation regarding its critical level and ease of mitigation (Table 4).

Table 4. Critical success factors of GDPR implementation.

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

These results show that people, processes and technology are the core drivers in the journey of GDPR compliance.

Starting by people - culture by itself has a significant presence in both enablers and barriers (not only "Organizational culture", but also "Change resistance"), as well as expertise and engagement ("Enterprise engagement", "Training awareness", "Lack of privacy knowledge and expertise" and "Lack of human resources"); the most important CSF is the support, sponsorship and commitment from the management level, both in enablers and barriers, where decisions are made.

Then, processes (or IT Governance) also play a key role in GDPR implementation, with "Data protection and security policies", "Collaboration between IT and Legal Departments", "Security measures and mechanisms" and "Lack of security practices".

Finally, technology, with "Right level of technology" and "Lack of required technology".

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.

Regarding limitations, the Delphi method has some drawbacks, such as subtle pressures to conform with group ratings [15] or sloppy executions from the participants without a genuine reflection on the questionnaires [14]. Furthermore, participants can also deliberately promote desired outcomes [14].

There are also few inconsistencies between the top10 rank and the critical level and ease of mitigation/implementation values, already presented in the Delphi discussion, which may mean that there are also other important parameters to decide the relevance of both enablers and barriers in the compliance process.

The study would also improve its results with a bigger panel of experts or with a more experienced one. However, these are often very busy to complete a full Delphi study.

In the future, and in order to validate and deepen the identified critical success factors, other research methods could be used such as case studies or interviews, to complement the obtained results - when the study was performed, the literature was missing similar studies. Moreover, understanding the relationship between enablers and barriers may be useful for organizations, since some barriers may affect other enablers and their ease of implementation.

It would also be useful to distinguish the importance of these critical success factors between governmental organizations and businesses, since these have different characteristics and needs.

Future research may also focus on using the identified critical success factors for defining an implementation roadmap, which would be very useful for organizations to use as a guideline, helping them to ease GDPR implementation.

References

1. Almeida Teixeira, G., Mira da Silva, M., Pereira, R.: The critical success factors of GDPR implementation: a systematic literature review. Digital Policy, Regulation and Governance 21(4), 402-418 (2019)
2. Boban, M.: 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. ESD, Rome (2018)
3. Boynton, A. C., Zmud, R. W.: An Assessment of Critical Success Factors. Sloan Management Review 25(4), 17–27 (1984)
4. Cvik, E. D., Pelikánová, R. M., Malý, M.: Selected Issues from the Dark Side of the General Data Protection Regulation. Review of Economic Perspectives 18(4), 387–407 (2018)
5. Devries, H. J.: Performance-based Logistics - Barriers and Enablers to Effective Implementation. Defense Acquisition Review Journal 11(3), 243–254 (2005)
6. Drewer, D., Miladinova, V.: The canary in the data mine. Computer Law & Security Review 34, 806–815 (2018)
7. Ducato, R.: Cloud computing for s-Health and the data protection challenge. In: IEEE International Smart Cities Conference (ISC2). IEEE, Trento (2016)
8. 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. Official Journal of the European Union 59, 1–88 (2016)
9. Freitas, M. da C., Mira da Silva, M.: GDPR Compliance in SMEs: There is much to be done. Journal of Information Systems Engineering & Management 34(4), 30-37 (2018)
10. Gabriela, G., Cerasela, S.E., Alina, C. M.: The Eu General Data Protection Regulation Implications for Romanian Small and Medium-Sized Enterprises. Ovidius University Annals (Economic Science Series) 18, 88-91 (2018)
11. Geko, M., Tjoa, S.: An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security. In: Central European

Cybersecurity Conference. Ljubljana (2018)
12. Gichoya, D.: Factors Affecting the Successful Implementation of ICT Projects in Government. The Electronic Journal of E-Government 3(4), 175–184 (2005)
13. Gordon, T. J.: The Delphi Method. Futures Research Methodology (1994)
14. Gupta, U. G., Clarke, R. E.: Theory and Applications of the Delphi Technique: A Bibliography (1975-1994). Technological Forecasting and Social Change 53(2), 185–211 (1996)
15. Hsu, C., Sandford, B. A.: The Delphi Technique: Making Sense Of Consensus. Practical Assessment, Research & Evaluation 12(10), 1-8 (2007)
16. Kaushik, A., Kumar, S., Luthra, S., Haleem, A.: Technology transfer: enablers and barriers – a review. International Journal of Technology Policy and Management 14(2), 133–159 (2014)
17. Leidecker, J. K., Bruno, A. V.: Identifying and Using Critical Success Factors. Long Range Planning 17(1), 23–32 (1984)
18. Martínez-Martínez, D.: Unification of personal data protection in the European Union: Challenges and implications. El profesional de la información 27(1), 185-194 (2017)
19. McAllister, C.: What About Small Businesses? The GDPR and its Consequences for Small U.S.-Based Companies. Brooklyn Journal of Corporate, Financial & Commercial Law 12(1), 187-211 (2017)
20. Miller, D., Merrilees, B., Yakimova, R.: Corporate Rebranding: An Integrative Review of Major Enablers and Barriers to the Rebranding Process. International Journal of Management Reviews 16, 265–289 (2014)
21. O'Brien, R.: Privacy and security: The new European data protection regulation and it's data breach notification requirements. Business Information Review 33(2), 81–84 (2016)
22. Okoli, C., Pawlowski, S. D.: The Delphi method as a research tool: an example, design considerations and applications. Information & Management 42, 15–29 (2004)
23. Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C.: Backups and the right to be forgotten in the GDPR: An uneasy relationship. Computer Law & Security Review 34(6), 1247–1257 (2018)
24. Preuveneers, D., Joosen, W., Ilie-Zudor, E.: Data Protection Compliance Regulations and Implications for Smart Factories of the Future. In: 12th International Conference on Intelligent Environments. London (2016)
25. Rockart, J. F.: Chief Executives Define Their Own Data Needs. Harvard Business Review 57(2), 81–93 (1979)
26. Rodrigues, R., Barnard-Wills, D., De Hert, P., Papakonstantinou, V.: The future of privacy certification in Europe: an exploratory of options under article 42 of the GDPR. International Review of Law, Computers & Technology 30(3), 248-270 (2016)
27. Ryz, L., Grest, L.: A new era in data protection. Computer Fraud & Security 2016(3), 18-20 (2016)
28. Schmidt, R. C.: Managing Delphi Surveys Using Nonparametric Statistical Techniques. Decision Sciences 28(3), 763–774 (1997).
29. Schwerin, S.: 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 1(1), 1-77 (2018)
30. Sirur, S., Nurse, J., Webb, H.: 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. ACM, Toronto (2018)
31. Skulmoski, G. J., Hartman, F. T., Krahn, J.: The Delphi Method for Graduate Research. Journal of Information Technology Education 6(1), 1–21 (2007)
32. Staniszewska, S., Jones, N., Newburn, M., Marshall, S.: User involvement in the development of a research bid: barriers, enablers and impacts. Health Expectations 10(2), 173–183 (2007)
33. Tikkinen-piri, C., Rohunen, A., Markkula, J.: EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review 34, 134–153 (2018)

Appendix A

Table A.1. Acceptance rate from the CSFs previously identified in the literature.

	Critical Success Factors	Acceptance Rate
Enablers	Risks identification	95,45%
	Process documentation	95,45%
	Data management	90,91%
	Training awareness	90,91%
	Implementation roadmap	86,36%
	Security measures and mechanisms	86,36%
	GDPR analysis	77,27%
	Data Protection Officer	63,64%
Barriers	Lack of privacy knowledge and expertise	95,45%
	Lack of human resources	81,82%
	Lack of budget	68,18%
	Lack of required technology	68,18%
	Lack of practical guides or standard procedures	68,18%
	GDPR complexity	59,09%
	GDPR subjectivity	54,55%
	GDPR extension	50,00%

Appendix B

Table B.1. Enablers' critical level, ease of implementation and rank from rounds 2 and 3.

Enablers	Critical Level			Ease of Implementation			Rank		
	Rnd. 2	Rnd. 3	Δ	Rnd. 2	Rnd. 3	Δ	Rnd. 2	Rnd. 3	Δ
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	---

Table B.2. Barriers' critical level, ease of mitigation and rank from rounds 2 and 3.

Barriers	Critical Level			Ease of Mitigation			Rank		
	Rnd. 2	Rnd. 3	Δ	Rnd. 2	Rnd. 3	Δ	Rnd. 2	Rnd. 3	Δ
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 structure (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	---