# The GDPR Implementation Challenges Faced By Technology Startups In Catalonia

**DBA Thesis**

**Geneva Business School**

**Doctorate in International Management**

**Submitted by:**

**Victoriano Travieso Morales**

**Supervised by:**

**Kimberly A. Houser, J.D.**

**Barcelona, Spain**

**Date: 30/03/2023**

**Word count: 43.925**

## Declarations of Authorship

"I hereby declare:

- That I have written this work on my own without other people's help (copy-editing, translation, etc.) and without the use of any aids other than those indicated.
- That I have mentioned all the sources used and quoted them correctly in accordance with academic quotation rules.
- That the topic or parts of it are not already the object of any work or examination of another course unless this has been explicitly agreed on with the DBA Program Manager and supervisor in advance.
- That my work may be scanned in and electronically checked for plagiarism.
- That I understand that my work can be published online or deposited to the school repository. I understand that to limit access to my work due to the commercial sensitivity of the content or to protect my intellectual property or that of the company I worked with, I need to file a Bar on Access according to thesis guidelines."

Date: 30.03.2023

Name: Victoriano Travieso Morales

Signature: NOMBRE TRAVIESO MORALES VICTORIANO - NIF 42848372Q

Firmado digitalmente por NOMBRE TRAVIESO MORALES VICTORIANO - NIF 42848372Q
Fecha: 2023.03.30 22:44:58 +02'00'

## ACKNOWLEDGEMENT / COPYRIGHT

First and foremost, I am highly grateful to my supervisors, Kimberley A. Houser, J.D. and Yelena Smirnova, Ph.D., for their invaluable advice, continuous support, and patience during my DBA study. Their immense knowledge and ample experience have encouraged me in all the time of my academic research and daily life. I would also like to thank Oliver Elliott, Ph.D., Nicola Jackman and the DBA professors for all their continued support and Geneva Business School for the studentship that allowed me to conduct this thesis.

I would also like to thank all the startups that participated in the study since without then this study would have not been possible and to thank ACCIÓ for providing the database.

Finally, I would like to express my gratitude to my family and close friends. So, I can complete my study with their tremendous understanding and encouragement over the past few years.

## Table of Contents

## List of Abbreviations

| | |
|---|---|
| ACCIÓ | Agency for Business Competitiveness |
| AEPD | Spanish Data Protection Agency |
| AI | Artificial Intelligence |
| AMB | Metropolitan Area of Barcelona |
| ANOVA | Analysis of variance |
| APDCAT | Catalan Data Protection Authority |
| BCG | Boston Consulting Group |
| CELEX | Communitatis Europeae Lex |
| CEO | Chief Executive Officer |
| CFO | Chief Financial Officer |
| CMO | Chief Marketing Officer |
| COVID | Corona Virus Disease |
| CPO | Chief Privacy Officer |
| CTO | Chief Technology Officer |
| DESI | Digital Economy and Society Index |
| DLT | Distributed Ledger Technologies |
| DPA | Data Protection Authority |
| DPIA | Data Protection Impact Assessment |
| DPO | Data Protection Officer |
| EFA | Exploratory Factor Analysis |

| | |
|---|---|
| EM | Expectation Maximization |
| EU | European Union |
| EUR | Euro |
| FDI | Foreign Direct Investment |
| GDPR | General Data Protection Regulation |
| HARP | Heightening your Awareness of your Research Philosophy |
| HSD | Honestly Significant Difference |
| ICT | Information and Communications Technology |
| IDESCAT | Statistical Institute of Catalonia |
| IEC | The International Electrotechnical Commission |
| IED | Intelligent Electronic Device |
| INE | National Statistics Institute |
| IQR | Interquartile range |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| KMO | Kaiser-Meyer-Olkin |
| LOPDGDD | Organic Law on Personal Data Protection and Guarantee of Digital Rights |
| ML | Machine Learning |
| PCA | Principal Component Analysis |
| QQ | Quantile-Quantile |
| RGPD | General Data Protection Regulation |

| | |
|---|---|
| RQ | Research Question |
| SD | Standard Deviation |
| SME | Small Medium Enterprise |
| SPSS | Statistical Package for the Social Sciences |
| TIC | Information and Communication Technologies |
| UK | United Kingdom |
| UPC | Polytechnic University of Catalonia |
| US | United States |

## List of Tables

## List of Figures

# ABSTRACT

Startups and SMEs require attention, especially technology startups; while driven by innovation and pushing the boundaries of technologies, they need better data protection practices. This research aims to gather data on the startups' familiarity with the GDPR, identify the key challenges faced by technology startups in Catalonia when the GDPR became applicable in May 2018, and explore (1) whether there is a relationship between the identified challenges and the number and type of employees recruited, size of a startup, business sector, year of establishment; and (2) the time and money startups spent on compliance. The literature review highlighted gaps in the research and was used as the basis for analysing the challenges faced by startups resulting from the enforcement of the GDPR. Thirty-two challenges were identified related to GDPR and grouped into four constructs/categories: Compliance costs, regulation complexity, government support and process adaptation. The resulting insufficient government support is the highest challenge for the Catalonian startups participating in the survey. This study is among the first empirical studies on GDPR compliance efforts and challenges by Catalan technology startups that have been conducted using advanced statistical analysis techniques starting with ANOVA, followed by independent sample T-test, correlation analysis and regression analysis. Unfortunately, the results cannot be generalised to all startups in Catalonia because the required minimum sample size for representativeness was not met; 116 responses were collected compared to the 314 needed to reach the necessary sample size. Nevertheless, this research makes a practical contribution by (1) providing recommendations that help increase technology startups' awareness of the different types of challenges they must address and overcome to comply with GDPR and (2) it provides recommendations for the Catalan government to boost startup GDPR implementation.

Keywords— challenges, GDPR implementation, privacy issues, technology startups and SMEs.

# CHAPTER 1 INTRODUCTION

## 1.1. Background and motivation

It is essential to consider that this study concentrates on the implementation of GDPR in technology startups in Catalonia, which is one of Europe's largest ICT hubs and the leader destination for IED technology being Barcelona the 7th E.U. startup hub in future unicorns behind Paris, Berlin, Stockholm, Munich, Dublin, and Amsterdam and ahead of Madrid. Technologies 4.0 are predominant in the Catalonian startups with 75% that have implemented initiatives to improve the sustainability of their business (ACCIÓ, 2022)

The right to safety of personal data is a basic human right recognized in the Charter of Fundamental Rights of the European Union (Rodotà, 2009) and the EU, to protect consumers' privacy adopted the General Data Protection Regulation ("GDPR") (Bessen, Impink, Reichensperger, & Seamans, 2020). The GDPR is designed to provide uniform criteria for all the EU member states on data protection and introduces significant changes to personal data and privacy, which replaces and repeals the 1995 EU Data Protection Directive (Almeida Teixeira, Mira da Silva, & Pereira, 2019; (de Hert & Papakonstantinou, 2016).

The GDPR came into force on the 25th of May 2018 after a two-year transition period. Since technological development has favored the increasing collection of personal data, a balance must be found between economic benefit and customer data protection. Globalization and fast technological modification have facilitated citizens to conveniently share data about their behaviour and preferences (sometimes without their express prior consent), and often this information becomes accessible to other organizations worldwide (Poritskiy et al., 2019). The studies by McDermott (2017) and Polykalas & Prezerakos (2019) show that the proliferation of big data tools allows a cross-analysis of personal data and most mobile applications require access to a considerable amount of personal data (Poritskiy et al., 2019). Although many of those mobile applications are free to download users are still "paying" with their personal data.

The GDPR aims to give people in the EU more control over their data, strengthen their rights, reform how organizations see and control that data, and remove barriers to cross-border trade to allow businesses to expand more naturally across Europe ensuring the free flow of personal data between EU member states (Almeida Teixeira et al., 2019; (Sirur, Nurse, & Webb, 2018). The GDPR aims to instill confidence in the digital economy and harmonize data protection across the EU, in line with the Digital Single Market strategy (Seo, Kim, Park, Park, & Lee, 2017).

The study carried out by Poritskiy et al. (2019) indicate that there is no doubt that all areas of activity must know and apply the GDPR. However, the technology companies are among the most affected, as they not only apply the rules of the GDPR when processing personal data, but also have to expand technological solutions that comply with the rules of the GDPR. Despite the significance of GDPR for technology companies especially SMEs and technology startups, no previous studies have been conducted Poritskiy et al. (2019).

Discussions on data protection and the GDPR in particular have focused on the larger technology companies such as Facebook and Google and the importance of these laws for the users of such services (e.g. see Houser and Voss, 2018) and the discussions that have focused on small technology startups, have primarily focused on one country**,** the U.K. (e.g. see Norval et al., 2021). However, startups and SMEs also require attention, especially technology startups which are driven by innovation, pushing the boundaries of technology but lacking established best practices for data protection. Initial decisions by startups can certainly have negative long-term effects. Therefore, ensuring that tech startups' innovations and practices are robust, appropriate and acceptable should be a high priority (Norval et al., 2021). Supervisory Authorities need to provide more support to the technology startups, in terms of increasing awareness and guidance. They must also take an active role in loss prevention and deterrence so that startups have the best opportunities to innovate under the GDPR framework (Norval et al., 2021). There is an assumption that the Supervisory Authorities are concentrating more on the larger tech firms than the small tech startups and SMEs; if that is the case, the negative long-term impact can be devastating.

Previous research studies in this area, such as (Freitas et al., 2018; Härting et al., 2020; Härting et al., 2021, Jonas, 2018; Poritskiy et al., 2019; TrustArc, 2018), are of value and although they mainly considered companies of all sizes and major sectors, they did not concentrate on technology companies and when they did they concentrated on SMEs and not technology startups. Moreover, the research study by Norval et al., (2021), and the TrustArc report (TrustArc, 2017) are also of value. However, they concentrated only on technology startups in the UK, the UK and the US, respectively, before GDPR enforcement. That is also why research on technology startups is essential.

The analysis of previous studies on the challenges of the GDPR implementation faced by companies and especially technology ones SMEs and startups show that they exist. Furthermore, several authors have found that the technology companies are one of the most affected ones in terms of processing data and developing technological solutions that comply with the GDPR (Härting et al., 2020; Härting et al., 2021, Norval et al., 2021; and Poritskiy et al., 2019), in terms of compliance costs (Freitas et al., 2018; Härting et al., 2020; and Härting et al., 2021), government support (Härting et al., 2020; Härting et al., 2021; and Norval et al., 2021), regulation complexity (Härting et al., 2020; Härting et al., 2021; and Norval et al., 2021), and process adaptation (Poritskiy et al., 2019).

The literature research helped the author decide on an appropriate structure for the framework and highlighted a gap in the challenges faced by startups due to the execution of the General Data Protection Regulation (GDPR) from May 2018.

However, there is a lack of information on how familiar technology startups are with the GDPR three years after the GDPR came into force, including: the key challenges of the GDPR implementation faced by them, whether they are associated with compliance costs, regulation complexity, insufficient government support or process adaptation and if there is any relationship between the challenges faced by them and the year of establishment, size, business sector, and annual expenditure on GDPR compliance. Thus, further research is needed since by identifying challenges, the organizations will take care to avoid errors and drawbacks throughout the GDPR implementation process and it may be useful for the governments to take measures to support organizations with challenges of implementing GDPR.

## 1.2. Research scope, aim, objectives and questions

The general purpose of the study is to gather a wide range of opinions from technology startup professionals in order to identify:

- The key challenges faced by the technology startups in Catalonia resulting from the applicability of the GDPR,

- If the key challenges are associated with compliance costs, regulation complexity, insufficient government support or process adaptation,

- If there is any relationship between the challenges faced by technology startups and the year of establishment, size, business sector, and annual expenditures on GDPR compliance.

- the level of GDPR knowledge of the startup's representatives.

The aim was to collect data to enable both descriptive and inferential statistical analysis in order to generalize and draw conclusions from the sample to identify a set of quantitative GDPR implementation challenges to provide recommendations to help to increase technology startups' awareness in Catalonia to address and overcome the challenges to comply with GDPR and for the Catalan government to support technology startups with challenges of implementing GDPR.

The 'target population' for the research were technology startups in Catalonia and for the representative sample the database of technology companies in Catalonia administered by ACCIÓ was used. ACCIÓ administers the Barcelona and Catalonia Startup Hub, including a database of technology companies in Catalonia and their members met the admission criteria as good representatives of technology companies in Catalonia.

The distribution of the questionnaire and collection of responses started on the 7th of May 2021 and finished on the 29th of November 2021.

This research is broken down into two literature review chapters. Chapter two deals with the management challenges faced by the US and the EU companies before GDPR enforcement, the implementation challenges after GDPR came into force, the effect of GDPR on the US and the EU technology startups and SMEs as well as with the theoretical framework. Chapter three deals with technology startups in Catalonia, identifying the challenges they face resulting from the applicability of the GDPR, to answer the following research questions:

In relation to **RQ 1**: How familiar are technology startups in Catalonia with the GDPR?

In relation to **RQ 2**: What are the key challenges of the GDPR implementation faced by technology startups in Catalonia?

In relation to **RQ 2.1**: Are the key challenges associated with compliance costs, regulation complexity, insufficient government support or process adaptation?

In relation to **RQ 2.2**: Is there any relationship between the challenges faced by technology startups and the number and type of employees recruited, size, business sector, year of establishment, GDPR annual spending and time to achieve compliance?

In relation to **RQ 3**: What recommendations can be provided to help technology startups in Catalonia overcome the challenges resulting from the GDPR?

## 1.3. Study methodology

Beginning with the literature search, a review protocol was performed, that defined the search string to be applied in the selected datasets to retrieve the maximum variety of studies that can address the proposed research questions Almeida Teixeira et al., (2019). Thereafter, inclusion and exclusion criteria were used to filter the documents received and the initial group of documents was obtained. In the first phase, the abstracts were then examined with regard to their importance for the research. Finally, these documents were read to make the final choice of studies to conduct the review. Based on the work carried out by Almeida Teixeira et al., (2019) after using the described search string in the shown data sets, 4170 documents were found. With the inclusion and exclusion criteria, 98 papers were received, except duplicates. The summaries were then read to further determine the importance of the documents, with 68 documents collected. Each of these documents has been read, yielding 58 related studies for the research.

For the creation of the theoretical framework using the academic search engine Scopus in October 2021, five search strings in English and Spanish languages were applied. The literature research helped the author decide on an appropriate structure for the framework and highlighted a gap in the challenges faced by startups resulting from the enforcement of the General Data Protection Regulation (GDPR) as of May 2018. In analysing the paper title and abstracts, 27 were categorised as relevant. Thirty-two challenges were identified related to GDPR and grouped into the four different constructs/categories: Compliance costs, regulation complexity, government support and process adaptation These challenges are also confirmed by the researcher's interviews with three Catalan startups registered in the Agency for Business Competitiveness (ACCIÓ).

Surveys were preferred because of the quantitative deductive elements of the research since they allow to collect primary data which can be analysed and based on which inferences can be made regarding the answers to the research questions.

A respondent and company profile were carried out by describing the demographic profile of the respondents, the number of years the companies have been established, the number of persons employed in the company and the weighted frequencies of the respondents by business sectors. Also, it was carried out a descriptive statistics analysis, ANOVA tests, independent sample T-test analysis, correlation test and regression models analysis results.

## 1.4. Research contributions

This thesis represents a unique and significant contribution to the current body of data privacy from the research and practical perspectives.

From the research perspective, it is among the first empirical studies on Catalan technology startups’ GDPR compliance efforts and contributes to the literature on data privacy research. This study is among the first empirical studies on technology startups’ GDPR challenges that have conducted advanced statistical analysis techniques starting with ANOVA, followed by independent sample T-test, correlation analysis and regression analysis, which supports the findings.

From a practical perspective, Huth et al. (2018) evidenced that the centre of activity in the GDPR revolves around the data subject and the controller and between the controller and the supervisory authority and concludes that the leading actor in the GDPR is the data controller.

This research study is useful for the controller, the processor, the data protection officer, the supervisory authority, and regional government's agency authorities, but it is most useful for the data controller and the national supervisory and regional government agency authorities (especially for the Catalan technology companies and for ACCIÓ and Barcelona Activa).

## 1.5. Research limitations

The main research limitations are the lack of well-documented studies in the field, difficulty in the data collection due to the COVID pandemic crisis and the acquiescence effect phenomenon (Hinz, et al., 2007). Additionally, the results cannot be generalised to all startups in Catalonia and only provide inferences about those surveyed because the required minimum sample size for representativeness was not met; 116 responses were collected compared to the 314 needed to reach the necessary sample size. Moreover, national mentality could skew the results as the results in other countries could be different despite having the same law (Härting et al., 2020). Also, the mobility and food tech sectors that received only two respondents were not considered for the ANOVA test business sectors. Finally, although the Startup Act came into force on the 22nd of December 2022, this study considers the definition of a startup provided by ACCIÓ since the researcher uses the data base provided by ACCIÓ, the theoretical framework was defined and the data was collected from May 2021 to November 2021. In the context of the recent enforcement of the Startup Act, it can be considered a limitation.

## 1.6. Thesis structure

This section provides a summary of the work, which consists of six chapters in total.

In Chapter 1, we present an introduction that covers the background and purposes of study, study goals and objectives, research questions, and the main contributions of this research.

In Chapter 2 we analyzed and discussed the prior literature on the challenges faced by companies with an emphasis on technology companies and especially SMEs and tech startups.

There are two main implications from this review. First, this chapter presents a survey on the GDPR challenges faced by companies. Therefore, the knowledge derived from business could serve useful for the governments to take measures to support organizations with challenges of implementing GDPR. Second, by identifying challenges, the organizations will take care to sidestep errors and drawbacks throughout the GDPR implementation procedure.

In Chapter 3 we analyzed and discussed the existing definitions of startup, the statistics on the digital economy in Catalonia, the positioning of Catalonia and Barcelona and the main features of the startup in Catalonia for then thanks to three Barcelona tech startups to identify the GDPR implementation challenges faced by technological startups in Catalonia. Three main implications can be derived from this review. Firstly, for researchers interested in Catalan or Spanish startups, this chapter presents the two definitions of startup the one that will be applicable in Spain when the Startup Law is enforced and the ACCIÓ definition of a startup as the criteria used for the startups forming part of the startup directory. Secondly, for researchers interested in conducting research in GDPR challenges in Catalonia or the rest of Spain, this chapter presents Catalonia as one of Europe's largest ICT hubs and the leader destiny for IED technology being Barcelona the $7^{th}$ E.U. startup hub in future unicorns behind Paris, Berlin, Stockholm, Munich, Dublin, and Amsterdam and ahead of Madrid. Technologies 4.0 are predominant in the Catalonian startups with 75% that have implemented initiatives to improve the sustainability of their business. Thirdly, for researchers interested in conducting research in GDPR challenges, this chapter presents a survey on the GDPR challenges faced by three technological startups. Therefore, the knowledge gained from business could be useful for governments to take action to support organizations with GDPR implementation challenges. Secondly, by identifying challenges, the organizations will be careful to avoid errors and drawbacks throughout the process of GDPR implementation.

In Chapter 4 we explained the philosophical views and approaches to the design and illustrated how the decision was made to go with the quantitative method and the use of SPSS to generate the descriptive and inferential statistics with data collected from the '*GDPR Challenges'* questionnaire were clearly explained. The questionnaire yielded 116 answers, 107 of which presented valid cases. This allowed the fulfilment of the research objective, formulating several hypotheses relative to the research questions and establishing a series of variables that would form the basis for the study's quantitative analysis. Moreover, the data collection technique has been explained, and the preliminary data testing for the quantitative study was carried out, including the exploratory factor analysis and the reliability analysis and the advanced statistical techniques has been described.

In Chapter 5 we described and discussed the analysis's results. Starting with the respondent, company profile and the startups by sectors by describing the demographic profile of the respondents, the number of years the company's respondents have been established, the number of years the respondent has been employed in the company and the weighted frequencies of the respondents by business sectors. Followed by the descriptive statistics analysis, the eight ANOVA test results analysis, the independent sample T-test analysis, the correlation test results analysis and the four regression models analysis results.

In Chapter 6 we reflected on the research aim and objectives while answering the research questions based on the Catalonian technology startups that participated in the survey, followed by a discussion of the research contribution to the body of knowledge from the research and practical perspective, presenting the practical implications of the research results, detailing the implications of the research for the key stakeholders, presenting policy recommendations, reviewing the research limitations, and proposing recommendations for future research studies.

## 1.7. Summary

This chapter presents an introduction to the research, which includes a presentation of the background to the research problem addressing the challenges organisations face arising from the enforcement of the GDPR as of May 2018. In addition, this chapter discusses the research scope, aim, objectives and questions of the study, its contributions, and the thesis structure.

The next chapter presents the literature review on the proposed topic, which includes analyzes and discusses the prior literature on the challenges faced by companies with an emphasis on technology companies and especially SMEs and tech startups, the research gap and future research directions.

# CHAPTER 2 LITERATURE REVIEW

## 2.1. Introduction

Technological development has favoured the growing collection, processing and storage of large amounts of personal data (Almeida Teixeira et al., 2019), necessitating a balance between the economic benefit of this data and customer data privacy. Globalisation and fast technological change have facilitated citizens to conveniently share data about their behaviour and preferences, sometimes without their express prior consent. This information often becomes globally available to other organisations (Poritskiy et al., 2019). The research by McDermott (2017) and Polykalas & Prezerakos (2019) show that the increasing use of big data tools allows a comprehensive analysis of personal data. Most mobile applications need access a significant amount of personal data. Because many of those mobile applications are free to download, users may still pay with their data.

The digital revolution and increasing collection of personal data by organisations has resulted in many security challenges and risks (Agarwal, 2016) as described in the artificial intelligence ("A.I.") Index 2019 Annual Report (Perrault et al., 2019). Many scholars believe that A.I. can increase human productivity and financial growth Furman & Seamans (2019). However, scholars also worry that these gains may come with costs, including possible displacement from work, income inequality and loss of confidentiality Furman & Seamans (2019).

In the European Union (E.U.), "the protection of natural persons in relation to the processing of personal data" is considered a fundamental right recognised under the Charter of Fundamental Rights of the European Union (Rodotà, 2009) and stated under the first recital of the General Data Protection Regulation ("GDPR") (European Parliament, 2016; Rodotà, 2009). The GDPR became applicable on the 25th of May 2018 after a two-year transition period ( European Parliament & Council of the European Union, 2016). The European Union's GDPR has been adopted to protect consumers' privacy (Bessen, Impink, Reichensperger, & Seamans, 2020). The principal GDPR aim is to provide E.U. natural persons within the E.U. control of their data to garner trust in the digital economy and harmonise data protection laws throughout the E.U. as part of the Digital Single Market strategy (Seo et al., 2017).

The GDPR was designed to establish uniform criteria for all the E.U. member states regarding data protection and update the requirements for the handling of personal data and privacy, which replaces and cancels the E.U.'s 1995 Data Protection Directive (de Hert & Papakonstantinou, 2016). The GDPR also aims to reform how organisations view and govern these data and remove barriers to cross-border trades, allowing the natural expansion of businesses across Europe and guaranteeing the free movement of personal data between E.U. member states (Sirur et al., 2018).

The GDPR is the starting reference point for E.U. and non-EU organisations to handle their E.U. citizens' data legally and ethically. The GDPR states the legal standards and principles for collecting and using personal data belonging to E.U. citizens. Furthermore, the GDPR grants powers to the E.U. courts to sanction any enterprise that mistreats its citizens' data according to the regulation (European Parliament, 2016). The GDPR also aims to offer an in-depth set of standards for personal data protection.

The study carried out by (Poritskiy et al., 2019) demonstrates that all industry sectors must know and exert the GDPR. However, the technology companies are the most affected ones since they must apply the established in the GDPR to process personal data and develop technology solutions that are compliant with the rules of the GDPR. Moreover, the research carried out by Norval, Janssen, Cobbe, & Singh (2021) before the GDPR came into force revealed that U.K. tech startups perceive GDPR as "vague" and "open to interpretation" and feel frustrated since there is no clear set of implementation guidelines.

However, despite the significance of GDPR for technology companies, especially tech startups, little scholarship exists on the issues faced by technology companies in their GDPR implementation technology. This study seeks to close this gap.

This chapter discusses and evaluates the literature on the challenges of GDPR implementation faced by companies before and after GDPR came into force, emphasising technology companies. The following section discusses the topic background, the main aims of the GDPR and the rise of discussions and controversies in many businesses with the GDPR implementation. This is followed by the method used in this chapter, the review of studies on GDPR implementation challenges and the effect of GDPR on technology startups and SMEs. It highlights the research gap and the issues which must be further addressed. Finally, with the help of the literature research, a conceptual framework is proposed after identifying the challenges related to GDPR implementation.

## 2.2. Context of the literature review and GDPR implementation challenges

This research provides detailed information on the GDPR challenges companies face and summarises previous research findings, particularly in the context of technology companies and the effect of GDPR on technology SMEs and startups.

The main question that has been considered to search for relevant articles is the following:

What are the key challenges of the GDPR implementation faced by technology companies?

While the literature examining the challenges associated with the GDPR implementation and the impact faced by the E.U. technology startups and SMEs is relatively large, the previous studies have generally focused on large tech companies or concentrated on specific challenges. The researchers Jian Jia & Liad Wagman (2018) concentrated only on the effect of the GDPR in the E.U. tech startups by comparing venture activity in the E.U. and the U.S. before and after GDPR came into force. The report research carried out by Populos under the order of Senzing (Jonas, 2018) concentrated only on the level of GDPR compliance, mainly on data location, of E.U. companies before the GDPR came into force. On the other hand, the report research carried out by (Norval et al. (2021) concentrated on exploring the attitudes and preparedness of some of the U.K. tech startups towards the data protection issues before the GDPR came into force. The independent report research carried out by Dimensional Research under TrustArc (TrustArc, 2017) concentrated on the level of GDPR compliance in U.K. and the U.S. companies of all sizes before the GDPR came into force. Their latest independent report research carried out by Dimensional Research under the order of TrustArc (TrustArc, 2018) concentrated in making a comparison on the level of GDPR compliance among companies of all sizes based in the U.S., U.K. and E.U. (countries other than the U.K.) after the GDPR coming into force as well as in terms of costs expenditure, efforts, most significant challenges, and motivations to become GDPR compliant by the deadline.

The study carried out by (Poritskiy et al*.,* 2019) indicate that protecting personal data, whether physical or digital, compels organisations to reinforce protection measures. This will impose a significant effort on organisations, regardless of size, to monitor and control the flow of personal data and increase awareness of potential privacy risks (Poritskiy et al*.,* 2019). Tikkinen-Piri et al. (2018) claim that the GDPR will require significant economic and human resources. It will also be necessary to adequately train employees to deal with GDPR requirements (Tikkinen-Piri et al., 2018).

Other studies by (Freitas & Mira da Silva, 2018) and (Kapoor, Renaud, & Archibald, 2018) indicate that the implementation process of the GDPR and the challenges that companies face differ, especially depending on the size of the company for small and medium-sized companies (SMEs). For SMEs with limited resources and an information management system, this is a lot of work, requiring a structured method to ensure they do not miss anything (Brodin, 2019; Supyuenyong, Islam, & Kulkarni, 2009).

Despite the importance of the GDPR for technology companies, especially technology startups, no previous studies were done on identifying the challenges faced by technology startups in Catalonia resulting from the enforcement of the GDPR, which needs to be explored.

## 2.3. Phases of the literature review

Beginning with the literature review, a review protocol describing the search string used in the selected datasets was performed in order to obtain the widest possible variety of studies capable of answering the the proposed research questions. The search terminology used, and the records are shown below:

Search string 1: GDPR AND (Challenge OR Implementation OR Impact OR Effect OR Compliance OR Adoption OR Implications OR Business OR SMEs OR tech Startups)

Search string 2: RGPD AND (Reto OR Implementación OR Impacto OR Efecto OR Compliance OR Adopción OR Implicaciones OR Compañías OR SMEs OR tech Startups)

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

Thereafter, inclusion and exclusion criteria were applied to filter the received documents. The criteria used are shown in Table 2.1. The year 2016 was chosen as the publication date, so that the literature already reflects the finally adopted GDPR.

Table 2.1: Inclusion and Exclusion Criteria

| **Inclusion criteria** | **Exclusion criteria** |
|---|---|
| Written in English or Spanish | Not written in English or Spanish |
| Release date after 2016 up to and including 2022 | Release date before 2016 |
| Scientific publications in conferences or journals | Non-free documents nor master dissertation |
| Relevance of the title in relation to the GDPR | No title relevance in relation to the GDPR |

After that, the initial group of documents were procured. In the first phase, the abstracts were then examined with regard to their importance for research. Finally, these documents were read to attain the final choice of studies to conduct the review.

We started using the previously determined verification protocol and performed an evaluation on the extracted data. Based on the work carried out by Almeida Teixeira et al., (2019) after applying the defined search string in the listed data sets, 4170 documents were obtained. With the inclusion and exclusion criteria shown in Table 2.1, 98 papers were obtained, except duplicates.

The abstracts were then read to further determine the importance of the documents, with 68 documents collected. Each of these documents have been read, yielding 58 related research for our investigation. This information is summarized in Table 2.2, as shown below.

Table 2.2: Selection of studies

| Review protocol phase | No. of studies |
|---|---|
| Data set search with string | 4170 |
| Inclusion and exclusion criteria | 98 |
| Viewed abstracts | 68 |
| Full-text document | 58 |

## 2.4. GDPR implementation challenges

GDPR gives rise to numerous discussions and controversies in numerous organisations. Research conducted by Lindgren (2018) indicated that organisations were especially concerned about the consequences – hefty fines – if they did not follow the GDRP procedures. Further, irritation with the GDPR regulation resulted in a recalcitrance to perform the required procedures. Managers and employees felt as though it was harmful to the company and its business models – especially in relation to the dimensions of the value chain. As indicated by Lindgren (2018), the business's most significant challenge might be implementing the GDPR in practice –especially for the SMEs and that the implementation of the GDPR required sweeping changes to the business's practice, especially for businesses that had not implemented a comparable level of privacy before the regulation. A number of businesses lacked internal privacy experts and knowledge about the new requirements for the protection and handling of personal data. Therefore, many of the companies surveyed indicated a strong need for training related to data protection and privacy. However, many companies did not have additional resources to address this issue – even though they saw it as a crucial factor in meeting the new GDPR requirements. Different interpretations of GDPR within companies (managers and employees) and outside companies (customers and network- partners) lead to different GDPR solutions and data protection layers.

Studies carried out by Freitas & Mira da Silva (2018) and Kapoor et al. (2018) indicate that the GDPR implementation process and the challenges faced by companies differed depending on the companies' size, with SMEs and startups facing the highest levels of challanges. The coming into force of the GDPR has had a significant impact on how tech startups and SMEs manage their businesses. This is because the GDPR is here to stay, and the tech startups and SMEs already existing at the time of the GDPR became applicable have had to adapt the way they work to meet requirements (Tikkinen-Piri et al., 2018). This has not been easy because GDPR does not provide specific guidelines to adopt its requirements (Tikkinen-Piri et al., 2018). That is why every company had to find and adopt managerial and technological solutions to achieve GDPR compliance (Tikkinen-Piri et al., 2018).

### 2.4.1. Difficulties faced by companies before GDPR enforcement

E.U. companies have faced and are still facing problems with becoming GDPR compliant. Report research carried out between the 9th and the 15th of January 2018 by Populos under the order of Senzing Jonas (2018) revealed that before the entry into force of the GDPR, 60% of the E.U. companies were not ready. The report is based on a survey of one thousand fifteen companies based in UK, Germany, France, Spain, and Italy which cover all size companies. The respondents from large companies (companies employing more than two hundred fifty people) were selected because they have been responsible for or had an impact on data protection regulations within the company or had excellent practical knowledge of data protection compliance (Jonas, 2018). Respondents from SMEs (companies employing between ten and two hundred forty-nine people) and micro-businesses (self-employed and companies employing less than ten people) were selected based on seniority (management or board level) Jonas (2018). The GDPR readiness scale was quantified based on responses to queries about knowledge, understanding and actions taken concerning GDPR.

The report survey questions designed by Jonas (2018) were directed at determining the level of knowledge about where data was stored, the level of confidence in being able to consider all different databases, the measures taken to prepare for the GDPR, the level of awareness of the reputational impact of non-compliance with the GDPR, the fines resulting from the GDPR non-compliance and confidence that the company can respond to data requests within the 30-day commitment. The results of this report research show that 60% of all participating companies were not GDPR ready to deal with the challenges that GDPR compliance would pose, and that more than about a tenth (12%) of the companies were not sure was knowing where all their data was housed Jonas (2018).

The report research by (Jonas, 2018) is relevant to the present research because it assesses the level of GDPR compliance of companies, especially the SMEs and the tech startups, before the GDPR implementation. However, although this report is of great value for the issue of GDPR compliance, mainly on data location, it does not concentrate on tech startups but companies of all sizes based in the UK, Germany, France, Spain, and Italy.

Research carried out by Norval et al., (2021) before the GDPR came into force revealed that for U.K. blockchain startups the right of erasure stated under art. 17 of the GDPR was the biggest GDPR challenge they face because "you can’t eradicate [the data], you need to find a means of making the data unavailable”.

The research carried out by Norval et al., (2021) is relevant to the present research as it assesses the GDPR challenges encountered by U.K. tech startups before GDPR implementation. The findings suggest that many U.K. tech startups struggled and or misinterpreted how compliance could be achieved. However, although the Norval research brings more light to the issue of GDPR challenges around the U.K. tech startups before the GDPR implementation, it does not concentrate on tech startups in Spain or Catalonia.

The TrustArc report TrustArc (2017) detailed the findings of their studies on U.S. and E.U I.T and Legal professionals. TrustArc retained Dimensional Research to conduct a set of surveys which concentrated on the level of GDPR compliance on U.K. and U.S. companies before the GDPR came into force and revealed the extent of the help required for U.S. and U.K. privacy professionals to comply with these data privacy requirements TrustArc (2017). For U.S. and U.K. respondents, developing a GDPR plan topped the list. Significant investments were required for consultants, new hires and technology to meet the GDPR deadline TrustArc (2017). The information on previous studies is summarised in Table 2.3, as shown below.

Table 2.3: Difficulties faced by companies before GDPR enforcement.

| AUTHOR | COUNTRY | DIFFICULTIES FACED BY COMPANIES BEFORE GDPR ENFORCEMENT | RESULTS | LIMITATIONS |
|---|---|---|---|---|
| J. Jonas., Research by Populos under the order of Senzing, (2018) | UK, GERMANY, FRANCE, SPAIN, AND ITALY. | • The level of knowledge about where data is stored.<br>• The level of confidence that all different databases can be accounted for.<br>• The actions being taken to prepare for GDPR.<br>• The level of awareness of the reputational impact and fines resulting from non-compliance with GDPR.<br>• The level of confidence that the organization can respond to data requests within the thirty-day commitment. | • 60% of the 1.015 participating companies are not GDPR ready.<br>• 12% of companies do not trust themselves to know where all their data is stored. | It does not concentrate on technology companies, but on companies of all sizes and major industry sectors based in UK, Germany, France, Spain and Italy. |
| Norval et al. (2021) | UK | • GDPR is vague and open to interpretation.<br>• No clear set of implementation guidelines.<br>• The right of erasure. | • The right to erasure as a GDPR problem for blockchain companies.<br>• Misinterpretation on how compliance could be achieved.<br>• The conviction that supervisory authorities are concentrating more on the larger | It does not concentrate on tech startups in Spain or Catalonia, but on UK blockchain startups. |

| | | | | |
|---|---|---|---|---|
| | | | tech firms than the small tech startups and SMEs. | |
| TrustArc, (2017) | US and UK | • Developing a GDPR plan<br>• High costs<br>• Privacy professionals needed the most help in complying with privacy requirements | • Developing a GDPR plan.<br>• High costs. | It does not concentrate on tech start-ups in Spain or Catalonia, but on the UK and US. |

### 2.4.2. Implementation challenges after GDPR came into force.

The latest independent report research carried out by Dimensional Research under the order of TrustArc in June 2018 TrustArc (2018) concentrated in making a comparison on the level of GDPR compliance among companies of all sizes based in the U.S., U.K. and E.U. (countries other than the U.K.) as well as in terms of costs expenditure, efforts, most significant challenges and motivations to become GDPR compliant by the deadline. Six hundred legal, information technology and privacy professionals, split evenly between the U.S., the U.K. and a selection of other E.U. countries, were surveyed. For all respondents, data protection represented at least twenty-five per cent of their work. Participating companies included small, medium and large companies from all major industries.

The report research TrustArc (2018) concludes that achieving and maintaining GDPR compliance is a complicated and expensive initiative for companies of all sizes across all geographies and industries. While 20% reported being compliant by the 25th of May deadline, 90% had started, three quarters expected to be compliant by the end of 2018 and almost all expected to be fully compliant sometime in 2019. The good news was that 87% of companies reported that the importance of privacy would continue to increase at their company, their GDPR budgets will remain active in the second half of 2018, and 80% expected to invest more in technology tools.

The report research TrustArc (2018) came out with some findings: GDPR is a work in progress, companies are motivated more by values and customer and other third party expectations than by fear of fines and litigation, companies are further ahead with updating policies and cookie management than with international data transfer and vendor risk management and GDPR has been challenging but rewarding. In the report's findings as top challenges came out GDPR complexity, lack of expertise, qualified staff and GDPR technology and tools, 65% of the respondents confirm to be optimistic about the impact of GDPR on their business, that GDPR will continue to dominate privacy efforts and that achieving, maintaining, and demonstrating GDPR compliance are the top three privacy priorities over the next 6-12 months and 50% of the respondents will seek a third party GDPR validation rather than wait for the official GDPR certification.

Although this report is of great value, it does not concentrate on the GDPR level of compliance and challenges for the startups, but on the level of GDPR compliance among companies of all sizes based in the U.S., U.K., and E.U. (countries other than the U.K.).

The research study carried out by Poritskiy et al. (2019) applies a quantitative methodology, based on a survey undertaken with 286 Portuguese I.T. companies indicates as two of the main challenges for GDPR compliance, first the complexity to execute periodic audits to ensure that all processes are compliant with GDPR and second, to establish a straightforward procedure to delete an individual's data. Although this report is also of great value, it does not address the types of challenges presented at each stage of GDPR adoption, and does not consider the specifics of the activities undertaken by each company. The main findings of these two studies are summarized in Table 2.4, as shown below.

Table 2.4: Implementation challenges after GDPR coming into force.

| AUTHOR | COUNTRY | IMPLEMENTATION CHALLENGES AFTER GDPR COMING INTO FORCE | RESULTS | LIMITATIONS |
|---|---|---|---|---|
| TrustArc, (2018) | US, UK AND EU | • GDPR complexity.<br>• Lack of qualified staff<br>• Lack of GDPR technology and tools<br>• Costs<br>• Expenditure.<br>• Effort | • 65% achieving, maintaining, and demonstrating GDPR compliance are top priorities.<br>• 50% will seek a third party GDPR validation rather than wait for the official GDPR certification. | It does not concentrate on technology companies in the EU and the US, but on companies of all sizes from all major industry sectors. |
| Poritskiy et al. (2019) | PORTUGAL | • Conducting audits of systems and processes.<br>• Application of the right to erasure. | • The state of implementation of the gdpr and the kind of company are discriminatory determinants.<br>• The application of the right to erase | It does not:<br>• Search the types of challenges faced at each phase of GDPR adoption.<br>• Consider the specific of the activities carried out by each company. |

## 2.5. The effect of GDPR on technology startups and SMEs

Discussions on data protection and especially GDPR have focused on the larger tech companies like Facebook and Google and what these laws mean to users of such services (e.g. see Houser & Voss (2018)) and the discussions that have focused on small tech startups, have been specially about one country**,** the U.K. (e.g. see Norval et al. (2021)). However, startups and SMEs also require attention, especially tech startups which are driven by innovation, pushing the boundaries of technology but lacking established best practices for data protection. Initial decisions by startups can certainly have negative long-term effects. Therefore, ensuring that tech startups' innovations and practices are robust, appropriate, and acceptable should be a high priority (Norval et al., 2021). Supervisory Authorities need to provide more support to the tech startups, in terms of increasing awareness and guidance. They also need to take an active role to prevent harm and deter so that the startups get the best opportunities to innovate within the framework of the GDPR (Norval et al., 2021). There is the conviction that the Supervisory Authorities are concentrating more on the larger tech firms than the small tech startups and SMEs; if that is the case, the negative long-term impact can be devastating.

Moreover, the GDPR costs implication for the tech startups and the SMEs are creating struggles in innovation. Theoretical works of Krasteva, Sharma, & Wagman (2015) and Campbell, Goldfarb, & Tucker (2015) show that compliance costs and data regulation can create barriers to entry and may negatively affect innovation. The researchers Campbell et al. (2015) show that although privacy regulation forces costs on all companies, the small and new companies are the most negatively affected, especially for goods where the price mechanisms do not mediate the effect, such as the advertising-supported internet. Also, the researchers Krasteva et al. (2015) show that as the costs of compliance by small companies increase, more innovations will be developed within established companies. As the work of Kortum & Lerner (2000) shows that the industrial innovations that venture capitalists help facilitate are a multiple of the ratio of venture capital to the R&D expenditures (as cited in Jia, Jin ann Wagman (2018)).

The researchers Goldberg, Johnson, & Shriver (2019) show in their study that the GDPR has impacted online outcomes; research using data from Adobe Analytics quantified the impact of GDPR on critical economic outcomes for a diverse set of firms. Significant mean impacts were noted: page views per week decreased by approximately 4%, and revenue per week decreased by 8%. These are economically large numbers, with an 8% revenue per week drop corresponding to an $8,000 drop-in weekly revenue for the median in their sample (Goldberg et al., 2019). However, researchers provide evidence that changes in user behaviour do not directly drive these results. From a researcher's perspective, the above results evidently illustrate the complexity and high costs of privacy regulation. The Adobe Analytics data illustrated just a portion of the total cost of complying with GDPR - omitting high operational and infrastructure costs (Goldberg et al., 2019). However, more research still needs to be carried out to quantify the benefits to GDPR’s users to understand the trade-offs better.

Research carried out by Norval et al. (2019) before the GDPR came into force revealed that some U.K. tech startups remained unable or unwilling to make a continuing GDPR compliance effort. However, tech startups always need to take their regulatory obligations seriously. Therefore, although this report is of great value, primarily because it mainly deals with tech startups, it could have been more relevant for this study if companies from the E.U. and specifically from Spain had also participated.

The research report by TrustArc (2018) reveals that E.U. companies regardless of the size have faced and are still facing problems such as GDPR complexity, lack of expertise, qualified staff and GDPR technologies and tools to be GDPR compliant. Being GDPR compliant is not a one-off event but a long-term commitment. Companies cannot make the mistake of not thinking about it anymore, as this could be very costly. Rob Perry (2019) mentions that a key strategy and challenge is to develop and implement a set of best practices to set up permanent automated GDPR processes without investing as much time, resources and money and the appointment of a Data Protection Officer (DPO) to consider wisely.

DPOs appear to be especially valuable for startups that innovate with technology, as they can continuously support the business with compliance and best practices over the entire product lifecycle: beginning, design, implementation, and operations. However, research indicates that many startups either do not see a DPO as appropriate for their organization or have appointed someone internally as a DPO, regardless of their data protection expertise or organizational independence Lachaud (2014). A DPO should have expert knowledge of data protection laws and practices. The researcher's perception of why this may be happening lies in the complexity and difficulty of understanding the GDPR and that it is costly to invest in a DPO or a Chief Privacy Officer (CPO). Determann (2020), a CPO, should also be considered since many companies understanding what is required to become compliant has been one of the biggest problems because the GDPR does not offer the practical solutions to be GDPR compliant. The roles of DPO and CPO are not identical, while the DPO reports to the highest levels in the company; his or her role is to guarantee data compliance. In U.S. firms, the CPO assumes more of a strategic, forward-planning role for activities globally, rather than a DPO, who will report a reduction in redundancies and costs (Voss & Houser, 2019)**.** Moreover, Professors Bamberger and Mulligan describe their studies on U.S. practices as follows: "The CPOs described a forward-looking focus on identifying future challenges rather than meeting existing mandates. They also underscore the potential for environmental ambiguity, combined with credible threats with meaningful sanction, to compromise the scope of the privacy function within corporate organisations. Our respondents described a wide reach across the organization, authority to participate in strategic decisions about the company's business, and relatively wide latitude to establish company practices and define their responsibilities." (Bamberger & Mulligan, 2015, p. 194-95). Many companies voluntarily appoint a CPO to show internally and externally that the company takes data protection compliance seriously, but this is challenging for startups with a limited budget.

## 2.6. Research gap and issues to be addressed.

Previous research studies in this area mainly emphasize on companies of all sizes, major sectors and especially on SMEs and does not consider the specific of the activities carried out by each company nor concentrate on technology companies and when it does it concentrates on SMEs and not tech startups, as shown in Table 2.5.

For example, Freitas et al. (2018) carried out a qualitative research of 10 Portuguese SMEs' to find out whether those companies were GDPR compliant or conducting activities to adjust to the most critical issues of the new Regulation. Härting et al. (2020) first carried out a qualitative research project, developed a hypothesis model, and from the analysis of which six constructs emerged: Know-how, expenditure of time, uncertainty, costs, provision of information, and process adaption; to find out that each of these constructs has a negative impact on the dependant variable "impacts on the implementation of GDPR in pre-existing business models for SMEs". Norval et al. (2021) carried out qualitative research on 15 UK tech startups to explore how they perceived GDPR coming into force, the impact and implementation to find out that many of these tech startups struggled and/or misinterpreted how compliance could be achieved and the importance of the role of regulators in providing more support.

Table 2.5: Related work

| **AUTHOR** | **COUNTRY** | **GDPR IMPLEMENTATION CHALLENGES** | **RESULTS** | **LIMITATIONS** |
|---|---|---|---|---|
| J. Jonas., research by Populos under the order of Senzing, (2018) | UK, GERMANY, FRANCE, SPAIN, AND ITALY. | The level of knowledge about where data is stored.<br>The level of confidence that all different databases can be accounted for.<br>The actions being taken to prepare for GDPR.<br>The level of awareness of the reputational impact and fines resulting from non-compliance with GDPR.<br>The level of confidence that the organization can respond to data requests within the thirty-day commitment. | 60% of the 1.015 participating companies are not GDPR ready.<br>12% of companies do not trust themselves to know where all their data is stored. | It does not concentrate on technology companies, but on companies of all sizes and major industry sectors based in UK, Germany, France, Spain and Italy. |
| Norval et al. (2021) | UK | GDPR is vague and open to interpretation.<br>No clear set of implementation guidelines.<br>The right of erasure. | The right to erasure as a GDPR challenge for blockchain companies.<br>Misinterpretation on how compliance could be achieved.<br>The conviction that supervisory authorities are concentrating more on the larger tech firms than the small tech startups and SMEs. | It does not concentrate on tech start-ups in Spain or Catalonia, but on UK blockchain startups. |
| TrustArc, (2017) | US AND UK | Developing a gdpr plan.<br>High costs. | Development of a GDPR plan. | It does not concentrate on tech |

| | | | | |
|---|---|---|---|---|
| | | Privacy professionals needed the most help in complying with privacy requirements. | High costs. | start-ups in Spain or Catalonia, but on the UK and US. |
| TrustArc, (2018) | US, UK, AND EU | GDPR complexity.<br>Lack of qualified staff.<br>Lack of GDPR technology and tools.<br>Costs.<br>Expenditure.<br>Effort. | 65% achieving, maintaining, and demonstrating GDPR compliance are top priorities.<br>50% will seek a third party GDPR validation rather than wait for the official GDPR certification. | It does not concentrate on technology companies in the EU and the US, but on companies of all sizes from all major industry sectors. |
| Poritskiy et al. (2019) | PORTUGAL | Conducting audits of methods and processes.<br>The use of the right to erase. | The level of implementation of the GDPR and the type of company are discriminating factors.<br>The application of the right to erase. | It does not:<br>examine the types of challenges presented at each phase of GDPR adoption.<br>Consider the specifics of the activities carried out by each company. |
| Freitas & Mira da Silva (2018) | PORTUGAL | GDPR is a very complex and extensive regulation.<br>High costs.<br>Missing know-how.<br>Unaware of their obligations. | SMEs lack of awareness and high costs has a significant influence on the GDPR implementation. | It does not consider the specifics of the activities carried out by each company.<br>Qualitative research of 10 SMEs Portuguese companies. |
| Härting et al. (2020) | GERMANY | Lack of know-how.<br>Time expenditure.<br>Uncertainty.<br>High costs.<br>Insufficient information provision.<br>Process adaptation. | Know-how, costs, information provision and process adaptation have a negative impact on GDPR implementation. | Only for existing business models for German SMEs.<br>The questionnaire is only designed for German-speaking areas. National mentality could affect the results. The results could seem different in other countries despite the identical legal situation. |

The analysis of previous studies on the challenges of the GDPR implementation faced by companies and especially technology SMEs and startups show that they exist. Furthermore several authors agree that the technology companies are one of the most affected in terms of processing data and developing technological solutions that comply with the GDPR (Härting et al., 2020; Härting et al., 2021; Norval et al., 2021; and Poritskiy et al., 2019), in terms of compliance costs (Freitas et al., 2018; Härting et al., 2020; and Härting et al., 2021) government support (Härting et al., 2020; Härting et al., 2021; and Norval et al., 2021), regulation complexity (Härting et al., 2020; Härting et al., 2021; and Norval et al., 2021) and government support (Härting et al., 2020; and Härting et al., 2021), and process adaptation (Poritskiy et al., 2019).

However, there is a lack of information on how familiar technology startups are with the GDPR five years after the GDPR came into force, including: the key challenges of the GDPR implementation faced by them, whether they are associated with compliance costs, regulation complexity, insufficient government support or process adaptation and if there is any relationship between the challenges faced by them and the year of establishment, size, business sector, and annual expenditure on GDPR compliance. Thus, further research is needed since by identifying challenges, the organizations will be careful to sidestep errors and drawbacks throughout the procedure of GDPR implementation and it may be useful for the governments to take measures to support organizations with challenges of implementing GDPR.

## 2.7. Conceptual framework

For the creation of the theoretical framework using the academic search engine Scopus in October 2021, five search strings in English and Spanish languages were applied, and the results are summarized as shown in Table 2.6.

Table 2.6: Search Strings

| **Number** | **Search Strings** | **Nº documents** |
|---|---|---|
| 1 | GDPR OR "general data protection regulation") AND challenge* AND (startup OR startup OR "entrepreneurial enterprise") AND (Europe* OR "E.U." OR "European Union | 3 |

| | | |
|---|---|---|
| 2 | ((GDPR OR "general data protection regulation") AND challenge* AND (SME OR "small and medium enterprise") AND (Europe* OR "E.U." OR "European Union")) | 10 |
| 3 | ((GDPR OR "general data protection regulation") AND challenge* AND (startup OR start-up OR "entrepreneurial enterprise") AND (Spain OR span* OR catalonia* OR catalan)) | 0 |
| 4 | ((GDPR OR "general data protection regulation") AND challenge* AND (SME OR "small and medium enterprise") AND (Spain OR span* OR Catalonia* OR Catalan)) | 0 |
| 5 | (GDPR OR "general data protection regulation") AND challenge* | 524 |

Because after applying the first four search strings, very few studies were found, it was broadened and added one more string. The literature research helped the author decide on an appropriate structure for the framework and highlighted a gap in the challenges faced by startups resulting from the implementation of the General Data Protection Regulation (GDPR) as of May 2018.

In analysing the paper title and abstracts, 27 were categorised as relevant. Thirty-two challenges were identified related to GDPR and grouped into the four different constructs/categories: Compliance costs (Campbell et al., 2015; Freitas & Mira da Silva, 2018; Hurdik, 2018; Krasteva et al., 2015; Pedroso, Araujo, Cota, & Magalhaes, 2021; Tikkinen-Piri et al., 2018), regulation complexity (Härting, Kaim, & Ruch, 2020; Presthus & Sønslien, 2021), government support (Norval et al., 2021; Cochrane, L., Jasmontaite-Zaniewicz, L., Barnard-Wills, 2020; Hurdik, J 2018) and process adaptation (Poritskiy et al., 2019; Grundstrom, Väyrynen, Iivari, & Isomursu, 2019; Mansfield-Devine, 2016; Ahmed et al., 2020; Sarkar, Banatre, Rilling, & Morin, 2018; Rhahla, Allegue, & Abdellatif, 2021; Mangini, Tal, & Moldovan, 2020; Politou, Alepis, & Patsakis, 2018). These challenges are also confirmed by the researcher's interviews with three Catalan startups registered in the Agency for Business Competitiveness (ACCIÓ).

COMPLIANCE COSTS.

The work of Hurdik (2018) shows that one of the key challenges for the Czech business concerning the implementation of GDPR is the lack of financial means. The works of Freitas & Mira da Silva (2018), Tikkinen-Piri et al. (2018), Layton & Elaluf-Calderwood (2019), Sirur et al. (2018) and Yeung & Bygrave (2022) show that the implementation of GDPR is a challenge for any company, and in particular for small and medium-sized enterprises (SMEs), since they have fewer human and financial resources to carry out the necessary measures to comply with the regulation. In the research work of Pedroso et al. (2021) and Li, Werner, & Ernst (2019) it was found that while large companies can implement and respond appropriately to the GDPR implementation challenges, SMEs and startups do not always have the expertise and resources to do so. Within the research findings of Grundstrom et al. (2019) and Nabbosa & Iftikhar (2019) research work findings, participants also perceived the GDPR compliance process negatively due to its cost.

REGULATION COMPLEXITY.

The research study by Härting et al. (2020) consisted of semi-structured interviews with thirteen German experts in data security or data protection responsible for their respective companies. The company itself had to be an SME, with no more than 500 employees or an annual turnover of 50 million euros. Härting et al. (2020) handled the analysis of the interviews by utilizing two techniques, a hybrid model of a cluster analysis according to Landau et al. (2011) and a structured content analysis according to Mayring (2000). The six constructs crystallized out of the analysis: know-how, expenditure of time, uncertainty, costs, provision of information, and process adaptation. Although the research by Härting et al. (2020) concentrated on German SMEs, their research is still valuable for the study considering similar constructs.

The studies carried out by Presthus & Sønslien (2021), Martínez-Martínez (2018), Yeung & Bygrave (2022) and Jantti (2020) confirm that GDPR is complex and challenging as also claimed by Almeida Teixeira et al. (2019) and Koops (2014). Koops argues that in practice the GDPR complicates data protection with ambiguous wording and complex dependencies between some articles. There is a disconnect between law and reality. Moreover, Tikkinen-Piri et al. (2018)

(Mansfield-Devine (2016) argue that the GDPR does not ‘spell out’ what companies need to do to be compliant and Politou et al. (2018) argues that GDPR is mainly a legal document, which lacks on technical guidance to the companies that are obliged to implement it (Grundstrom et al., 2019). Additionally the study by Nabbosa & Iftikhar (2019) confirms how challenging is for companies to ensure their providers, suppliers and vendors, among others, comply with the GDPR and the research work by Grundstrom et al. (2019) and Jantti (2020) also proves that companies find challenging to change the company mindset to ensure that each employee starting with the top management follows GDPR principles. The research work by Li et al. (2019) finds also challenging for startups to train existing employees about GDPR requirements, limiting the company's ability to comply.

GOVERNMENT SUPPORT.

Pedroso et al. (2021) refer into their work the communication from the European Commission to the European Parliament and the Council on two years of application of the GDPR report (European Commission, 2020). The communication highlights the need for more practical advice, including more concrete examples, and for data protection authorities to be given the necessary human, technical, and financial resources to carry out their tasks effectively Pedroso et al. (2021).

Cochrane, Jasmontaite-Zaniewicz & Barnard-Wills (2020) carried out an online survey of 52-60 SMEs representatives and semi-structured qualitative interviews with 18 Data Protection Authorities (DPAs), 22 SME Association representatives and 11 SME representatives. The researchers found that SMEs and SME Associations argue for more practical guidelines from the DPAs to comply with GDPR, for more specific instruments or tools such as templates that could be easy to adapt to the specific context of the company and for more information support from the DPAs since the guidance provided is theoretical, generic and vague (Cochrane, Jasmontaite-Zaniewicz, Barnard-Wills, 2020).

Within the research findings of Grundstrom et al. (2019) and Sirur et al. (2018) the challenge of companies providing evidence for accountability came up since there is a risk of companies being accountable when there are not clear GDPR guidelines to follow. The research study carried out by Ryan, Crane, & Brennan (2021) shows that a key challenge for regulatory technology companies is that GDPR does not provide any specific instruments or tools for companies to demonstrate compliance.

PROCESS ADAPTATION.

Tim Erridge, Context Information Security in an interview carried out by Steve Mansfield-Devine, editor of the Computer Fraud & Security (Mansfield-Devine, 2016), when asked how do you know if your systems are compliant with GDPR, he states that GDPR is not a compliance framework, it is about being able to demonstrate due diligence, that you have done all you can to safeguard that data. Therefore, a key challenge for any company is to demonstrate an already developed cyber incident response plan that will meet the spirit of GDPR and reduce the risk of fines (Mansfield-Devine, 2016).

For Politou et al. (2018), it is a challenge to apply emergent technologies such as Big Data to achieve better compliance with the GDPR, and for Politou et al. (2018), Mangini et al. (2020) and Sarkar et al. (2018) it is also a challenge to establish a straightforward procedure to delete an individual’s data. For Raschke et al. (2018), Rhahla et al. (2021) and Jantti (2020), it is also challenging for companies in times of Big Data and Cloud Computing to achieve better compliance with the GDPR, considering the large amount of data a controller might process of a single data subject and especially when the processing also involves external third parties with the use of one or several service providers.

Grundstrom et al. (2019) carried out an ethnographic qualitative descriptive study of a 2-day workshop in which five European insurance companies shared sensemaking results in their companies and knowledge around GDPR. Grundstrom et al. (2019) examined how the participants interpreted the GDPR and the compliance challenges they faced by categorising them into the following four dimensions of personal data access: Procedure, protection, privacy and proliferation. Grundstrom et al. (2019) found that processing data quickly is one of the biggest challenges for companies to process since more and more data comes in every day. Among the other challenges is the difficulty of ensuring the portability of personal data, especially when there is no standard format available, to provide the company's stakeholders with access to their data and establish a straightforward procedure to delete an individual's data.

The research by Nabbosa & Iftikhar (2019) work research identifies the following GDPR challenges faced by digital retailers when applying emergent technologies, the difficulty of developing a cyber incident response plan and adapting their existing business model to ensure successful GDPR compliance.

A study carried out by Poritskiy et al. (2019) applies a quantitative method based on a survey undertaken with 286 Portuguese I.T. companies delineates two main challenges for GDPR compliance, first, the complexity to execute periodic audits to ensure that all processes are compliant with GDPR and second, to establish a straightforward procedure to delete an individual's data.

(Ahmed et al., 2020) in their research on online social networks investigates the link between GDPR provisions and blockchain technology to solve the consent management problem in online social networks. (Ahmed et al., 2020) confirm the existence of challenges to be GDPR compliant such as the informed consent, the data erasure and identifying the data controller when applying emergent technologies, in this case, blockchain, to achieve better compliance with GDPR. Fähnrich & Kubach (2019) based on their experience as consulting companies regarding I.T. security and privacy matters, their study concludes that GDPR exceeds previous regulations and challenges companies of any size, especially SMEs, since there is a lack of resources and expertise to adapt their existing business model.

## 2.8. Summary

In this chapter, we analyzed and discussed the prior literature on the challenges faced by companies with an emphasis on technology companies and especially SMEs and tech startups. There are two main implications from this review. First, this chapter presents a review on the GDPR challenges faced by companies. Therefore, the knowledge derived from business could serve useful for the governments to take measures to support organizations with challenges of implementing GDPR. Second, by identifying challenges, the organizations will be careful to sidestep mistakes and drawbacks throughout the procedure of GDPR implementation.

# Chapter 3 Technological startups in Catalonia

## 3.1. Introduction

As many startups increasingly embrace growth and transformational technology while remaining private, they have become an integral part of the economy. They have a substantial influence on employees, communities, and other stakeholders. It is time to pay much more attention to understanding their inner dynamics and the recurring problems they face (Pollman, 2019).

The coming into force of the GDPR has had a significant impact on how tech startups manage their businesses. The GDPR has come to stay, and the tech startups already existing at the time of the GDPR coming into force have had to adapt the way they work to comply, making it a critical current issue partially due to the governance complexity of extreme late-stage startup (Pollman, 2019).

## 3.2. Definitions of startup

Research shows that innovations developed by startups are often created by former employees of firms who undertake projects that had been overlooked by their employers (Sørensen & Fassiotto, 2011). Despite the significant tax, information, and scale advantages an employer has over a venture-backed startup, many employers have preferred to have their employees pursue a venture backed startup. Because the cost of increased property-rights-perfecting activity associated with an increase in incentive necessary to retain an employee would exceed the benefit of retaining the innovation (Bankman, Gilson, Bankman, & Gilson, 1999).

There are quite a few definitions of startups, (Kollmann, Jung, Kleine-Stegemann, Ataee, & de Cruppe, 2020) define startups as those younger than ten years old and (highly) innovative in their technology and/or their business model, and have or are aiming for significant growth in the number of employees and/or revenue. Ries (2011) identified a startup as an institution that operates under highly uncertain conditions to develop new products or services.

In addition, the Spanish Startup Act 28/2022 defines the startup concept. It targets startups or companies of less than 5 years (7 years in the case of biotechnology, energy, industrial and other strategic sectors, or that have developed their technology designed entirely in Spain). Furthermore, the startups or companies must also be independent of other companies, not listed in a stock market, do not distribute or have distributed profits, are innovative and have an annual turnover of up to €5 million (Secretaría de Estado de Comunicación. Consejo de Ministros., 2021). Although the Startup Act came into force on the 22nd of December 2022, the research will be based on the definition of startup provided by ACCIÓ since the researcher uses the data base provided by ACCIÓ, the theoretical framework was defined, and the data was collected from May 2021 to November 2021. In the context of the recent enforcement of the Startup Act, it can be considered a limitation, although the results present enormous value.

ACCIÓ is the Catalan Government's agency for business competitiveness and is part of the Ministry of Economy and Employment; it is the public accessible organisation that works to contribute to the transformation of Catalan companies, collaborating with public and private institutions in building tomorrow's company today. ACCIÓ manages the Barcelona and Catalonia Startup Hub, including over 1.700 startups in Catalonia, and provides activity and contact details information and shows aggregate graphic information. It enables searches by industry, technology, region, business model, company size, and financing phase. It allows spinoffs to be filtered and provides information on their main public players. It contains links to collaborators and online sources of information and offers the possibility to register via a data registration form.

Within the requirements to be part of the home directory (Strategic and Competitive Intelligence Unit ACCIÓ, 2021), the following definition of a startup is stated:

“A startup is a company:

- With a NIF number (not the self-employed).
- Created by entrepreneurs who want to make it grow (ambition).

- Recently established (less than 10 years since inception) and with a finished product for sale (except biotech).
- Scalable with high growth potential, with the ability to grow without being hampered by its structure or available resources (time and money).
- Highly innovative or technological and aimed at the international market.
- That does not provide consulting or program/app development services only on customer request but as its product. This should also not be a static website/landing page.
- This category also includes spin-offs, i.e. companies founded by members of a research centre such as a university. The goal is the transfer of knowledge into an application area that is ideal for the R&D area. In addition, it offers researchers the opportunity to put their projects into practice. The original institutes are involved in the new company.

A company is no longer a startup when:

- It has been taken over by a corporation or taken public *(EXIT)*.
- The founders no longer have managerial responsibilities and have become pure shareholders.
- It remains inactive for more than 1 year" (Strategic and Competitive Intelligence Unit ACCIÓ, 2021).

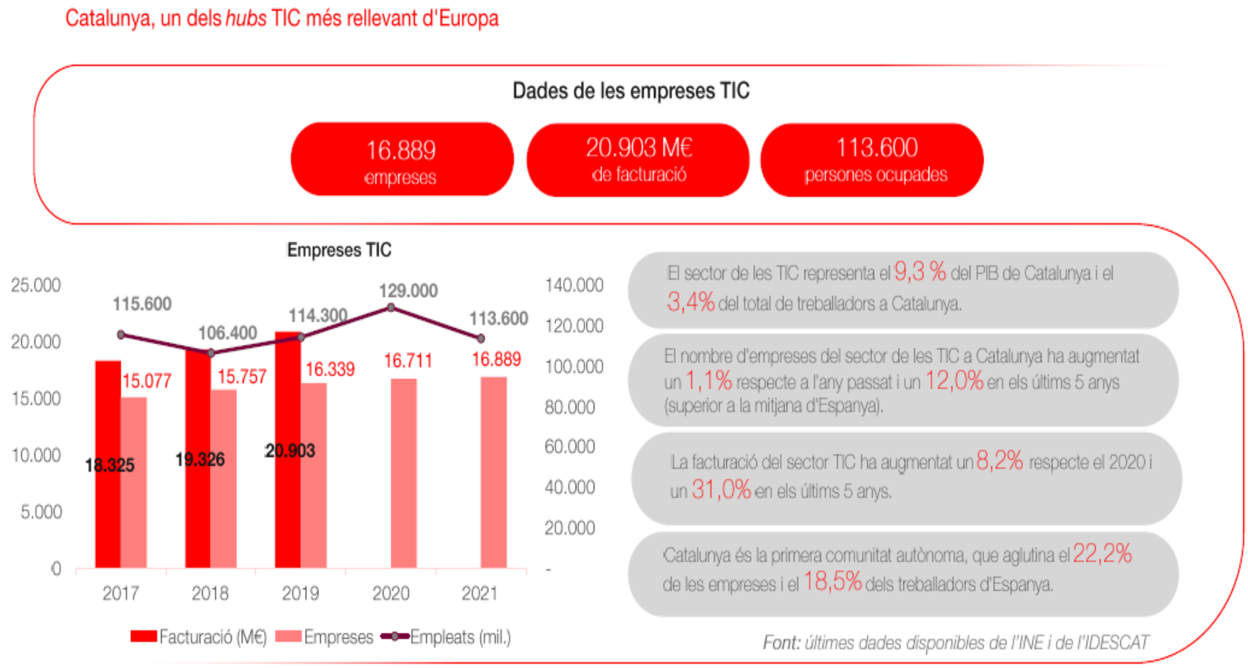
## 3.3. Catalonia as a world-leading technological hub

### 3.3.1. The digital economy in Catalonia

Based on the Digital Economy in Catalonia sector snapshot (Strategic and Competitive Intelligence Unit ACCIÓ, 2022), Catalonia's industrial, technological, and Digital economy has converted Catalonia into a technologic hub of world reference since Catalonia has a muscular TIC and Digital ecosystem. Catalonia is the fifth region most digitalized of the EU, with prestigious R+D centres that support the transfer of technology, clusters, and universities and have many initiatives that support the technology companies. With more than 300 technological projects and 2.800 M€ of invested capital between 2017 and 2021, Catalonia is a leading destination in occidental Europe in the digital economy (Strategic and Competitive Intelligence Unit ACCIÓ, 2022). The talent, market, and positioning make the companies' difference in investing in technology in Catalonia. So, companies such as Microsoft, Facebook and Seat have their Digital Innovation Hubs in Catalonia. The investments in Digital Hubs have increased from 9 to 34 in one year (Strategic and Competitive Intelligence Unit ACCIÓ, 2022).

In their study frame, the Strategic and Competitive Intelligence Unit ACCIÓ (2022) have considered as Digital Economy the combination of the companies included in the TIC sector and the rest of other digital sectors that revolve around the sector's digitalisation to transform the world into a more intelligent and connected place. These digital areas are the videogames, the audio-visual sector, electronic commerce, startups, industry 4.0, the smart cities and the engineering related to the TIC. The digital economy accelerated because of the continuity of innovation with diapositive's and technological infrastructures, each time more intelligent and connected (Strategic and Competitive Intelligence Unit ACCIÓ, 2022). As crucial data of the digital economy in Catalonia in 2021, there were 19.148 companies, 29.520 M€ invoicing and 175.949 people working (Strategic and Competitive Intelligence Unit ACCIÓ, 2022). Catalonia is one of the TIC hubs more relevant in Europe, as seen on the figure 3.1.

Figure3.1: Catalonia, one of Europe's largest ICT hubs.



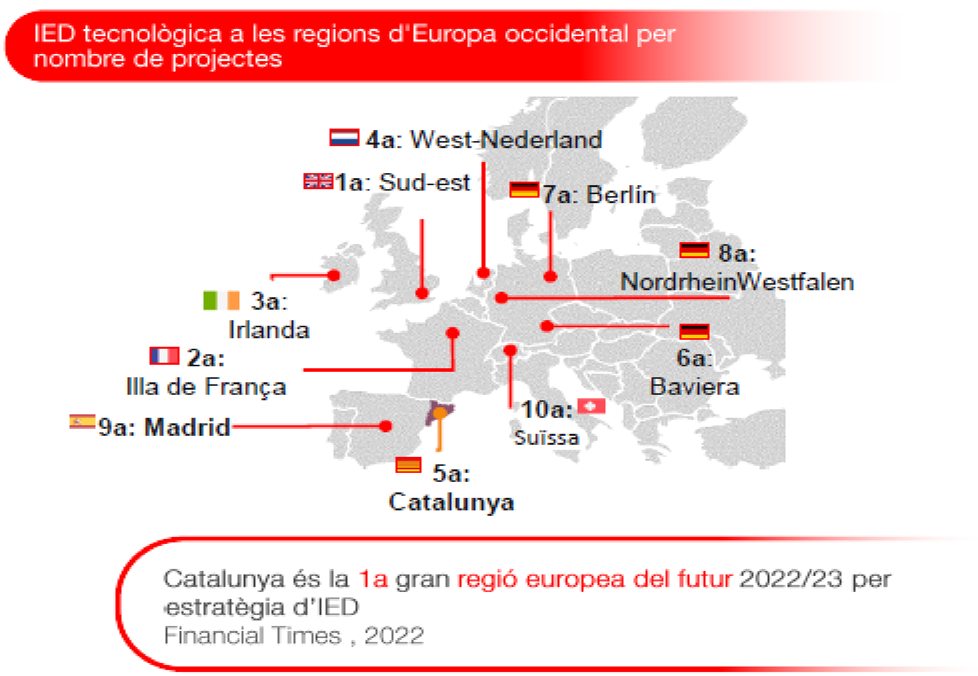

Source: ACCIÓ obtaining the latest data available from INE and IDESCAT.

### 3.3.2. Catalonia on the global startup stage

The European Commission monitors the digital progression of member states using the Digital Economy and Society Index (DESI), and in 2021 Catalonia appears the 5th region most digitalised of the E.U. after Finland, Sweden, Denmark, and the Netherlands. Moreover, in 2019 Aliança 5G Barcelona reported that Catalonia is the first European region to open a 5G lab. Based on the BCG report, 34 of the 50 top global innovative companies are found in Catalonia (D'ACCIÓ, 2022). In the year 2021, it was successfully launched the first Catalan nanosatellite designed by the Universitat Politècnica de Catalunya (UPC) to gather data to fight against climate change. Catalonia is house to several scientific and research institutions of the first level. Prestigious research groups support the technology transfer, and an entire group of scientific and technological centres are the base of the Catalonian research and innovation programme (D'ACCIÓ, 2022).

As seen below on the figure3.2, Catalonia is the leader destiny for IED technology. It occupies 5th place on the Occidental European Regions in many technological projects, the 5th in occupation creation and the 9th on capital investment. 3,7% of the technological projects on Occidental Europe, 4,7% of jobs created and 2,2% of the invested capital. Between 2017 and 2021, Catalonia was the first destination of the IED technology in Spain, with 39,7% of the IED projects, 38,8% jobs created and 28,4% of the investment.

Figure 3.2: Technological FDI into Western Europe regions by number of projects.




Source: ACCIÓ obtaining the data available from fDi Market 2017-2021.

In 2021, 34 of the 66 (51%) of the technological projects carried out are installations of innovative Digital Hubs in Catalonia. This amount has been increasing last years due to innovative and technology company investments in Catalonia, which in the case of Digital Hubs has increased dramatically in 2021, passing from 9 to 34 in one year. It represents an increase of 278%.

### 3.3.3. Barcelona on the global startup stage

Based on the Global Startup Ecosystem Index report by StartupBlink (StartupBlink, 2021), Barcelona is the 5th ecosystem in the E.U. to set up a startup behind Paris, Berlin, Stockholm and Amsterdam, and ahead of Munich, Helsinki, Madrid, Dublin and Milan. Updated annually since 2017, StartupBlink's Global Startup Ecosystem Index is the most comprehensive startup ecosystem in the world, ranking in 1000 cities and 100 countries. The Global Startup Ecosystem Index is based on hundreds of thousands of data points, which are treated by an algorithm that takes into consideration several dozen parameters, such as data on registered startups, accelerators and coworking spaces, among others.

Based on the Startup Heatmap Europe report 2021 (Startup Heatmap Europe, 2021), Barcelona is the 2nd E.U. startup hub of founders for setting up a startup behind Berlin. Furthermore, 17% of founders see the city as an attractive hub. Barcelona has remained in this position for the fourth year running. Barcelona is also the $2^{nd}$ E.U. startup hub with the highest global founders. This makes Barcelona one of the most cosmopolitan hubs, just behind Berlin and ahead of Amsterdam, Stockholm, or Helsinki.

Based on Dealroom sources dated 26/01/2022 introduced within the Barcelona & Catalonia Startup Hub 2021 Analysis (Strategic and Competitive Intelligence Unit ACCIÓ, 2021), Barcelona is the $4^{th}$ E.U. hub in terms of the amount of rounds of funding raised for startups in venture capital just behind Paris, Berlin, and Amsterdam. Furthermore, Barcelona in 2021 is the $6^{th}$ hub in the E.U. in the volume of finance raised for startups in venture capital.

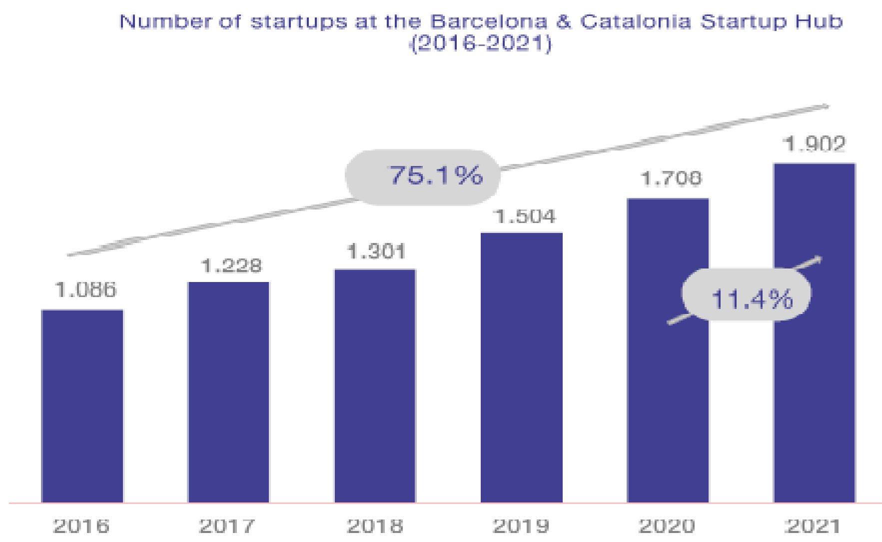
Based on the Dealroom sources dated December 2021 introduced within the Barcelona & Catalonia Startup Hub 2021 analysis (Strategic and Competitive Intelligence Unit ACCIÓ, 2021), Barcelona is the $4^{th}$ ecosystem in the E.U. with the highest number of scaleups. A scaleup is a startup that has raised over US$1 million, excluding those taken over or that have gone public (exits). Barcelona is also the $7^{th}$ E.U. startup hub in future unicorns behind Paris, Berlin, Stockholm, Munich, Dublin, and Amsterdam and ahead of Madrid. A future unicorn is a tech company valued at more than US$250M but less than US$1B, excluding those taken over or that have gone public (exits).

## 3.4. Main features of startups in Catalonia

Based on the Barcelona & Catalonia Startup Hub 2021 analysis (Strategic and Competitive Intelligence Unit ACCIÓ, 2021), in 2021, 1.902 startups were identified in the Barcelona & Catalonia Startup Hub, which represents an increase of 75,1% between 2016 and 2021, 47% of the startups were set up within the past five years, 87,7% of the startups are located in the Metropolitan Area of Barcelona. Health, business services, ICT/Mobile, and leisure account for 42% of the startups, 86,8% of the startups work with technologies linked to industry 4.0, 47,3% of the startups work with technologies related to Deeptech, 46% of the startups have a patent or system to protect their knowledge, 67% of the startups implement shared value models; 75%, sustainability models. Ecommerce & Marketplace, and SaaS are the predominant business models. The data was analysed based on the 1.902 startups in the ACCIÓ Barcelona & Catalonia Startup Hub on the 31st of December 2021.

The number of startups in Catalonia has increased by 75.1% since the creation of the Barcelona & Catalonia Startup Hub from 1,086 startups in 2016 to 1,902 in 2021. The startups in the Barcelona and Catalonia Startup Hub grew by 11.4% between 2020 and 2021 as seen on the figure 3.3. The Barcelona and Catalonia Startup Hub identifies more and more startups in Catalonia every year. In line with what they consider to be a startup, the companies established over 10 years ago and those no longer trading are excluded from the Hub. In 2021, 503 new companies were registered and 309 were excluded.

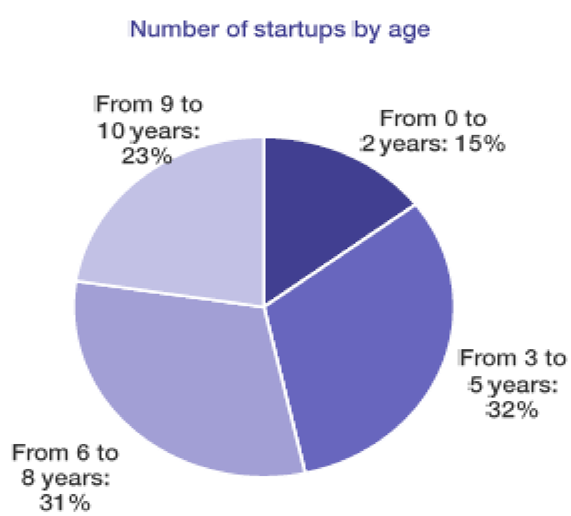
Figure 3.3: Number of startups at the Barcelona & Catalonia Startup Hub (2016-2021).




Source: Barcelona & Catalonia Startup Hub 2021

Based on the Barcelona & Catalonia Startup Hub 2021 analysis (Strategic and Competitive Intelligence Unit ACCIÓ, 2021) 47% of the Barcelona & Catalonia Startup Hub startups were set up within the past five years, 1,021 startups were set up between 2016 and 2021, and 271 within the past two years (2020-2021) as seen on the figure 3.4.

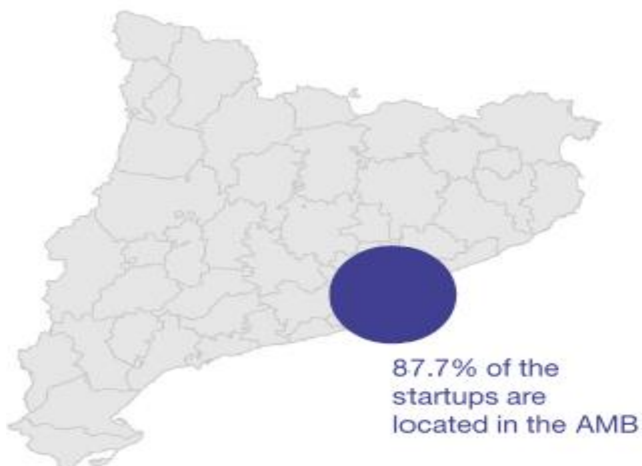
Figure 3.4: Number of startups in Barcelona by age.



Source: Barcelona & Catalonia Startup Hub 2021, ACCIÓ. The diagram was created using data from the 1.844 startups that had indicated the date when the company was established (less than 10 years ago), and 99 of the startups were set up in 2021.

Based on the Barcelona & Catalonia Startup Hub report (Strategic and Competitive Intelligence Unit ACCIÓ, 2021) 87.7% of the startups are located in the Metropolitan Area of Barcelona (AMB), and the district with most startups is Barcelona (68.2%), followed by Vallès Occidental (10%) and Baix Llobregat (6.3%) as seen on the figure 3.5 and 3.6.

Figure 3.5: Startups located in the AMB.




Source: Barcelona & Catalonia Startup Hub 2021, ACCIÓ.

Figure 3.6: Startups located in the AMB

| Comarca | Nº Startups | % |
|---|---|---|
| Barcelonès | 1.277 | 68,3% |
| Vallès Occidental | 187 | 10,0% |
| Baix Llobregat | 118 | 6,3% |
| Maresme | 58 | 3,1% |
| Vallès Oriental | 33 | 1,8% |
| Gironès | 28 | 1,5% |
| Segrià | 28 | 1,5% |
| Bages | 20 | 1,1% |
| Tarragonès | 19 | 1,0% |
| Osona | 16 | 0,9% |
| Anoia | 15 | 0,8% |
| Baix Camp | 13 | 0,7% |
| Garraf | 11 | 0,6% |
| Alt Penedès | 7 | 0,4% |
| Baix Empordà | 7 | 0,4% |
| Selva | 5 | 0,3% |
| Alt Empordà | 4 | 0,2% |
| Pla de l'Estany | 4 | 0,2% |
| Alt Camp | 3 | 0,2% |
| Baix Ebre | 3 | 0,2% |
| Garrotxa | 3 | 0,2% |
| Montsià | 2 | 0,1% |
| Terra Alta | 2 | 0,1% |
| Urgell | 2 | 0,1% |
| Garrigues | 2 | 0,1% |
| Moianès | 1 | 0,1% |
| Pla d'Urgell | 1 | 0,1% |
| Ribera d'Ebre | 1 | 0,1% |
| Solsonès | 1 | 0,1% |
| **TOTAL** | 1.871 | |

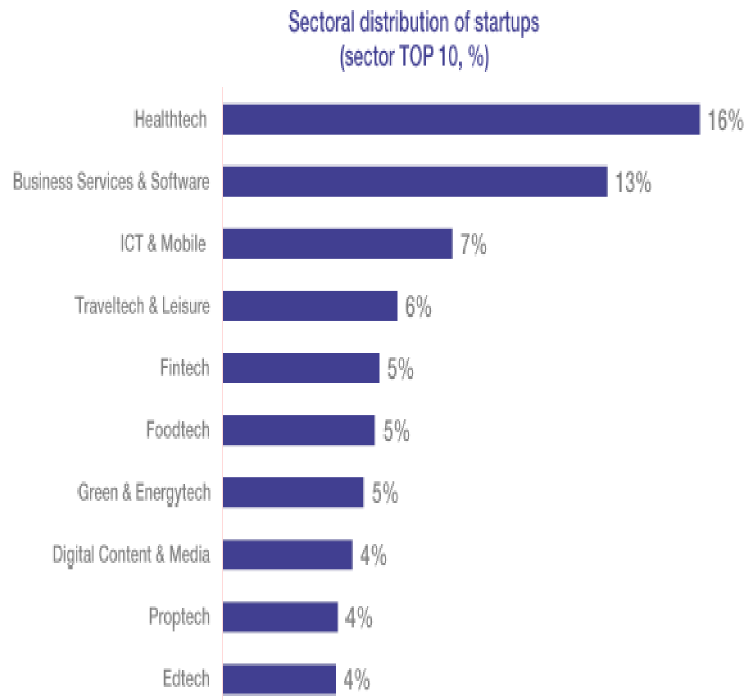
| Region | Region | Nº Startups | % |
|---|---|---|---|
| Barcelonès | Barcelona | 1277 | 68,3% |
| Vallès Occidental | Vallès Western | 187 | 10,0% |
| Baix Llobregat | Baix Llobregat | 118 | 6,3% |
| Maresme | Maresme | 58 | 3,1% |
| Vallès Oriental | Vallès Oriental | 33 | 1,8% |
| Gironès | Gironès | 28 | 1,5% |
| Segrià | Segrià | 28 | 1,5% |
| Bages | Bages | 20 | 1,1% |
| Tarragonès | Tarragonès | 19 | 1,0% |
| Osona | Osona | 16 | 0,9% |
| Anoia | Anoia | 15 | 0,8% |
| Baix Camp | Baix Camp | 13 | 0,7% |
| Garraf | Carafe | 11 | 0,6% |
| Alt Penedès | Alt Penedès | 7 | 0,4% |
| Baix Empordà | Baix Empordà | 7 | 0,4% |
| Selva | Selva | 5 | 0,3% |
| Alt Empordà | Alt Empordà | 4 | 0,2% |
| Pla de l'Estany | Pla de l'Estany | 4 | 0,2% |
| Alt Camp | Alt Camp | 3 | 0,2% |
| Baix Ebre | Baix Ebre | 3 | 0,2% |
| Garrotxa | Garrotxa | 3 | 0,2% |
| Montsià | Montsià | 2 | 0,1% |
| Terra Alta | Terra Alta | 2 | 0,1% |
| Urgell | Urgell | 2 | 0,1% |
| Garrigues | Garrigues | 2 | 0,1% |
| Moianès | Moianès | 1 | 0,1% |
| Pla d'Urgell | Pla d'Urgell | 1 | 0,1% |
| Ribera d'Ebre | Ribera d'Ebre | 1 | 0,1% |
| Solsonès | Solsonès | 1 | 0,1% |
| | **TOTAL** | **1.871** | |

Source: Barcelona & Catalonia Startup Hub 2021, ACCIÓ. Figure 3.5 was created using data from the 1.871 startups with location data. The Metropolitan Area of Barcelona includes 36 municipalities in the districts of Barcelona, Baix Llobregat, Vallès Occidental and Maresme.

Based on the Barcelona & Catalonia Startup Hub analysis (Strategic and Competitive Intelligence Unit ACCIÓ, 2021) the health, business services, ICT and Mobile and leisure sectors account for 42% of startups as seen on the figure 3.7.

Figure 3.7: Sectoral distribution of startups.

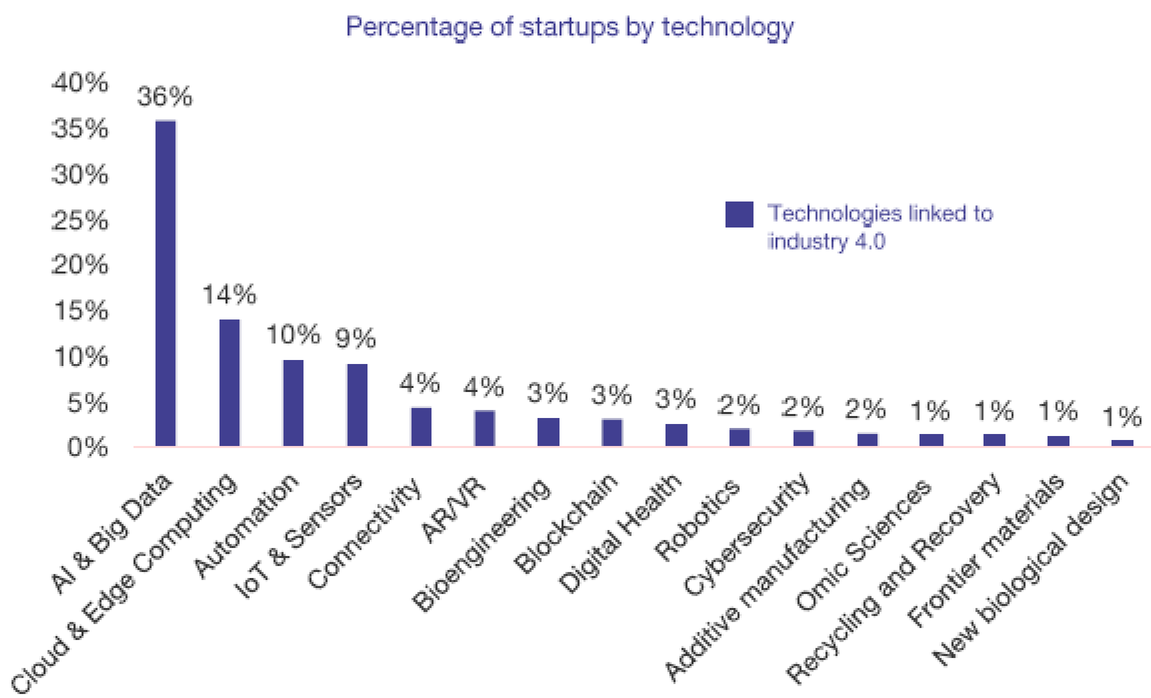
| Sector | Nº Startups |
|---|---|
| Healthtech | 295 |
| Business Services & Software | 238 |
| ICT & Mobile | 142 |
| Traveltech & Leisure | 108 |
| Fintech | 97 |
| Foodtech | 94 |
| Green & Energytech | 87 |
| Digital Content & Media | 80 |
| Proptech | 71 |
| Edtech | 70 |
| Fashion & Design | 68 |
| Ecommerce | 66 |
| Adtech | 65 |
| Sports | 64 |
| Sustainable mobility | 62 |
| Hardware | 61 |
| Community & Social network | 53 |
| Gaming | 49 |
| Logistic Tech | 48 |
| Legaltech | 32 |
| Agritech | 26 |
| Beauty & personal care | 26 |
| **TOTAL** | **1.902** |




Source: Barcelona & Catalonia Startup Hub 2021, ACCIÓ. This figure was created by ACCIÓ using data from the 1,902 startups from the directory with this information available. The analysis was performed using the main sector of each company.

Based on the Barcelona & Catalonia Startup Hub report (Strategic and Competitive Intelligence Unit ACCIÓ, 2021) technologies 4.0 are predominant in startups. Indusry 4.0 includes artificial intelligence and Big Data, automation, cloud, loT and sensors, virtual reality and augmented reality, robotics, frontier materials, connectivity, blockchain, cybersecurity, photonics and quantum sciences, and digital simulation/twins. Based on the Barcelona & Catalonia Startup Hub analysis (Strategic and Competitive Intelligence Unit ACCIÓ, 2021) 86.8% of the startups work with technologies linked to industry 4.0. More particularly, 36% of startups use Artificial Intelligence and Big Data as their primary technology as seen on the figure 3.8.

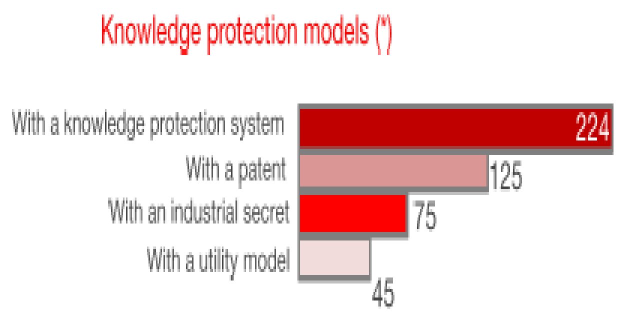
Figure 3.8: Percentage of startups by technology.

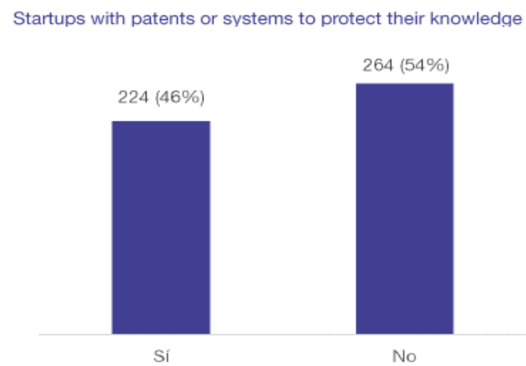



Source: Barcelona & Catalonia Startup Hub 2021, ACCIÓ. This figure was created by ACCIÓ using data from the 1,844 startups of the Barcelona & Catalonia Startup Hub with this information available. The analysis was performed using the main technology of each company.

Based on the Barcelona & Catalonia Startup Hub report (Strategic and Competitive Intelligence Unit ACCIÓ, 2021) 46% of the startups indicate that they have patent or system to protect their knowledge and of the 224 companies with knowledge protection systems, 125 (56%) have at least one patent, 75 (33%) have an industrial secret, and 45 (20%) have a utility model. However, some of those companies may have more than one knowledge protection system as seen on the figure 3.9.

Figure 3.9: Knowledge protection system

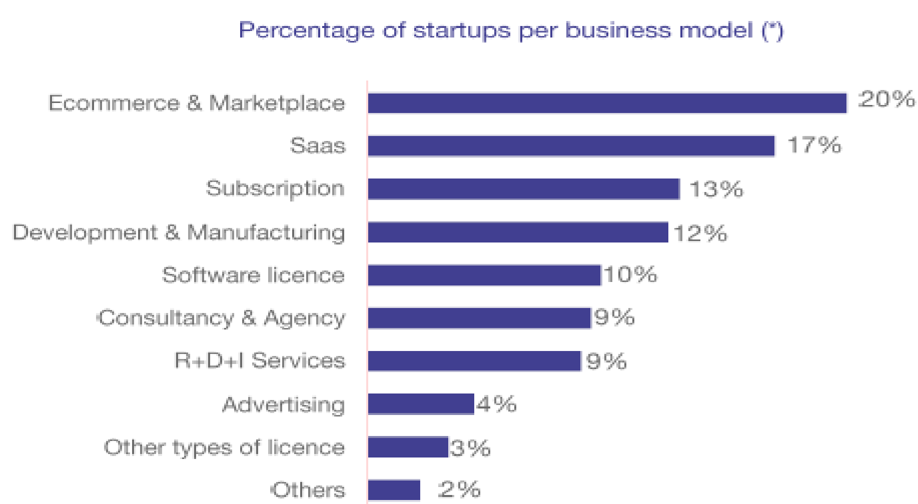



Source: Barcelona & Catalonia Startup Hub 2021, ACCIÓ. This figure was created using the data available from 488 companies answering the question in the 2021 survey.

Ecommerce & Marketplace and Software as a Service (SaaS) are the predominant business models among startups. Both account for 37% of the business models indicated by the startups. Although, startups can have more than one business model, subscriptions account for 13%: product development for 12%, and software licences for 10% as seen on the figure 3.10.

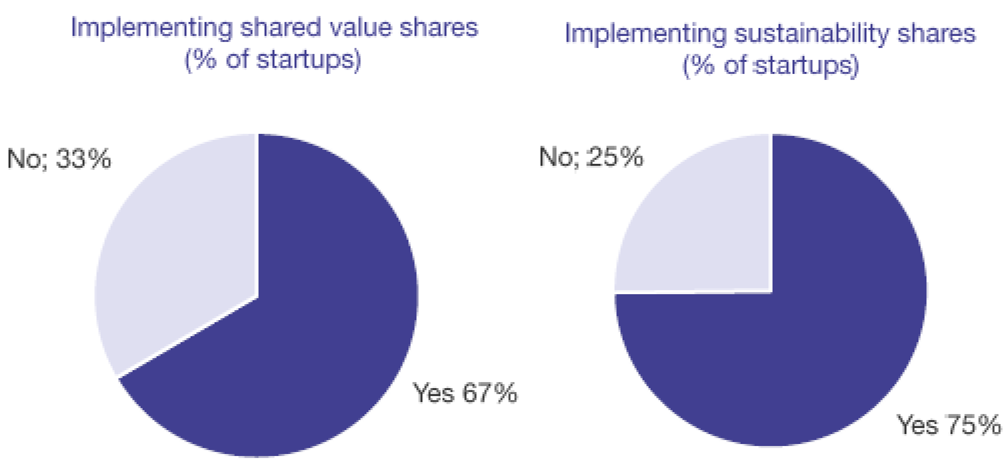
Figure 3.10: Percentage of startups per business model.



Source: Barcelona & Catalonia Startup Hub 2021, ACCIÓ. This figure was created using the data available from 1.902 startups and the companies chose the business models they are applying being more than one if necessary.

In terms of shared valued and sustainability models, 67% of the startups indicate that they promote action to prioritise shared value and 75% have initiatives implemented to improve the sustainability of their business. Being shared value considered as the set of practices that improve the competitiveness of a business while helping improve the economic and social conditions of the community in which it operates as seen on the figure 3.11.

Figure 3.11: Startups implementing shared value and sustainability.




Source: Barcelona & Catalonia Startup Hub 2021, ACCIÓ. The data was taken from 579 companies answering the 2021 survey.

## 3.5. The GDPR implementation challenges faced by technological startups in Catalonia

In order to confirm the researcher's observations and support the research questions of the study about GDPR challenges, the researcher decided to conduct face-to-face interviews with the representatives of several startups in Barcelona. The interviews were scheduled with three companies to find out how they perceive and are familiar with the GDPR and whether they have faced any challenges resulting from the enforcement of the GDPR as of May 2018. The qualitative data were collected utilizing semi-structured interviews, which were advantageous in verifying what was already known and uncovering recent themes by permitting respondents to express their ideas in their own words (Flick, 2022). In addition, one-to-one interviews offer a chance to gain in-depth knowledge of individual GDPR awareness and implementation challenges (McAdam & Galloway, 2005). Furthermore, it gives respondents a chance to pose queries to the interviewer to clarify a particular point or provide original ideas on the topic, generating a semi-structured interview that stimulates two-way communication (Creswel, 2009). In addition, open-ended sequential questions were adopted to guide the interviews. Each interview lasted about half an hour, and after each interview, the interviewer's notes and respondent's responses were reviewed for analysis.

Regarding the startups and the interviewed profile data was gathered concerning the company’s month and year of establishment, the role in the company of the person interviewed, the person responsible for GDPR compliance in the company, the time it took them to achieve compliance, the highest GDPR compliance costs for the company and their annual expenditure for being GDPR compliant.

*Startup 1* was created in November 2015 with more than 10 persons employed in specialisation eCommerce B2B. The role in the company of the person interviewed is responsible for the I.T. department and holds an I.T. professional degree. The person responsible for GDPR compliance in their company is a third-party consultant. It took them 4 to 6 months to achieve GDPR compliance. The highest GDPR compliance costs for the company are associated with introducing new policies and processes. They are spending less than €5000 on an annual basis for being GDPR compliant.

*Startup 2* was created in 2017 with more than 10 persons employed in the specialisation Biotech. The role in the company of the person interviewed is responsible for the administrative operations being the intermediate person working together with an external DPO and holds a master's degree in business administration. The person responsible for GDPR compliance in their company is an external lawyer who is also a DPO. It took them 13 to 18 months to achieve GDPR compliance. The highest GDPR compliance costs for the company are associated with monitoring compliance and having to recruit one person, spending less than €5000 on an annual basis for being GDPR compliant.

*Startup 3* was created in March 2019 with 15 persons employed in specialisation Smart Logistics (B2B). The role in the company of the person interviewed is the founder and holds a master's degree in business administration. The person responsible for GDPR compliance in their company is an external DPO. They have started but have not yet reached GDPR compliance. The highest GDPR compliance costs for the company are associated with compliance certification. They are spending less than €5000 on an annual basis for being GDPR compliant.

The following four opened main questions were asked of each of the startups:

- Question 1: Have there been any challenges for the company regarding GDPR compliance costs?
- Question 2: Have there been any challenges for the company regarding the complexity of the GDPR?
- Question 3: Have there been any challenges for the company regarding government support concerning compliance with the GDPR?
- Question 4: Have there been any challenges for the company to adapt company processes to comply with the GDPR?

Concerning Question 1 startups 1 and 3, when asked, stated, "(…) GDPR is expensive to comply with, and it is costly to invest in GDPR consultants (…). Startup 1 "I am the CTO; we spent many hours during the previous one and a half months before GDPR came into force, informing employees and clients and other stakeholders, the whole company was affected. There was an internal cost because I am the CTO. I was very busy with the GDPR implementation and an external cost because we had to contract the services of a specialised law firm". Startup 2, when asked, stated "(..) it is costly to invest in GDPR consultants, to invest in new hires to meet the demands of GDPR (…). We had to hire a DPO lawyer. We are spending much time and significant financial resources to be GDPR compliant. We got the ISO certification last year, which is part of

GDPR compliance". Startup 3 "I am the founder and the DPO because we cannot pay one, and it is scary. (…) The cost can also be expressed in the activities that we cannot carry out, such as easily acquiring contact data which is extremely necessary for a startup like ours to grow."

About Question 2 startup 1, when asked, stated, "(…) GDPR is complex and difficult to understand (…). It is a regulation, and legal terminology is difficult to understand, even if I belong to the technological area. We created informative documents in plain language to understand and comply with GDPR. By default, when an employee has an issue or a query related to GDPR directly, most of the time I cannot answer since I am not a lawyer, and I think this happens in many companies. I am registered as the DPO for the company. Still, since I am not a lawyer, we have contracted the services of a specialised law firm". Startup 2, when asked, stated, "our company had difficulties understanding and interpreting GDPR. I read the GDPR, and it is not easy to understand. That is why I work piece by piece with our DPO. GDPR is complex for one person and then passed on to the clients, employees, and service providers. It is challenging to train existing employees about GDPR requirements. It was difficult to change the company mindset to ensure that each employee follows GDPR principles (…) that is why we invested in a DPO lawyer. Startup 3, when asked, stated, "(…) GDPR is complex and difficult to understand, it lacks precision and clarity (…). Our company had difficulties with understanding and interpreting GDPR (…)."

Concerning Question 3, startups 1 and 2, when asked, stated that was not a challenge for them. Startup 1 "(..) I have no direct experience; we were presented with the necessity to comply with GDPR, and I found the way by contacting a specialised law firm. I am sure that the government bodies have done thousands of things. Still, I am not aware of them.". Startup 2 "(…) our company forms part of the incubator of Barcelona Activa, I believe. Still, I am not sure that we received support from Barcelona Activa since; also, we receive public funding from Spain and the European Union.". Startup 3, when asked, stated, "(…) there is a lack of information support from the government bodies about GDPR (…). GDPR does not provide any recommendations regarding the use of technology helping to comply with its requirements (…). GDPR does not provide specific instruments or tools for companies (…). There is a risk of being accountable when there are not clear GDPR guidelines to follow (…). Government fines for GDPR incompliance are too high (…). We are growing, and most clients prefer that the data is processed within their servers. Still, it will come a day as it happened to us one month after we started our activity back in April 2019 that we are about to sign an important contract with a new client. They asked us for the GDPR compliance certificate, which we do not have because it costs much money; although we do not know how much, we do not have the money (..). It will be interesting to receive some help from the governmental institutions to provide us with professionals who can help us process and obtain the GDPR certification. We get free help for the basic stages and pay a symbolic amount for the more advanced stage to obtain the GDPR certification. Nevertheless, now we need to go to a lawyer or expert, which costs lots of money. Also, a guide of best practices on what is allowed and not allowed will help. I believe that GDPR is made for large companies and not for small ones. The language of the GDPR seems to be a bit disconnected from the startup adhere an explanation more customised for the dynamic of sales and marketing will be interesting."

Concerning Question 4 startup 1, when asked, he stated, "(…) we cannot have a person performing the processing if a data subject opts out of automated processing. (…) it is not easy to develop a cyber incident response plan. However, we have not had to make important technological changes. Still, to define a series of internal processes, if somebody asks for their data, how to find it and how to deliver it within the required 24 hours, we received some requests just a few days after the GDPR came into force. It worked well". Startup 2, when asked, stated, "(…) it was challenging to adapt the company's existing business model to ensure successful GDPR compliance. (…) it is not easy to know where all the personal data of our stakeholders is stored. (…) it is challenging to apply emergent technologies to better comply with the GDPR". Startup 3, when asked, stated, "(…) it is hard to ensure portability of personal data".

Startups 2 and 3 agree that it is challenging to respond to data enquiries within a 30-day obligation period. "(…) it is challenging to provide our stakeholders (customers, employees, suppliers, government, etc.) with access to personal data. (…) it is not easy to establish a straightforward procedure to delete an individual's data. (…) it is challenging to process growing data quickly."

The three startups agree that it is complex to execute periodic audits to ensure that all processes are compliant with GDPR.

These interviews support a need for deeper study of the challenges faced by the technological startups in Catalonia resulting from the enforcement of the GDPR on the 18th of May 2018. In terms of government support to the startups in Catalonia, Barcelona Activa and ACCIÓ have provided some master classes on the impact of GDPR around the time of the regulation coming into force. Although there are no specific web-published Catalan official reports on the challenges faced by the technology startups, there are reports on artificial intelligence (A.I.) published by the Catalan Data Protection Authority since Catalonia is a major driving force in technological development, but do not consider the GDPR challenges faced by the technology startups (Catalan Data Protection Authority, 2020). The Catalan data protection authority has launched a specific project, based on the work it has carried out in recent years in the field of ethics and data protection to identify how A.I. is used in Catalonia and how the ethical aspect is built into these attitudes. The Catalan Data Protection Authority wants to contribute to the elaboration of the principles governing the design, development and use of A.I. (Catalan Data Protection Authority, 2020).

ACCIÓ & Generalitat de Catalunya (2020) published cybersecurity in Catalonia technology report on the constantly growing of the cybersecurity industry in Catalonia, the relevance of the sector, the increased number of SMEs and startups in the sector, the necessity of more experts with approximately 4000 jobs to be filled and the creation of the Center for Cybersecurity Research of Catalonia (Cybercat) which mission is to promote cybersecurity and privacy research in the information in Catalonia and strengthen its international projection, as well as how to strengthen and extend high-level training in this field and consolidate the existing research relationships between the six universities participating. However, nothing can be found on Catalan startup challenges to comply with the GDPR, such as the difficulty of developing a cyber incident response plan or meeting the costs on GDPR certifications.

Cordero (2021) in his research provides a holistic overview of the primary standards that affect privacy and data protection, especially those that derive from the international reference standard ISO/IEC 27000 (series), in particular ISO/IEC 27001 (information security) and 27701 (privacy information management). Cordero (2021) considers that the company costs for these certifications for effective compliance of the GDPR can compromise the viability of these standards, especially for small companies or with more limited resources. That is why the national DPAs should promote new schemes of medium-term certification to ensure maximum protection with data legislation.

## 3.6. Summary

In this chapter, we have analyzed and discussed the existing definitions of a startup, the statistics on the digital economy in Catalonia, the positioning of Catalonia and Barcelona, the main features of the startup in Catalonia, and with the semi-structured interviews of three Barcelona tech startups to identify the GDPR implementation challenges faced by technological startups in Catalonia. Three main implications can be drawn from this review. Firstly, for researchers interested in Catalan or Spanish startups, this chapter presents the two definitions of startup: the one that applies now that the Startup Law has been enforced and the ACCIÓ definition of a startup as the criteria used for the startups forming part of the startup directory. Secondly, for researchers interested in GDPR challenges in Catalonia or the rest of Spain, this chapter presents Catalonia as one of Europe's largest ICT hubs and the leader destination for IED technology being Barcelona the 7$^{th}$ E.U. startup hub in future unicorns behind Paris, Berlin, Stockholm, Munich, Dublin, and Amsterdam and ahead of Madrid. Technologies 4.0 are predominant in the Catalonian startups with 75% that have implemented initiatives to improve the sustainability of their business. Thirdly, for researchers interested in GDPR challenges, this chapter presents the findings of the interviews on the GDPR challenges faced by three technological startups. Therefore, the knowledge derived from business could serve useful for the governments to take measures to support organizations with challenges of implementing GDPR. Secondly, by identifying challenges, the organizations will be careful to avoid mistakes and pitfalls throughout the process of GDPR implementation.

# Chapter 4 Research methodology

## 4.1. Introduction

To carry out research within the allotted period and resources, it is essential to examine certain research techniques or methods to associate, select, handle, and assess data about a suggested investigation theme. This chapter covers formulating a relevant research method to attain the investigation goals and answer the research questions. In addition, the chapter describes the proposed research philosophy, research design, research approach, strategy, and methods selected for this proposed research, and the rationale behind selecting these methods. Additionally, the chapter examines the data collection technique and the preliminary data testing for the quantitative study. Finally, this chapter concentrates on the "what" and "why" of the methods and techniques selected, as well as information on “how” the research techniques and methods used.

## 4.2. Research design

This section aims to illustrate the general research design and philosophical approach. For example, Crotty (1998) stated that researchers should be able to come up with a credible design to explain their results. Likewise, Saunders, Lewis and Thornhill (2019, p.130) noted that a “well-thought-out and consistent set of assumptions will constitute a credible research philosophy, underpin your methodological choice, research strategy, data collection techniques, and analysis procedures".

The “research onion” served as a frame of reference. First developed by Saunders et al. (2016), it provides a familiar framework that numerous researchers have adopted to illustrate philosophical assumptions and the underlying problems surrounding their data collection and analysis decisions, as shown in Appendix A.

### 4.2.1. Research choice

The third layer of the research onion affects the selection of a study type from the qualitative, quantitative, or mixed methods. Saunders et al. (2016, p. 177) defines the research strategy as an action plan how the researcher will answer his research question. The selected research choice for this study is the quantitative research while a questionnaire is designed and used to obtain responses to explore the relationship between variables to be measured numerically and analysed using a range of statistical and graphical techniques Saunders et al. (2016, p. 178).

### 4.2.2. Research strategy

The fourth layer of the research onion concerns the selection of one or more strategies within their research design as part of the planning process for how the researcher will answer or approach a research question (Saunders et al., 2019). Saunders et al. (2019) defined the research as a variety of possible approaches that have evolved. Table 4.1 shows some alternative research strategies used by Saunders et al. (2019) to better understand the possible strategies.

Table 4.1: Alternative research strategies (Saunders et al., 2019)

| **Research strategy** | **Observations about the individual research strategies – based on the list in (Saunders et al., 2019)** |
|---|---|
| Experiment | It has its roots in "natural science". The purpose is "to study the probability of change in an independent variable causing a change in another, dependant variable" Saunders et al. (2019, p. 190). |
| Survey | The intention is to answer “what, who, where how much and how many questions”. Easy to administer to a high number of people and can be “analysed with descriptive and inferential statistics” and is usually done anonymously with a limited number of questions. Questions need to be carefully thought out as there is no second chance to query the results (Saunders et al. (2019, p. 193). |
| Archival and documentary research | Uses many online sources and databases. In addition, there is a range of possible sources referred to as secondary data. Extra care needs to be taken as the documents were not specifically developed for the research. Some documents may also miss or omit certain relevant data Saunders et al. (2019, p. 196). |
| Case study | It is an in-depth study of a subject or phenomenon in its real-world setting Yin (2017). Understanding the perspective is fundamental to case study research (Saunders et al., 2019). It may be used not only for exploratory but also for descriptive and explanatory purposes Yin (2017). It can involve single or multiple case studies (Saunders et al., 2019). Can generate “rich, empirical descriptions and the development of a theory” Yin (2017). |
| Ethnography | “Used to study the culture or social world of a group” Saunders et al. (2019, p. 199) with its origins in colonial anthropology. A set of ethnographic approaches of which Cunliffe (2010) outlines three: realist, impressionist or interpretive and crucial ethnography (Saunders et al., 2019). “Relevant for modern organisations such as market research”. “Requires to build trust in the field if working with people.” Saunders et al. (2019, p. 201). |
| Action research | “It is an emergent and iterative process of enquiry”. It encourages organisational learning to achieve practical results by identifying problems, planning and evaluating actions. It starts within a specific context and with a research question which focuses may change as the research develops.” Saunders et al. (2019, p. 202). |
| Grounded | “Developed by Glaser and Strauss (1967) as response to the extreme positivism”. “Uses an abductive approach, moving between induction and deduction ” “Researchers collect and |

| | |
|---|---|
| | analyses data simultaneously using coding, comparison and self-memos before collecting more data" Saunders et al. (2019, p. 206). |
| Narrative enquiry | Participants were invited to provide a complete narrative of their experience. "Seeks to preserve chronological connections and the sequencing of events". "When there is more than one participant providing a personal account of a given context, the narrative researcher will also be able to compare and triangulate" Saunders et al. (2019, p. 209). |

**Survey research.** Surveys were preferred for the quantitative deductive determinants of the research, as they allow to gather primary data that can be analysed and based on which conclusions can be drawn on the main challenges of the implementation of the GDPR for technology startups in Catalonia if the challenges are associated with compliance costs, regulatory complexity, insufficient government support or process adaptation if there is correlation between the challenges and the year of establishment, the size, the business sector, and the annual expenditure for GDPR compliance and the level of knowledge of the GDPR representatives of startups.

### 4.2.3. Research time horizon

"The final layer of the research onion, before reaching the core, highlights the time horizon over which the researcher undertakes the research" Saunders & Tosey (2013, p. 59). Where the research is undertaken to answer a question or address a problem at a particular time, this "snapshot" is cross-sectional Saunders et al. (2019, p. 212) or longitudinal "when the researcher when answering the question or addressing the problem requires data being collected for an extended period of time" to "observe changes over a long period of time" (Saunders & Tosey, 2013, p. 59) the "diary" perspective (Saunders et al. 2019, p. 212).

The researcher related to Saunders et al., (2019, p. 212), who suggested that "cross-sectional studies involve the study of a particular phenomenon at a particular time and that often employ the survey strategy". Since the research is undertaken to answer three research questions at a particular time from May 2021 to November 2021 and by employing a survey strategy, this research is cross-sectional.

## 4.3. Research questions and hypothesis development

Using a conceptual framework created with the help of the literature research that identified the challenges faced by companies resulting from the GDPR implementation, this study focused on exploring the challenges faced by technology startups in Catalonia resulting from the enforcement of the GDPR on the 18th of May 2018.

In relation to **RQ 2:** What are the key challenges of the GDPR implementation faced by technology startups in Catalonia?

> **RQ 2.1:** Are the key challenges associated with compliance costs, regulation complexity, insufficient government support or process adaptation?
>
> **RQ 2.2:** Is there any relationship between the challenges faced by technology startups and the number and type of employees recruited, size, business sector, year of establishment; as well as GDPR annual spending and time to achieve compliance?

Research question 2.1. will be answered with the descriptive statistical analysis of the four constructs mean and standard deviation.

The corresponding hypotheses for research question 2.2 are:

***Hypothesis 1:***

$H_o1$: There is no significant relationship between the number of new employees recruited to facilitate GDPR compliance versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years of startup established.

$H_{A1}$: There is significant relationship between the number of new employees recruited to facilitate GDPR compliance versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years of startup established.

***Hypothesis 2:***

$H_{o1}$: There is no significant relationship between responsible for GDPR compliance in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years startup established.

$H_{A1}$: There is significant relationship between responsible for GDPR compliance in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years startup established.

***Hypothesis 3:***

$H_{o1}$: There is no significant relationship between total number of employees in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and number of years startup established.

$H_{A1}$: There is significant relationship between total number of employees in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and number of years startup established.

***Hypothesis 4:***

$H_{o1}$: There is no significant relationship between startup business sector versus compliance costs, staff training, regulation complexity and process adaptation.

$H_{A1}$: There is significant relationship between startup business sector versus compliance costs, staff training, regulation complexity and process adaptation.

***Hypothesis 5:***

$H_{o1}$: There is no significant relationship between startup business sector versus GDPR annual spending and months to achieve compliance.

$H_{A1}$: There is significant relationship between startup business sector versus GDPR annual spending and months to achieve compliance.

***Hypothesis 6:***

$H_{o1}$: There is no significant relationship between respondent’s role in a start-up versus compliance costs, staff training, regulation complexity and process adaptation.

$H_{A1}$: There is significant relationship between respondent’s role in a start-up versus compliance costs, staff training, regulation complexity and process adaptation.

***Hypothesis 7:***

$H_{o1}$: There is no significant relationship between respondent’s level of education versus compliance costs, staff training, regulation complexity and process adaptation.

$H_{A1}$: There is significant relationship between respondent’s level of education versus compliance costs, staff training, regulation complexity and process adaptation.

***Hypothesis 8:***

$H_{o1}$: There is no significant relationship between respondent's field of education versus compliance costs, staff training, regulation complexity and process adaptation.

$H_{A1}$: There is significant relationship between respondent's field of education versus compliance costs, staff training, regulation complexity and process adaptation.

***Hypothesis 9:***

$H_{o1}$: There is no significant difference between males and females in their perceptions of GDPR compliance costs, staff training, regulation complexity and process adaptation.

$H_{A1}$: There is significant difference between males and females in their perceptions of GDPR compliance costs, staff training, regulation complexity and process adaptation.

***Hypothesis 10:***

$H_{o1}$: Compliance costs are not affected by staff training, regulation complexity and process adaptation.

$H_{A1}$: Compliance costs are affected by staff training, regulation complexity and process adaptation.

***Hypothesis 11:***

$H_{o1}$: Staff training is not affected by regulation complexity and process adaptation.

$H_{A1}$: Staff training is affected by regulation complexity and process adaptation.

***Hypothesis 12:***

$H_{o1}$: Process adaptation is not affected by staff training, regulation complexity and GDPR annual spending.

$H_{A1}$: Process adaptation is affected by staff training, regulation complexity and GDPR annual spending.

***Hypothesis 13:***

$H_{o1}$: Months to achieve compliance are not affected by staff training, process adaptation, compliance costs and year company established.

$H_{A1}$: Months to achieve compliance are affected by staff training, process adaptation, compliance costs and year company established.

## 4.4. Quantitative methodology and approval

This section explains the method used to tackle the research objective from Chapter 1: to identify the key challenges faced by technology startups in Catalonia resulting from the enforcement of the GDPR as of May 2018, to provide recommendations to help to increase technology startup's awareness in Catalonia to address and overcome the challenges to comply with GDPR and for the Catalan government to take measures to support technology startups with challenges of implementing GDPR.

### 4.4.1. The nature and logic of the selected approach

The section summarizes the quantitative approach, which used the 'GDPR Challenges' questionnaire to analyze the level of understanding of GDPR by the startup representatives and identify the challenges faced by technology startups in Catalonia resulting from the enforcement of the GDPR in May 2018.

Concerning quantitative research, Saunders et al. (2019, p. 178) noted that it "examines relationships between variables, measured numerically and analysed using a range of statistical and graphical techniques". The techniques include "true experiments and the less rigorous experiments called quasi-experiments" (Creswell, 2014, p.12).

Commonly a quantitative approach is linked with a deductive approach and positivist philosophy. This was consistent with the researcher's pragmatic philosophical approach using a quantitative method. The objective was to include statistical analysis and inferential analysis. As the aim of the research was to collect information to identify the key challenges faced by technology startups in Catalonia resulting from the enforcement of the GDPR as of May 2018, the association of these key challenges with compliance costs, regulation complexity, insufficient government support or process adaptation, the existence or not of a relationship between the challenges and the year of establishment, size, business sector, and annual expenditures on GDPR compliance and the level of GDPR knowledge of the startup's representatives, a questionnaire approach was considered more suitable. This aligned with Saunders et al. (2019, p. 504), who observed that "the questionnaire is one of the most widely used data collection techniques within the survey strategy". They added that it "provides an efficient way of collecting responses from a large sample prior to quantitative analysis” Saunders et al. (2019, p. 212). Fowler (2013) proposed that the principal goal consists of collecting data that can be utilized to provide numerical descriptions and perform statistical analysis on specific aspects of the study population. Creswell (2014, p. 157) agreed, noting that researchers can "generalise from a sample to a population so that inferences can be made about some characteristic, attitude or behaviour of this population". The approach would support the research goal of identifying quantitative GDPR challenges from the target population (technology companies in Catalonia) and to enable the collection of data to test hypotheses to determine if there are important associations. The next stage was the design of the questionnaire.

### 4.4.2. Questionnaire design

This section describes the approach used to define the questionnaire aims and objectives, the population and sampling frame, to design the questionnaire by developing the questions for the constructs, to deal with the questionnaire administration and ethics and the management and validation of questionnaire data.

#### 4.4.2.1. Defining the questionnaire aims and objectives

The ‘*GDPR Challenges* questionnaire was a cross-sectional (i.e. timely) approach to gather a wide range of opinions from technology startups professionals to identify:

- The key challenges faced by the technology startups in Catalonia resulting from the enforcement of the GDPR,

- If the key challenges are associated with compliance costs, regulation complexity, insufficient government support or process adaptation,

- If there is any relationship between the challenges faced by technology startups and the year of establishment, size, business sector, and annual expenditures on GDPR compliance.

- the level of GDPR knowledge of the startup’s representatives.

The goal was to collect information to allow both descriptive and inferential statistical analysis to generalise and draw conclusions from the sample to help identify a range of quantitative GDPR implementation challenges to provide recommendations to help to increase technology startups’ awareness in Catalonia to address and overcome the challenges to comply with GDPR and for the Catalan government to support technology startups with challenges of implementing GDPR.

#### 4.4.2.2. Defining the population and sampling frame

Sue & Ritter (2012, p. 2) pointed out the crucial significance of sampling for the research objectives. They proposed that "a good sample is representative of the population from which it is drawn". The 'target population' for the investigation were technology startups in Catalonia. Though, as Field (2009, p. 34) noted, "scientists rarely, if ever have access to every member of a population". Saunders et al. (2019, p. 292) suggested that researchers use a “representative sample” as a ‘census’, i.e. collecting data from all members of the population is not generally feasible. Creswell (2014) described this as ‘clustering’. This is where organisations are identified that have access to individuals within the main population. Sampling then occurs "within those clusters” Creswell (2014, p. 158).

The most logical method to accessing a 'representative sample' of general technology startups in Catalonia consisted of contacting a suitable institutional organisation that could be considered the most representative of the sample sought. As a result, ACCIÓ was selected as being the main Catalan institutional body promoting technology startups in Catalonia.

ACCIÓ administers the Barcelona and Catalonia Startup Hub, including a database of technology companies in Catalonia and its members met the 'selection criteria as a good representation of technology companies in Catalonia. Therefore, ACCIÓ was contacted, and they agreed to provide the raw database of 1703 technology startups listed in their Hub. About calculating the representative sample, the recommendation of Sue and Ritter (2012) was to attain this by measuring the margin of error and confidence level with a 95% confidence level.

Using a 95% confidence level, a margin of error of 5%, a population proportion of 50% and a population size of 1703 startups, the sample size is 314. This means 314 or more measurements/surveys are needed to have a confidence level of 95% that the real value is within ±5% of the measured/surveyed value, as represented in table 4.2.

Table 4.2: Sample size

| | |
|---|---|
| Confidence Level | 95% |
| Margin of Error | 5% |
| Population Proportion | 50% if not sure |
| Population Size | 1703 |
| Sample size | 314 |

### 4.4.2.3. Development of questions

Saunders et al. (2019, p. 361) informed that researchers should "collect the precise data that you require to answer your research question(s)". This approach was taken to ascertain which questions would offer the best data. It was crucial to develop clear and coherent questions, notably given the cross-sectional design that offers only one way of data collection. The main objective was to identify the key challenges faced by technology startups in Catalonia resulting from the enforcement of the GDPR, so questions were evolved using the constructs found in the literature search and the conceptual framework (chapter 2), as shown in table 4.5. To help improve the design, three technology startups from Catalonia were interviewed (chapter 3). As a result, numerous proposed question formats could be tested, and the results incorporated into the development of the research questionnaire. It was considered essential to include questions measuring the understanding of GDPR and the technology sector's perception of the challenges of GDPR implementation.

The researcher is in a position to design the questionnaire after having already carefully reviewed the existing literature, conceptualized this research as shown in table 4.3, discussed with colleagues, professors and supervisors and finally ran three semi-structured interviews with three technology startups in Catalonia registered with the Barcelona and Catalonia Startup Hub for the understanding of the challenges faced resulting from the enforcement of the GDPR.

Table 4.3: Questions for the constructs.

| CONSTRUCT | QUESTIONS | STUDIES TAKEN AS A BASIS |
|---|---|---|
| Compliance costs | GDPR is expensive to comply with | Campbell et al. (2015; Freitas & Mira da Silva (2018), Hurdik (2018), Krasteva et al., 2015, Pedroso et al. (2021); |
| Compliance Costs | The company budget has been significantly increased because of GDPR | |

| | | |
|---|---|---|
| Compliance Costs | It is costly to invest in GDPR consultants | Tikkinen-Piri et al. (2018), TrustArc (2018). |
| Compliance Costs | It is costly to invest in new hires to meet the demands of GDPR | |
| Compliance Costs | We had to acquire new technology solutions to comply with GDPR | |
| Compliance Costs | It was costly to invest in new technology | |
| Compliance Costs | We are spending a lot of time to be GDPR compliant | |
| Regulation Complexity | GDPR is complex and difficult to understand | Freitas & da Silva (2018; Härting, et al. (2020); Presthus & Sønslien (2021). |
| Regulation Complexity | GDPR lacks precision and clarity | |
| Regulation Complexity | Our company had difficulties with understanding and interpreting GDPR | |
| Regulation Complexity | It is difficult to ensure that our providers / suppliers / vendors follow the regulation for personal data protection (GDPR) | |
| Regulation Complexity | It was challenging to train existing employees about GDPR requirements | |
| Regulation Complexity | It is challenging to train new employees about GDPR requirements | |
| Regulation Complexity | It was difficult to change the company mindset to ensure that each employee follows GDPR principles. | |
| Government Support | There is a lack of information support from the government bodies in relation to GDPR. | Cochrane et al.(2020); Hurdik (2018); Norval et al. (2021); Härting et al. (2020) |
| Government Support | There is a lack of practical guidelines from the government bodies to follow standard procedures correctly. | |
| Government Support | GDPR does not provide any recommendations regarding the use of technology helping to comply with its requirements | |
| Government Support | GDPR does not provide any specific instruments or tools for companies | |
| Government Support | There is a risk of being accountable when there are no clear GDPR guidelines to follow. | |
| Government Support | Government fines for GDPR incompliance are too high | |
| Process Adaptation | It was difficult to adapt the existing business model of the company to ensure successful GDPR compliance. | Ahmed et al. (2020), Grundstrom et al. (2019); Mangini et al. (2020); Mansfield-Devine (2016); Politou et al. |

| | | |
|---|---|---|
| Process Adaptation | It is challenging to provide our stakeholders (customers, employees, suppliers, government, etc.) with the access to personal data. | (2018); Poritskiy et al. (2019); Rhahla et al. (2021); Sarkar et al. (2018), Härting et al. (2020) |
| Process Adaptation | It is not easy to establish a clear procedure to delete an individual's data. | |
| Process Adaptation | It is challenging to process growing data in a quick way | |
| Process Adaptation | It is hard to ensure portability of personal data | |
| Process Adaptation | We are not able to have a person performing the processing if a data subject opts out of automated processing. | |
| Process Adaptation | It is not easy to develop a cyber incident response plan | |
| Process Adaptation | It is not easy to know where all the personal data of our stakeholders is stored. | |
| Process Adaptation | It is challenging to respond to data enquiries within a 30-day obligation period. | |
| Process Adaptation | It is challenging to apply emergent technologies (artificial intelligence, robotics, cloud computing, blockchain, etc.) to achieve better compliance with the GDPR. | |
| Process Adaptation | It is complex to execute periodic audits to ensure that all processes are compliant with GDPR. | |

Saunders et al. (2019) suggested inspecting for “validity” and decreasing “social desirability bias”. This required formatting the questions in a way that made it socially acceptable for respondents to say they were unfamiliar with certain subjects. (Saunders et al., 2019) also recommended, "Likert-style rating scales in which the respondent is asked how strongly she or he agrees or disagrees with a statement”. With regard to the analysis phase, the nature of the data, or “scale of measurement” for the questions was taken into account, as suggested by Saunders et al. (2019, p. 567). The big majority of the measurement items are based on a five-point Likert scale ranging of total rejection to full approval (1: Strongly disagree, 2: Disagree, 3: Neither agree nor disagree, 4: Agree, 5: Strongly agree**)**. The respondents will also be provided with answering "Not applicable" and "I don't know" to the Likert scale. Every question must be answered in order to get valid results.

Company and respondent’s profile questions were incorporated to gather background knowledge about companies such as the number of persons employed, area of specialisation of the enterprise (business sector) and about respondents such as the role in the company, gender, highest level of education and study field associated with their highest education for descriptive statistics.

This helped guarantee the correct kind of data was being collected to enable design analysis intent and hypothesis testing. The following data types were taken into account while creating the questions:

• **Descriptive/nominal:** not related with numerical values or ordered in any way (numbers may be related to answer choices but are random and have no inherent significance).

• **Ranked/ordinal data:** can be ranked with a motive behind the rank order. These can be ordered with a figure method, but the spaces between the attributes are not equal.

• **Interval data:** with explainable relative position or distance between values, e.g., role in the company or gender.

The scales used in the study are nominal, ordinal, and interval scales. In the present research, a Likert or ordinal variable with five or more categories will be used as continuous without any harm to the analysis the researcher is planning to use them in. In such cases, researchers typically refer to the variable as an "ordinal approximation of a continuous variable." (Johnson & Creech, 1983; Norman, 2010; Sullivan & Artino, 2013; Zumbo & Zimmerman, 1993)

The question order/layout/look has been completed to ensure a plausible flow from begin to end. The layout has been completed with suitable sections and then sent to an English official translator to have the questionnaire translated into Spanish. Once the questionnaire was officially translated into Spanish, it was introduced in a Google form making all questions mandatory to be answered.

The questionnaire's Spanish official translation is shown in Appendix B and the final format of the English version of the questionnaire is shown in Appendix C.

#### 4.4.2.4. Questionnaire administration and ethics

As recommended by Dillman (2007) and Creswell (2014), a specific introductory text was included to inform potential respondents of the overall purpose of the questionnaire. This described that the survey was conducted as part of the research study carried out on behalf of Geneva Business School, Barcelona, the aim of the study, that the information they provided, and their answers were strictly confidential, that the company identification was needed for statistical purposes in order to keep track of the collected data to avoid contacting them again when they have answered the questionnaire.

The introductory text also included that the study results will be presented in the form of the aggregate data to allow people to choose whether they want to fill out the questionnaire freely. The questionnaire has been configured in Google forms to guarantee that all data is kept confidential and aggregated, so there is no possibility of revealing any individual's identity.

The questionnaire remained open from the 7th of May 2021 to the 29th of November 2021. On the closure of the questionnaire, an excel spreadsheet was created for data analysis.

#### 4.4.2.5. Management and validation of questionnaire data

The first stage in the data validation process was to perform an early study and data cleansing exercise on the Google Forms Excel spreadsheet. All fields have been verified to be completed with valid data entries. Incomplete or incorrectly filled out data have been left out.

The data was then imported into the established Statistical Package for Social Sciences (SPSS) and adopted for data analysis. Another step to ensure the clarity and validity of the data for the analysis phase was to re-code the data in SPSS. This included a manual review of coding labels to guarantee the data for all questions and associated variables were valid. In addition, some of the variables were recorded where needed to guarantee the precision of the categorical data analysis, in which selected variables were tested against each other to determine if there were significant associations between the two variables.

### 4.5. Variables in the study

This section presents the variables used for this study.

### 4.5.1. Scale variables

The following scale variables have been considered to assess to what extent startups respondents perceived them as a key challenge resulting from the enforcement of the GDPR, whether there was a relationship between them and other variables and whether this could lead to large discrepancies in the perceptions of the surveyed startups and what impact each of the scale variables could have in relation to other variables.

**Compliance costs.** This scale variable assessed responses to question items such as is GDPR expensive to comply with, has their company budget increased significantly because of GDPR, was it costly to invest in new hires to meet the demands of GDPR.

**Staff training.** This scale variable assessed responses to question items such as whether it was challenging to train existing and new employees about GDPR requirements and whether it was difficult to change the company mindset to ensure that each employee follows GDPR principles.

**Regulation complexity**. This scale assessed responses to question items such as the complexity and difficulty of understanding GDPR that lacks precision and clarity and whether they had difficulties understanding and interpreting the GDPR.

**Process adaptation.** This scale variable assessed responses to question items such as whether it was easy or not to develop a cyber incident response plan or to apply emergent technologies to achieve better compliance with the GDPR. It also assessed whether it was complex to execute periodic audits to ensure that all processes were compliant with GDPR.

**GDPR annual spending (euros).** This scale variable assessed responses to the startups' respondents' annual expenditure for being GDPR compliant.

**Months to achieve compliance.** This scale variable assessed responses to the startups' respondents on the number of months that the company needed to achieve GDPR compliance.

**Years company was established**. This scale variable assessed responses to the startups' respondents on the number of years in which the company was established.

### 4.5.2. Categorical variables

The following categorical variables have been considered to assess the company and respondent profile with the idea to run advanced statistical tests to examine whether demographic factors such as number of people employed, business sector, role in the company, gender, education, and education field can lead to significant discrepancies in respondents' perceptions on GDPR challenges.

It has also been considered as categorical variables the following:

**Highest GDPR compliance costs**. This categorical variable assessed responses from the startups respondents on what they have spent the most in terms of GDPR compliance. Whether it has been hiring a DPO or new employees accountable for data protection, training employees about GDPR, acquiring new technology solutions, modifying processes, introducing new policies and processes, monitoring compliance, data protection impact assessment (DPIA), risk assessment or other.

**Number of new people recruited for GDPR.** This categorical variable assessed responses from the startups' respondents on the number of new people recruited because of GDPR.

**Responsible for GDPR.** This categorical variable assessed responses from the startups' respondents on who is responsible for GDPR in their company. For example, is it a DPO, a CPO, a third-party consultant, the respondent or other?

**Number of people employed.** This categorical variable assessed responses from the startups' respondents on the number of persons employed by the startup.

**Business sector.** This categorical variable assessed responses from the startups' respondents on their startup area of specialization.

**Respondent's role.** This categorical variable assessed responses from the startups' respondents on their role in the startup.

**Respondent's gender.** This categorical variable assessed responses from the startups' respondent's gender.

**Respondent's education.** This categorical variable assessed responses from the startups' respondent's highest level of education.

**Respondent's study field.** This categorical variable assessed responses from the startups' respondent's study field associated with their highest education.

## 4.6. Data collection

The section outlines the quantitative data collection approach and its limitations.

### 4.6.1. The approach for collecting data

Saunders et al. (2019, p. 506) noted that that data collection for questionnaires/surveys could utilise several approaches, as shown in Figure 4.1.

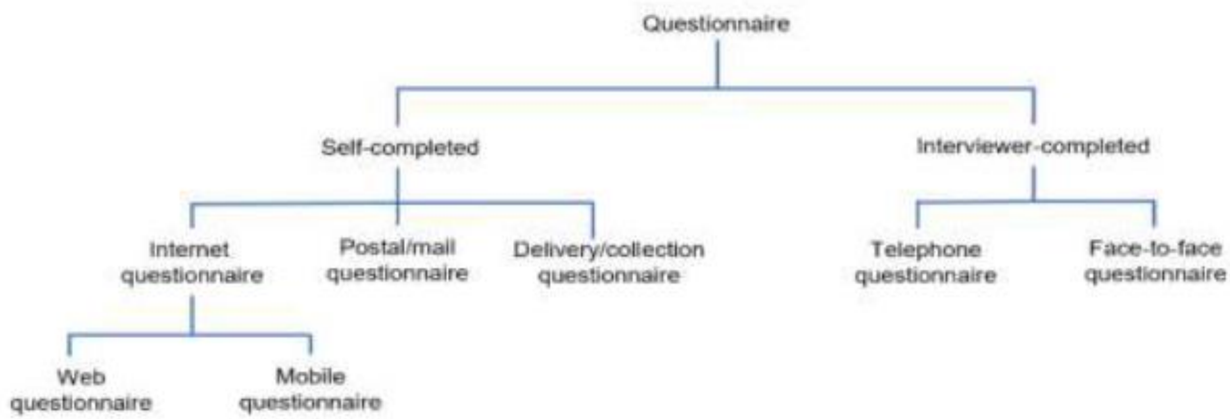



Figure 4.1: Questionnaire modes (Saunders et al., 2019)

The questionnaire will be self-completed and implemented via Google forms. The target group of the questionnaire consists of people who have experience or knowledge of GDPR. People responsible or partly responsible for data protection regulations are managers, directors, members of the board of directors, founder employees, DPOs, CPOs, and IT departments, among others.

The database provided by ACCIÓ did not include the contact person, telephone number and email address. Therefore, with the help of two research colleagues, the next step was to search for the missing contact data and identify the most appropriate and relevant person to be contacted in each startup. Once all the contact data was collected a table of 624 random numbers was produced and duplicate numbers were not allowed. Then this number was multiplied it by two as recommended some scientists when there is a threat of low response rate. Furthermore, since even duplicated sample size did not help and only few responses were collected, it was decided to proceed contacting all 1703 technology startups in Catalonia (the whole population) to intent to achieve the minimum sample size to be representative of the whole population.

The contacts were approached via email on two occasions, acting the second email as a reminder and, if not reaction, then by telephone call. In the email to the potential respondents, the researcher introduced himself and research colleague assistance, the aim of the study, that the information they provided, and their answers were strictly confidential, that the company identification was needed for statistical purposes only and that the results of the study will be presented in the form of aggregate data. The email also included a hyperlink to access the questionnaire in Spanish. The respondent was directed through the multiple question screens utilizing prompts in the software. A submit button was utilized to complete the procedure on the final screen.

The distribution of the questionnaire and collection of responses started on the 7$^{th}$ of May 2021 and finished on the 29$^{th}$ of November 2021.

### 4.6.2. Limitations

As already mentioned, the database provided by ACCIÓ did not include the contact person, telephone number and email address for each startup. Therefore, with the help of two research colleagues, the next step was to search for the missing contact data. However, there was no contact email or telephone number in some cases. Therefore, the researcher personally controlled the data collection by sending emails and reminders. Since only a tiny percentage of startups responded, the researcher started calling all the startups on the database that had published their telephone number. Many of the startups wanted to respond to the questionnaire. However, they did not have the time because of a lack of personnel.

Moreover, a small percentage of the potential respondents had closed their activity, some would not answer their phone, and the researcher would leave a message but not return the call. The Covid 19 pandemic also impacted the startups' ability to concentrate their efforts on applying for funding from government institutions. These limitations have impacted the number of surveys collected, 116 compared to the 314 needed to reach the sample size. Therefore, since the sample size does not represent the population, it is impossible to generalize the finding for all startups in Catalonia and only make inferences about the respondents (survey participants).

## 4.7. Preliminary data testing

The preliminary phase of data analysis involved selecting the most appropriate data analysis strategy to ensure the data was clean for data screening and precoding study responses (Creswel & Creswell, 2017; Creswell, 2009; Morse, 2003). In this study, each factor in the questionnaire was assigned numerical values for the precoding process, and version (23) of the Statistical Analysis Tool and Software Package (SPSS) was used when the study data was downloaded from a Google form in Microsoft Excel format. The data was then transferred to SPSS for additional analysis. In the second step, the cleaning and screening processes examined the study data for normality, data accuracy, missing values in the data and outliers.

### 4.7.1. Data cleaning and screening

Data cleaning and screening were essential steps in this study to ensure that the data analysis process is not negatively impacted by poor data quality, which will impact the study results, e.g. if values are missing or the data was not checked for inconsistencies.

Each factor has been subjected to frequency studies. This resulted in 9 answers from the participants been excluded because of data outliers and some inadequate responses – almost all the answers had the same number- like the respondents just wanted to get rid of the survey. This is one of the phenomena of the data collection limitation which is called acquiescence effect phenomenon (Hinz, et al., 2007). Therefore, 107 complete responses were deemed for further investigation in this study, providing a sufficient set of responses for quantitative research.

### 4.7.2. Missing data analysis

Missing value analysis was conducted in SPSS. The EM method was used to test the null hypothesis that the data are missing fully at random. Since the obtained p value (.478) proved to be insignificant, the null hypothesis was confirmed.

The obtained dataset contained some missing values since the respondents were provided with the option of answering "Not applicable" and "I don't know" on the Likert scale. The “I don’t know” response was treated as “3 - somewhat agree / somewhat disagree” for the study (Denman et al., 2018). Denman et al. (2018) considers the option to record "I don't know" as a neutral midpoint in a Likert response scale.

The "Not applicable" response was treated as system-missing data, avoiding any potential bias or reduction of variability introduced by an imputation procedure (Holman et al., 2004).

### 4.7.3. Data normality

**Normality Tests:** Before the study of the correlations could begin, standard statistical tests were performed to test whether the data were normally distributed or not. The result aided to decide whether to adopt 'parametric' or 'non-parametric' tests for additional analysis. Saunders et al. (2016, p. 533) noted that several standard statistical tests require that the 'dependant variable' is normally distributed for 'each category of the independent variable'. The data were normally distributed (resulting in the classic bell-shaped curve), then parametric tests could be used; if not, nonparametric tests would have to be used.

As noted by (Fisher, 1990), common statistical practice is that an acceptable level of significance is $p < 0.05$, where p means probability. Field (2009) noted that standard tests could be used to check normality, including:

• **Shapiro-Wilk** and **Kolmogorov-Smirnov***:* According to Shapiro & Wilk (1965), the p-value should be greater than 0.05.

• **Skewness and Kurtosis:** According to Doane & Seward (2011), z-values should be between -1.96 and +1.96.

• **Visual tests***:* According to Cramer & Howitt (2004), histograms, the quantile-quantile plots (Q-Q plots) and boxplots can be used as visual indicators. For example, according to (Hair et al., 2006), the results of a QQ plot and a histogram graph support the hypothesis that the data are normally distributed for a large sample size. To better comprehend a standard data distribution, some researchers suggest that it might be skewed, and this assessment varies from researcher to researcher.

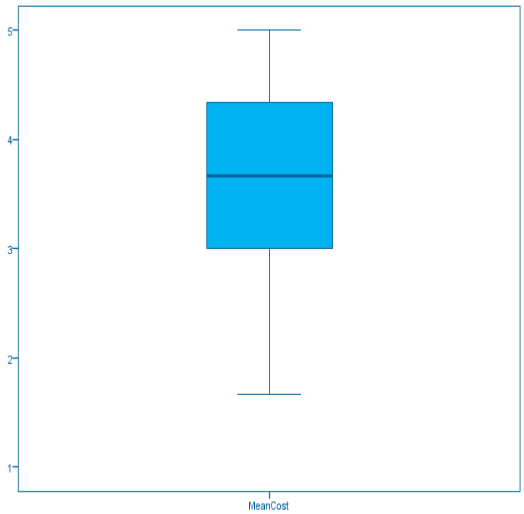
A multivariate analysis was performed below to support the previous findings: normality, linearity, and multicollinearity scores. In order to satisfy the normality assumption, in addition to analysing skewness and kurtosis, plotting and analysing normal Q-Q plot, detrended normal Q-Q plot, and box plot were also used to manage data outliers.

Data outliers are described as responses that differ significantly in some way. This is a key influencing factor as the outcome of the study analysis could present a bias in the assumed framework as outliers could produce a bias in the statistical mean and increase the statistical standard deviation (Krishnaiah et al., 1980; Marsh et al., 1988; Oster, 1999). In the case of data normality, the study data could have been influenced by outliers when accepting critical expectations for the adjustment of a statistical regression test. For this study the researcher used box-whisker diagram to identify outliers and controlled the normality of the data with the values of skewness and kurtosis.

It is only probable to resolve the outlier issue by changing the score, changing the data, or removing the cases, and for this research the problem was solved by removing cases – the outliers. According to Field (2013), the statistical procedure is widely used and chosen for this research, which involves measuring the statistical standard deviation from the statistical mean. Furthermore, Tabachnick & Fidell (2006) recommend examining the responses with standardised scores, which should be greater than 3.0 on a 5-point Likert scale.

After managing the outliers, we had normal data, from the normal Q-Q plot and the detrended normal Q-Q plot. The results appear to have a satisfactory degree of normality as points are aligned with the line and are normally distributed on the normal Q-Q plot. In addition, points are in the range of [-2, +2] in the detrended normal Q-Q plot.

Box plot is different approach to test normality of data. It presents the median as the horizontal line within the box and the IQR (range between the first and third quartiles) as the length of the box. The line extending from the top and bottom of the box represents the minimum and maximum values when they are within 1.5 times the IQR of each end of the box (i.e., Q1 − 1.5* IQR and Q3 + 1.5* IQR). Results >1.5x and 3x the IQR fall outside the box plot and are deemed outliers and extreme outliers, respectively. A symmetric box plot with the median line at approximately the centre of the box and with symmetric whiskers indicates that the data may have come from a normal distribution, as shown in figures 4.2, figure 4.3, figure 4.4 and figure 4.5.



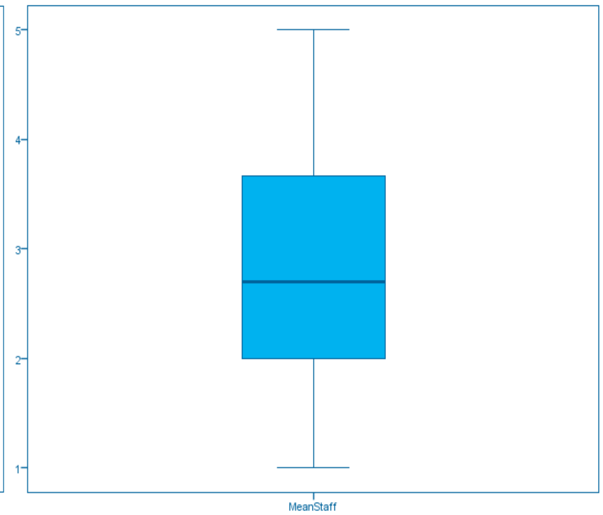
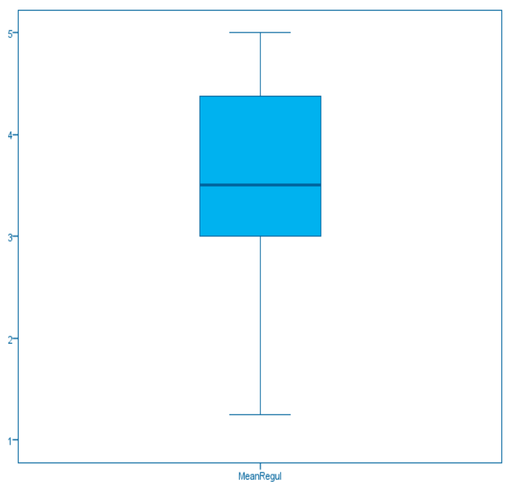




Figure 4.2 Box plot MeanCost

Figure 4.3 Box plot MeanStaff



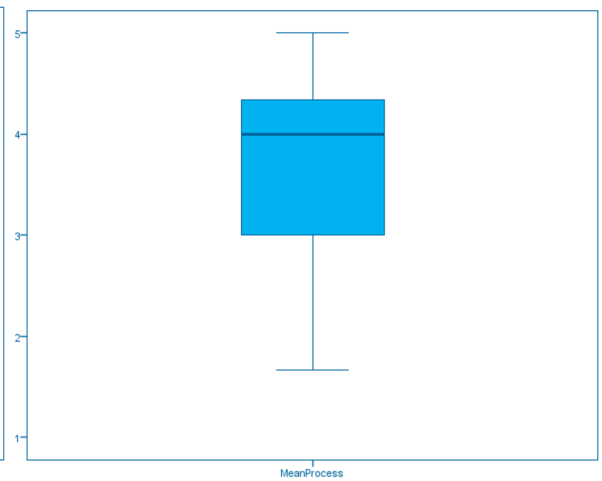




Figure 4.4 Box plot MeanRegul

Figure 4.5 Box plot MeanProcess

The graph itself cannot provide definitive evidence for the research findings (Hair et al., 2006). Therefore, for each construct item included in this study, values from a kurtosis and skewness test were assessed to authorize the normal distribution of the data (Hair et al., 2006). In addition, the data symmetry in the kurtosis and skewness tests can be skewed on the left side of the tail and point to the right side of the tail, meaning this is positive skewness. However, if the data symmetry is skewed on the right side of the tail and points to the left side of the tail, the offset will be negative. For comparison, peakedness identifies and quantifies the median around the central value. A standard measure of peakedness is kurtosis, a degree of peakedness of a probability distribution. Thus, with zero kurtosis and skewness, the study data are normally distributed.

However, normality decreases depending on whether the kurtosis and skewness test value is positive or negative (Hair et al., 2006). The rule of thumb for the skewness range at an acceptable index is less than the absolute value of 3 and the kurtosis is less than 10 Kline (2011). The ranges of results obtained are as follows: Mean cost. - skewness -.227, kurtosis -.701, mean staff. - skewness .142, kurtosis -.609, mean regulation. - skewness -.241, kurtosis -.348 and mean process. - skewness -.425, kurtosis -.270. This is another indication that the data set is normally distributed.

In this research, we applied skewness to four different construct items (mean cost, mean staff, mean regulation, and mean process) and the results show that in all four variables, the value of skewness is negative except for the mean staff, but still less than the absolute value of 3.

### 4.7.4. Exploratory factor analysis

Exploratory Factor Analysis (EFA) was performed to obtain statistical evidence of the construct validity. Before conducting an EFA, the normality of the data distribution was tested by considering skewness and kurtosis. (George, 2011) and Hair et al. (2010) argue that the data is considered normal if the values for skewness and kurtosis lie between -2 and +2. Since the normality of the distribution of our dataset was confirmed, the EFA was further carried out in SPSS (v23).

The exploratory factor analysis procedure began with an initial analysis run to attain eigenvalues for each component in the data as presented on table 4.4. The factor solution was determined based on the amount of eigenvalues greater than one. Multiple question items were adjusted based on EFA to attain higher construct reliability and better model fit. Initially 15 items of the questionnaire were selected to form four constructs two items were deleted, and gave the final scale 13 question items as presented in tables 4.4 and 4.5.

Table 4.4.- Total variance explained

| Total Variance Explained | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Component | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | | Rotation Sums of Squared Loadings | | |
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 4.598 | 35.373 | 35.373 | 4.598 | 35.373 | 35.373 | 2.960 | 22.768 | 22.768 |
| 2 | 2.123 | 16.330 | 51.703 | 2.123 | 16.330 | 51.703 | 2.467 | 18.975 | 41.743 |
| 3 | 1.391 | 10.701 | 62.404 | 1.391 | 10.701 | 62.404 | 1.929 | 14.840 | 56.583 |
| 4 | 1.122 | 8.627 | 71.031 | 1.122 | 8.627 | 71.031 | 1.878 | 14.448 | 71.031 |
| 5 | .864 | 6.648 | 77.679 | | | | | | |
| 6 | .785 | 6.035 | 83.714 | | | | | | |
| 7 | .554 | 4.259 | 87.973 | | | | | | |
| 8 | .463 | 3.562 | 91.535 | | | | | | |
| 9 | .377 | 2.901 | 94.436 | | | | | | |
| 10 | .307 | 2.362 | 96.798 | | | | | | |
| 11 | .200 | 1.541 | 98.339 | | | | | | |
| 12 | .144 | 1.111 | 99.449 | | | | | | |
| 13 | .072 | .551 | 100.000 | | | | | | |

Extraction Method: Principal Component Analysis.

Table 4.5.- After EFA analysis

| | | |
|---|---|---|
| **Compliance Costs** | B.1.1 | GDPR is expensive to comply with |
| **Compliance Costs** | B.1.3 | It is costly to invest in GDPR consultants |
| **Compliance Costs** | B.1.4 | It is costly to invest in new hires to meet the demands of GDPR |
| **Government Support** | B.3.1 | There is a lack of information support from the government bodies in relation to GDPR |
| **Government Support** | B.3.2 | There is a lack of practical guidelines from the government bodies to follow standard procedures correctly |
| **Government Support** | B.3.3 | GDPR does not provide any recommendations regarding the use of technology helping to comply with its requirements |
| **Government Support** | B.3.4 | GDPR does not provide any specific instruments or tools for companies |
| **Regulation Complexity** | B.2.5 | It was challenging to train existing employees about GDPR requirements |
| **Regulation Complexity** | B.2.6 | It is challenging to train new employees about GDPR requirements |
| **Regulation Complexity** | B.2.7 | It was difficult to change the company mindset to ensure that each employee follows GDPR principles |
| **Process Adaptation** | B.4.7 | It is not easy to develop a cyber incident response plan |

| | | |
|---|---|---|
| **Process Adaptation** | B.4.10 | It is challenging to apply emergent technologies (artificial intelligence, robotics, cloud computing, blockchain, etc.) to achieve better compliance with the GDPR |
| **Process Adaptation** | B.4.11 | It is complex to execute periodic audits to ensure that all processes are compliant with GDPR |

As presented on table 4.6 and table 4.7 the Principal Component Analysis (PCA) extraction using the Varimax Kaiser rotation method identified four factors explained 71% of the variance with acceptable factor loadings ranging from .679 to .908 (see Field, 2013: 692). To determine the validity and confirm that the data collected for an exploratory factor analysis was adequate, the Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy (KMO) test and Bartlett test of sphericity were performed, as presented on table 4.8. An obtained KMO value of .730 and a significance level for Bartlett's test below 0.05 suggest a substantial correlation in the data.

Table 4.6.- Component transformation matrix

| **Component Transformation Matrix** | | | | |
|---|---|---|---|---|
| Component | 1 | 2 | 3 | 4 |
| 1 | .611 | .579 | .361 | .402 |
| 2 | -.714 | .426 | .555 | -.027 |
| 3 | -.337 | .022 | -.409 | .848 |
| 4 | .060 | -.695 | .628 | .345 |

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

Table 4.7.- Rotated component matrix

| **Rotated Component Matrix** | | | | |
|---|---|---|---|---|
| | Component | | | |
| | 1 | 2 | 3 | 4 |
| B11 GDPR is expensive to comply with | | | .679 | |
| B13 It is costly to invest in GDPR consultants | | | .846 | |
| B14 It is costly to invest in new hires to meet the demands of GDPR | | | .768 | |
| B25 It was challenging to train existing employees about GDPR requirements | | .891 | | |
| B26 It is challenging to train new employees about GDPR requirements | | .908 | | |
| B27 It was difficult to change the company mindset to ensure that each employee follows GDPR principles | | .695 | | |
| B31 There is a lack of information support from the government bodies in relation to GDPR | .815 | | | |
| B32 There is a lack of practical guidelines from the government bodies to follow standard procedures correctly | .830 | | | |
| B33 GDPR does not provide any recommendations regarding the use of technology helping to comply with its requirements | .838 | | | |
| B34 GDPR does not provide any specific instruments or tools for companies | .821 | | | |
| B47 It is not easy to develop a cyber incident response plan | | | | .760 |

| | | | | |
|---|---|---|---|---|
| B410 It is challenging to apply emergent technologies (artificial intelligence, robotics, cloud computing, blockchain, etc.) to achieve better compliance with the GDPR | | | | .781 |
| B411 It is complex to execute periodic audits to ensure that all processes are compliant with GDPR | | | | .691 |

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 6 iterations.

Table 4.8.- KMO and Bartlett's Test

| **KMO and Bartlett's Test** | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .730 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 617.211 |
| | df | 78 |
| | Sig. | .000 |

### 4.7.5. Reliability analysis

The scales, their reliability, and sample items from the questionnaire are shown in Table 4.9. The measure of internal uniformity, Cronbach's alpha, ranges from .688 to .886, indicating an acceptable reliability level. The alpha value of Cronbach is considered acceptable if it is greater than 0.60 for all constructs in the model (Hair et al., 2021; Ramayah et al., 2014), which suggests that the instrument's reliability was satisfactory.

Table 4.9.- Scales, Reliability, and Sample Items of the Questionnaire

| **Construct** | **N items** | **Sample items** | **Cronbach's alpha (α)** |
|---|---|---|---|
| Compliance Costs | 3 | It is costly to invest in new hires to meet the demands of GDPR | .698 |
| Staff Training | 3 | It is challenging to train new employees about GDPR requirements | .886 |
| Regulation Complexity | 4 | There is a lack of practical guidelines from the government bodies to follow standard procedures correctly | .871 |
| Process Adaptation | 3 | It is not easy to develop a cyber incident response plan | .688 |

## 4.8. Statistical techniques used for data analysis

Tabachnick & Fidell (2006) describe the study factors, or mixtures of sub-factors, used to characterize the subject sample, which can then be described as descriptive statistic. Therefore, a graphical type of data analysis such as tables or charts, is repeatedly used to exhibit compact types of summary study data from numerous statistical tests, and results are presented in terms of standard deviation, mean, mode value, statistical frequency, and percent.

This study evaluates the familiarity of the technology startups in Catalonia with the GDPR, the key challenges of the GDPR implementation that they are facing, whether those key challenges are associated with compliance costs, regulation complexity, insufficient government support or process adaptation, whether there is any relationship between those challenges and the year of establishment, size, business sector, and annual expenditures on GDPR compliance also to provide recommendations to help technology startups in Catalonia to overcome the challenges resulting from the GDPR. For the purpose described advanced statistical analysis techniques will be used starting with ANOVA, followed by independent sample T-test, correlation analysis and regression analysis.

***1.- ANOVA. -*** A one-way ANOVA will be used to compare the effect of independent variables on dependent variables to determine whether startup's respondents' perceptions on GDPR challenges differed significantly depending on categorical and scale variables. The ANOVA tests to be ran will be as follows:

***ANOVA Test 1.***- The number of new employees recruited to facilitate GDPR compliance versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years startup established.

***ANOVA Test 2.***- Responsible for GDPR compliance in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years startup established.

***ANOVA test 3***.- Total number of employees in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years startup established.

***ANOVA test 4. Part 1***.- The startup business sector versus compliance costs, staff training, regulation complexity and process adaptation.

***ANOVA test 4. Part 2.***- The startup business sector versus GDPR annual spending and months to achieve compliance.

***ANOVA test 5.***- The respondent's role in a start-up versus compliance costs, staff training, regulation complexity and process adaptation.

***ANOVA test 6.***- The respondent's level of education versus compliance costs, staff training, regulation complexity and process adaptation.

***ANOVA test 7.***- The respondent's field of education versus compliance costs, staff training, regulation complexity and process adaptation.

***2.- Independent Sample T-test***. - Gender will be analyzed using Independent Sample T-Test since it consists of only two categories. The sample consists of 79 males and 28 females, and the test will be run in order to find out if there are significant difference in their perceptions in terms of GDPR challenges.

***3.- Correlation analysis***. -Correlation is a statistical measure that helps in determine the magnitude of the relationship between two or more variables or factors. To examine a possible relationship between different factors utilized in this study, a Pearson's R-correlation coefficient test is performed. Pearson's R is applied to measure the intensity of a linear relation between two variables or factors. The test is performed for the following scale variables: Compliance Costs, Staff Training, Regulation Complexity and Process Adaptation as the GDPR challenges.

In defining the correlations, Cohen (2013) research dictated that large correlations had *R* values greater than .50. Cohen (2013) further stated *R* values less than .30 have small correlations and less than .50 have medium correlations. In the analysis, a confidence interval of 99% and 95% will be set allowing only 1% or 5% error probability in the result. Both confidence intervals are used in social science studies using primary data to verify respondents' opinions/perspectives. Moreover, if the data is normally distributed the researcher will be doing parametric tests.

***4.- Regression analysis***. - The aim of the correlation analysis is to check how the scale variables relate to each other. If in the correlation test analysis is found the presence of correlation between compliance costs, regulation complexity, staff training and process adaptation, the next step is a regression test. For the regression test a linear regression test on SPSS is performed. Regression is a statistical technique to formulate the model and analyse the relationship rate between variables.

The regression models to be tested will be as follows:

The general mathematical equation for a linear regression model is ($y = a + b_1x_1 + b_2x_2 + ...b_nx_n$). Four linear regression models are proposed to test the degree of relationship between variables using hypothesis testing.

***Model 1.***- In this model will be analysed the rate of relationship between the dependant variable compliance costs and the variables staff training, regulation complexity and process adaptation.

Compliance costs = a + $b_1$Staff training + $b_2$Regulation complexity+$b_3$Process adaptation

The hypothesis to be tested are as follows:

- $H_{o1}$: Compliance costs are not affected by staff training, regulation complexity and process adaptation
- $H_{A1}$: Compliance costs are affected by staff training, regulation complexity and process adaptation

***Model 2.***- In this model it will be analysed the rate of relationship between the dependant variable staff training and the variables regulation complexity and process adaptation.

Staff training = a + $b_1$Regulation complexity + $b_2$Process adaptation

The hypothesis to be tested are as follows:

- $H_{o1}$: Staff training is not affected by regulation complexity and process adaptation.
- $H_{A1}$: Staff training is affected by regulation complexity and process adaptation.

***Model 3.-*** In this model it will be analysed the rate of relationship between the dependant variable process adaptation and the variables staff training, regulation complexity and GDPR annual spending (euros).

Process adaptation= a + $b_1$Staff training + $b_2$Regulation complexity + $b_3$GDPR annual spending

The hypothesis to be tested are as follows:

- $H_{o1}$: Process adaptation is not affected by staff training, regulation complexity and GDPR annual spending.
- $H_{A1}$: Process adaptation is affected by staff training, regulation complexity and GDPR annual spending.

***Model 4.***- In this model it will be analysed the rate of relationship between the qualitative variable months to achieve compliance and the variables staff training, process adaptation, compliance costs and years company established.

$$\text{Months to achieve compliance} = a + b_1\text{Staff training} + b_2\text{Process adaptation} + b_3\text{Compliance costs} + \text{Years Co established}$$

The hypothesis to be tested are as follows:

- $H_{o1}$: Months to achieve compliance are not affected by staff training, process adaptation, compliance costs and year company established.
- $H_{A1}$: Months to achieve compliance are affected by staff training, process adaptation, compliance costs and year company established.

Having framed the hypotheses needed to be tested for each of the four models the linear regression tests will be ran by using the software SPSS. After running the linear regression tests, the following four main tables will emerge for each of the models:

***1.- Variable table. -*** This table indicates the variables that were entered or removed from the model based on the method used for variable selection and it will not use for the result's interpretation since the variables are already known.

***2.- Model summary. -*** This second table will provide details about the characteristics of the model. The elements relevant to the interpretation of the results in each of the four models will be the R-value that represents the correlation between the dependent and independent variables, the R-square showing the total variation for the dependent variable that could be explained by the independent variables, and the adjusted R-square showing the generalization of the results.

***3.- ANOVA. -*** This third table determines whether the model is significant enough to determine the result. The elements relevant to the interpretation of the results are the P-value/Sig. value and the F-ratio. For this study, the 5% level of significance level is chosen. Therefore, the p-value should be less than 0.05 for the result to be significant. The F-ratio represents an improvement in predicting the variable by fitting the model after accounting for the uncertainty present in the model. A value is greater than 1 for F-ratio yield efficient model.

***4.- Coefficients of regression. -*** This fourth table will determine the strength of the relationship such as the significance of the variables in the model and the magnitude by which the dependent variable is influenced, which helps in conducting the hypothesis test for the study. The significance value is the only value important for interpretation and should be less than 0.05 for a 95% confidence interval in this study. Based on the significant value, if Sig. is <0.05 the null hypothesis is rejected and if the Sig. is >0.05, then the null hypothesis is not be rejected.

## 4.9. Summary

The philosophical views and approaches to the design were explained, illustrated how the decision to go with the quantitative method was made, and clearly explained the use of SPSS to generate the descriptive and inferential statistics with data collected from the '*GDPR Challenges*' questionnaire. The questionnaire yielded 116 answers, 107 of which presented valid cases. This allowed the fulfilment of the research objective, formulating several hypotheses relative to the research questions and establishing a series of variables that would form the basis for the study's quantitative analysis. Moreover, the data collection technique has been explained, and the preliminary data testing for the quantitative study was carried out, including the exploratory factor analysis and the reliability analysis and the advanced statistical techniques has been described. The detailed analysis and discussions from descriptive and inferential statistics are provided in Chapter 5.

# Chapter 5 Data analysis and discussions

## 5.1. Introduction

This chapter describes and discusses the analysis's results. Section 2 deals with the respondent and company profile by describing the demographic profile of the respondents, the number of years the companies have been established, the number of persons employed in the company and the weighted frequencies of the respondents by business sectors. Section 3 deals with the descriptive statistics analysis, section 4 deals with the seven ANOVA test results analysis, section 5 with the independent sample T-test analysis, section 6 with the correlation test results analysis and section 7 with the four regression models analysis results.

## 5.2. Demographic profile of survey participants

### 5.2.1. Respondent profile

In part C of the questionnaire respondents completed eight questions related to the respondent and company profile. After the data was cleaned and outliers were removed, the dataset had 107 valid responses. SPSS was used to analyse the demographic profile data of the respondents such as the study participants' role in the company, educational background, and gender. As presented in table 5.1, the highest percentage on the role of the respondents in the company is for the founder or member of the Board of Directors with a 62.6%, followed by the role as a CEO CFO, CMO and managing director with a 15% and manager / department manager with a 13.1%. Moreover, the highest percentage with the highest level of education is for the master degree with a 40.2%, followed by college degree with a 18.7%, bachelor degree with a 15.9%, doctorate degree with a 15.0%, professional degree with a 6.5% and high school diplomas with a 3.7%. In terms of the respondent's field of study, the highest is for Business & Economics Sciences with a 36.4%, followed by Engineering & ICT sciences with a 29.0%, Health sciences with a 17.8%, other within the field of architecture, design, history, tourism, and journalism with a 11.2% and Law sciences with a 5.6%. In terms of respondent's gender 73.8% male and 26.2% female.

Table 5.1 Demographic Profile of the Respondents

| Variables | Sample (n) | Frequency (%) |
|---|---|---|
| *Role of the respondent* | | |
| Founder / Member of the Board of Directors | 67 | 62.6% |
| CEO, CFO, CMO, Managing Director | 16 | 15.0% |
| Manager / Department Manager | 14 | 13.1% |
| Other | 10 | 9.3% |
| *Highest level of education* | | |
| High School Diploma | 4 | 3.7% |
| College Degree | 20 | 18.7% |
| Professional Degree | 7 | 6.5% |
| Bachelor's Degree | 17 | 15.9% |
| Master's Degree | 43 | 40.2% |
| Doctorate Degree | 16 | 15.0% |
| *Field of studies* | | |
| Business & Economics Sciences | 39 | 36.4% |
| Engineering & ICT sciences | 31 | 29.0% |
| Health sciences | 19 | 17.8% |
| Law sciences | 6 | 5.6% |
| Other (architecture, design, history, tourism, journalism) | 12 | 11.2% |
| *Gender* | | |
| Male | 79 | 73.8% |
| Female | 28 | 26.2% |

## 5.2.2 Company profile

SPSS was used to analyse the demographic profile data of the companies that took part in the survey such when the company was established, and the number of persons employed on the company. As presented on the histogram figure 5.1, the highest percentage of companies have been established in the past two to three years with a 22.8%, followed closely by those companies established in the past four to five years with a 22.3%, in the past six to seven years with a 17.8%, in the past eight to nine years with a 16.9%, in the past ten years or more with a 16.5% and with a 3.7% companies that have been established one year ago or less. As presented on the histogram figure 5.2, the highest percentage of companies have two to nine persons working which represents a 57.4% followed by the companies which have ten to forty nine persons working with a 29% and finally the companies with zero to one person employed with a 13.6%.

Figure 5.1 Histogram number of years company established.

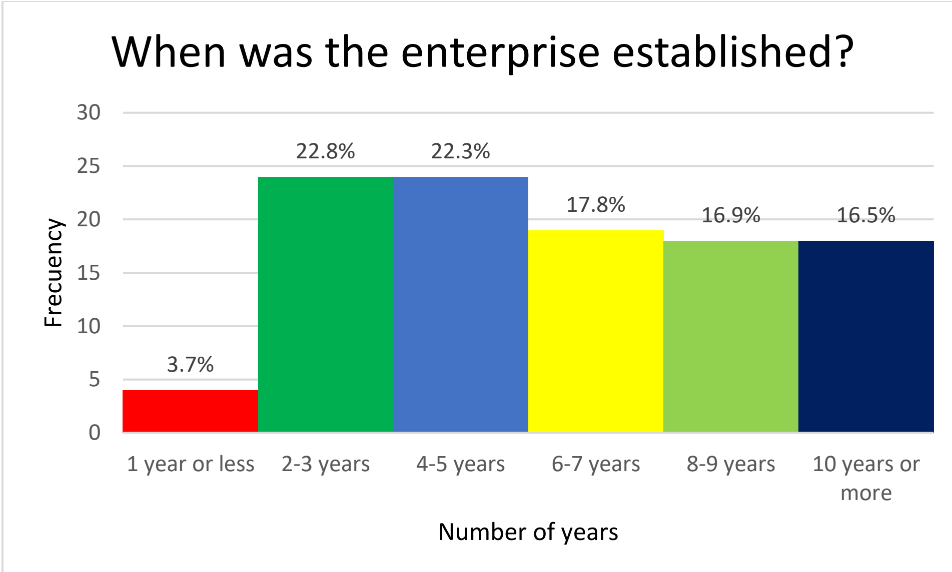
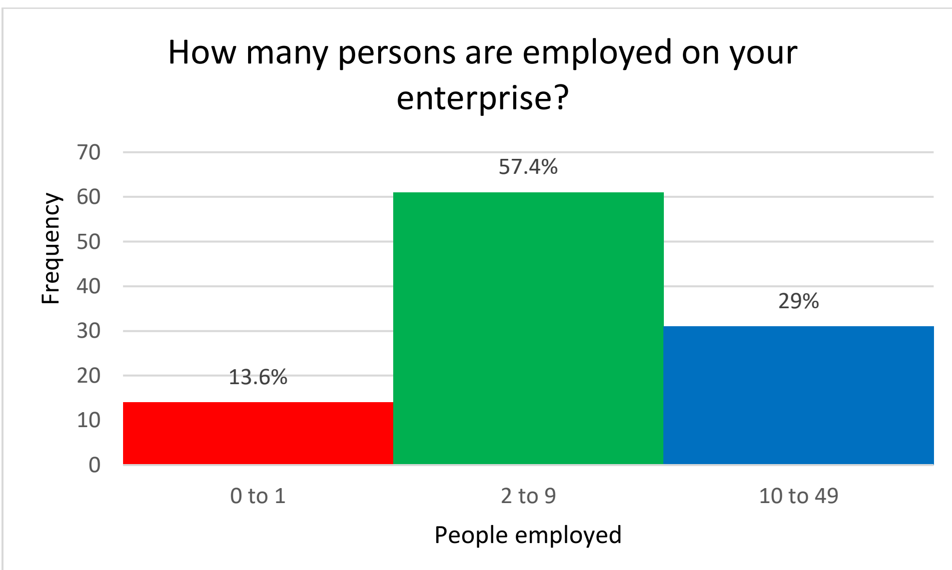



Figure 5.2 Histogram number of years employed on the company.




The business sector from each of the participant companies was also analysed since the respondents had to answer in the survey what was the area of specialization of their company. As presented in table 5.2, the respondents worked within one of the following business sectors, ICT, leisure, health, business services, foodtech & drinks, e-commerce & logistics, fintech & insurtech, greentech, mobility, fashion & design and edtech.

Weighting factors were calculated to match the sample with the population for the business sector specialization of respondents based on official data of the Barcelona & Catalonia Startup Hub, 2020 and a weighted sample frequency was calculated to correct the under-representation of business sectors in the survey. The respondents on the ICT sector were 29, followed by the health sector with 22, the e-commerce & logistics with 19 and the leisure sector with 12 which in total represents the 83.3% of the sample. Moreover, the respondents on the greentech sector were 7, followed by the Business services sector with 5, the fashion and design sector with 4, the edtech sector with 3, the foodtech & drinks with 2, the fintech & insurtech with 2 and mobility with 2 which in total represents the 16.7% left of the sample.

Table 5.2 Startups by Business Sector: Weighted Frequencies

| Variable | Sample, n (frequency, %) | Population, N | Weight (population) | Frequency sample (weighted) |
|---|---|---|---|---|
| *Startup Economic Sector* | | | | |
| ICT | 29 (27.1%) | 374 | .22 | 21.6% |
| Leisure | 12 (11.2%) | 355 | .21 | 22.1% |
| Health | 22 (20.6%) | 289 | .17 | 17.2% |
| Business Services | 5 (4.7%) | 142 | .08 | 7.4% |
| Foodtech & Drinks | 2 (1.9%) | 97 | .06 | 6.0% |
| E-commerce & Logistics | 19 (17.8%) | 91 | .05 | 5.6% |
| Fintech & Insurtech | 2 (1.9%) | 88 | .05 | 3.6% |
| Greentech | 7 (6.5%) | 82 | .05 | 5.1% |
| Mobility | 2 (1.9%) | 72 | .04 | 4.5% |
| Fashion & Design | 4 (3.7%) | 57 | .03 | 3.5% |
| Edtech | 3 (2.8%) | 56 | .03 | 3.5% |

**Source:** For the population data: ACCIÓ Strategic and Competitive Intelligence Unit Barcelona, April 2021. Analysis of the Barcelona & Catalonia Startup Hub, 2020. Executive Summary Total: 1708 startups in 2020 (as of April 2021)

## 5.3. Statistical analysis: Descriptive statistical analysis

**Part A questionnaire.** In part A of the questionnaire the participants were presented as shown on table 5.3 with a series of questions about GDPR, personal data, and open data. The respondents completed eight questions items with answer options true / false/ I don’t know to find out their personal perceptions and familiarity with the GDPR. Questions 1 and 4 to 6 concerned GDPR, questions 2 and 3 concerned personal data and questions 7 and 8 concerned open data.

Table 5.3 The percentage of different responses for each question in Part A

| Question Items | True/False/Missing | Frequency | Valid Percent |
|---|---|---|---|
| The General Data Protection Regulation (GDPR) governs the processing of personal data (collection, storage, and use) | 1,00 true | 109 | 97.3 |
| | 3,00 I don't know | 3 | 2.7 |
| Any information that can be used to identify an individual is personal data | 1,00 true | 95 | 84.8 |
| | 2,00 false | 9 | 8.0 |
| | 3,00 I don't know | 8 | 7.1 |
| Location data collected by your mobile phone is not personal data | 1,00 true | 18 | 16.1 |
| | 2,00 false | 79 | 70.5 |
| | 3,00 I don't know | 15 | 13.4 |
| The General Data Protection Regulation (GDPR) does not give you the right to access the personal data organizations hold about you | 1,00 true | 24 | 21.4 |
| | 2,00 false | 84 | 75.0 |
| | 3,00 I don't know | 4 | 3.6 |
| There are still no financial penalties for companies that do not comply with the General Data Protection Regulation (GDPR) | 1,00 true | 5 | 4.5 |
| | 2,00 false | 97 | 86.6 |
| | 3,00 I don't know | 10 | 8.9 |
| The General Data Protection Regulation (GDPR) allows for 'data portability' meaning that you can take your data from one organization and give it to another | 1,00 true | 34 | 30.4 |
| | 2,00 false | 61 | 54.5 |
| | 3,00 I don't know | 17 | 15.2 |
| Open data does not generally include personal data | 1,00 true | 54 | 48.2 |
| | 2,00 false | 26 | 23.2 |
| | 3,00 I don't know | 32 | 28.6 |
| Open data can only be used, modified, and shared for non-commercial purposes | 1,00 true | 29 | 25.9 |
| | 2,00 false | 42 | 37.5 |
| | 3,00 I don't know | 41 | 36.6 |

The model questionnaire for this part A was adopted from the model presented by the authors (Hartman et al., 2020) which was also used to assess the respondents' existing knowledge and views about data practices. As presented on table 5.3, 112 valid responses were collected, and results in terms of familiarity and understanding of GDPR were mixed: 97,3% of the sample correctly answered a question about its primary purpose and 30,4% provided correct answers to a question about data portability. These results show certain similarity and contradiction to the results of Hartman et al. (2020) with a 93% of the sample correctly answered a question about its main purpose and 53% provided correct answers to a question about data portability and the cause could lie on the respondent's GDPR lack of awareness and training which also finds support on the study carried out by Tikkinen-Piri et al. (2018). Concerning the concept of personal data, respondents appeared most knowledgeable with more than 7 out of 10 respondents answering these questions correctly. These results show certain similarity to the results of Hartman et al. (2020) with more than 7 out of 10 respondents answering these questions correctly. Concerning open data, respondents were least knowledgeable with 48.2% and 37% respectively of respondents answering these questions correctly. These results show certain similarity and contradiction to the results of Hartman et al. (2020) with 48.9% and 48.2% respectively of respondents answering these questions correctly and the cause lies on the respondent's lack of knowledge on the type of data that are freely available to everyone to use and republish for their own purposes.

Table 5.4 shows the percentage of questions answered correctly by the respondents in relation to GDPR, personal data and open statements. Concerning the question of GDPR allowing for data portability, which means you can take your data from one organization and give it to another, only 30.4% of the respondents provided a correct answer. Moreover, concerning the two questions on open data an average of 42.8% of the respondents provided a correct answer. These results show certain similarity and contradiction to the results of Hartman et al. (2020) with 52.6% of the respondents providing a correct answer for data portability and with an average of 48.5% correctly answered for the two questions on open data. The more than 20% difference in terms of providing a correct answer for data portability could lie on the respondent's GDPR lack of awareness and lack of training Tikkinen-Piri et al. (2018).

Table 5.4 Percentage of questions answered correctly.

| Question (correct response) | % Correct |
|---|---|
| The General Data Protection Regulation (GDPR) governs the processing of personal data (collection, storage, and use). (True) | 96.4 |
| Any information that can be used to identify an individual is personal data | 84.8 |
| Location data collected by your mobile phone is not personal data. (True) | 70.5 |
| The General Data Protection Regulation (GDPR) does not give you the right to access the personal data organizations hold about you. (False) | 75.0 |
| There are still no financial penalties for companies that do not comply with the General Data Protection Regulation (GDPR). (False) | 86.6 |
| The General Data Protection Regulation (GDPR) allows for 'data portability' meaning that you can take your data from one organization and give it to another. (True) | 30.4 |
| Open data does not generally include personal data. (True) | 48.2 |
| Open data can only be used, modified, and shared for non-commercial purposes. (False) | 37.5 |

As presented on table 5.5 only 2 (1.8%) of the respondents answered 100% of the questions correctly, 22 (19.7%) of the respondents answered correctly minimum 7 out of 8 questions, 50 (44.7%) of the respondents answered correctly minimum 6 out of 8 questions and 80 (71.5%) respondents answered correctly minimum 5 out of 8 questions. These results could lie on the respondent's lack of awareness and therefore lack of training as also mentioned by Tikkinen-Piri et al. (2018) on their study.

Table 5.5. Total correct

| Nº Correct answers | Frequency | Valid Percent |
|---|---|---|
| 3 | 9 | 8.0 |
| 4 | 23 | 20.5 |
| 5 | 30 | 26.8 |
| 6 | 28 | 25.0 |
| 7 | 20 | 17.9 |
| 8 | 2 | 1.8 |
| Total | 112 | 100.0 |

**Part B questionnaire.** In part B of the questionnaire 107 respondents completed thirty-two scale questions items with a five-point Likert scale, ranging from '1.- strongly disagree' to '5 – strongly agree' to identify the challenges they have faced from the enforcement of the GDPR as of May 2018.

As presented on table 5.6a, respondents appeared most concerned with the risk of being accountable when there are not clear GDPR guidelines to follow and with the complexity to execute periodic audits to ensure that all processes are compliant with GDPR, both concerns with the highest mean 3.9346. The results in terms of not clear GDPR guidelines provides support to Härting et al. (2021) quantitative research in which confirms insufficient provision of information as a key challenge for SMEs in Germany without being able to confirm the indicators, which are missing guidelines and lacking support from authorities. The results on the complexity to execute periodic audits to ensure that all processes are compliant with GDPR can be compared to some extent with Poritskiy et al. (2019) quantitative research who while exploring the impact of GDPR challenges on micro, small, medium and large Portuguese organizations within the IT sector the execution of audits and systems also came out as a major challenge for micro organizations with a mean of 3.714.

Table 5.6a. The mean for each scale question in Part B.

| **Questions** | **N** | **Mean** | **Std. Deviation** |
|---|---|---|---|
| GDPR is expensive to comply with | 107 | 3.4673 | 1.03082 |
| The company budget has been significantly increased because of GDPR | 107 | **2.4019L** | 1.00808 |
| It is costly to invest in GDPR consultants | 107 | **3.8318H** | .97599 |
| It is costly to invest in new hires to meet the demands of GDPR | 107 | 3.3738 | 1.23260 |
| We had to acquire new technology solutions to comply with GDPR | 107 | 2.6449 | 1.32645 |
| It was costly to invest in new technology | 107 | 2.5981 | 1.18847 |
| We are spending a lot of time to be GDPR compliant | 107 | 2.6636 | 1.27341 |
| We are spending significant financial resources to be GDPR compliant | 107 | **2.3271L** | 1.10552 |
| GDPR is complex and difficult to understand | 107 | 3.4579 | 1.17586 |
| GDPR lacks precision and clarity | 107 | 3.0280 | 1.08557 |
| Our company had difficulties with understanding and interpreting GDPR | 107 | 2.9720 | 1.20108 |
| It is difficult to ensure that our providers / suppliers / vendors follow the regulation for personal data protection (GDPR) | 107 | 3.7290 | 1.17818 |
| It was challenging to train existing employees about GDPR requirements | 107 | 2.8318 | 1.15322 |
| It is challenging to train new employees about GDPR requirements | 107 | 2.7850 | 1.11616 |
| It was difficult to change the company mindset to ensure that each employee follows GDPR principles. | 107 | 2.7570 | 1.25022 |

| | | | |
|---|---|---|---|
| There is a lack of information support from the government bodies in relation to GDPR. | 107 | **3.7664H** | 1.11236 |
| There is a lack of practical guidelines from the government bodies to follow standard procedures correctly. | 107 | 3.7196 | 1.07978 |
| GDPR does not provide any recommendations regarding the use of technology helping to comply with its requirements | 107 | 3.6729 | 1.00729 |
| GDPR does not provide any specific instruments or tools for companies | 107 | 3.5981 | 1.07159 |
| There is a risk of being accountable when there are no clear GDPR guidelines to follow. | 107 | **3.9346H** | 1.10974 |
| Government fines for GDPR incompliance are too high | 107 | 3.6636 | 1.06349 |
| It was difficult to adapt the existing business model of the company to ensure successful GDPR compliance. | 107 | **2.5888L** | 1.23589 |
| It is challenging to provide our stakeholders (customers, employees, suppliers, government, etc.) with the access to personal data. | 107 | 3.0561 | 1.23496 |
| It is not easy to establish a clear procedure to delete an individual's data. | 107 | 3.2056 | 1.31564 |
| It is challenging to process growing data in a quick way | 107 | 3.5514 | 1.25317 |
| It is hard to ensure portability of personal data | 107 | 3.2243 | 1.15177 |
| We are not able to have a person performing the processing if a data subject opts out of automated processing. | 107 | 3.5607 | 1.36795 |
| It is not easy to develop a cyber incident response plan | 107 | **3.8598H** | 1.03202 |
| It is not easy to know where all the personal data of our stakeholders is stored. | 107 | 2.8224 | 1.25000 |
| It is challenging to respond to data enquiries within a 30-day obligation period. | 107 | 2.8879 | 1.32698 |
| It is challenging to apply emergent technologies (artificial intelligence, robotics, cloud computing, blockchain, etc.) to achieve better compliance with the GDPR. | 107 | 3.6168 | 1.08719 |
| It is complex to execute periodic audits to ensure that all processes are compliant with GDPR. | 107 | **3.9346H** | 1.03040 |

H Highest mean

L Lowest mean

Respondents are also concerned with the difficulty to develop a cyber incident response plan, the cost to invest in GDPR consultants and the lack of information support from the government bodies in relation to GDPR with a mean of 3.8598, 3.8318 and 3.7664 respectively. The results in the difficulty to develop a cyber incident response plan provides support to the view of Tim Erridge, context information security in an interview carried out by Steve Mansfield-Devine**,** editor of the Computer Fraud & Security (Mansfield-Devine, 2016) in which stated that a key challenge for any company is to demonstrate an already developed cyber incident response plan that will meet the spirit of GDPR and reduce the risk of fines (Mansfield-Devine, 2016).

The results in terms of the fact that is costly to invest in GDPR consultants provides support to the argument of Mangini et al. (2020) about their quantitative research on 49 EU executives in which costs and difficulty to implement GDPR without third party consulting came out as major concerns.

The results in terms of the lack of information support from the government bodies provides support to the previous study carried out by Cochrane et al. (2020) who underlined the importance for SMEs of receiving practical guidelines that would be tailored to their needs and to the previous qualitative study before GDPR coming into force carried out by Norval et al. (2021) who underlined the importance for UK based technology startups being more supported by the supervisory authorities.

On the other hand, for the startups adapting their existing business model of the company to ensure successful GDPR compliance is not really representing the problem of the startups with a mean of 2.5888 or whether their budget has been significantly increased because of GDPR and whether they are spending significant financial resources to be GDPR compliant with a mean of 2.4019 and 2.3271, respectively, are also not representing the problem for the startups. The author finds there is a logic to these results since the data collection took place from May 2021 to November 2021, and 22.8% of the startups that took part in the survey were already established in the past two to three years and 3.7% one year ago or less as presented on the histogram figure 5.1. If we take this into account and the fact that the GDPR came into force in May 2018, these startups had the opportunity to integrate GDPR into their business model from the start as what is known as data privacy by design and regulated under art. 25 of the GDPR which makes it for them less of a challenge not having to significantly increase their budget or spend significant financial resources since they most considerable expenditure would have been at the start when designing their business model.

However, by comparing the mean of the four constructs as presented on table 5.6b, the highest mean corresponds with the construct insufficient government support (M=3.7258; SD=1.07404), which is likely to agree that for the Catalonian technology startups that participated in the survey the lack of government support is the biggest challenge.

Table 5.6b. The mean for each construct

| Descriptive Statistics | | | |
|---|---|---|---|
| **Construct** | **Mean** | **Std. Deviation** | **N** |
| Compliance Costs | 2.9135 | 1.14266 | 107 |
| Regulation Complexity | 3.0801 | 1.16575 | 107 |
| Insufficient Government Support | 3.7258 | 1.07404 | 107 |
| Process Adaptation | 3.3007 | 1.20781 | 107 |

As explained in chapter 4 an EFA analysis was performed to obtain statistical evidence of the construct validity and the final scale resulted in 13 question items for later to carry out the correlation analysis, as presented in table 5.6c.

Table 5.6c.- After EFA analysis

| | | |
|---|---|---|
| **Compliance Costs** | B.1.1 | GDPR is expensive to comply with |
| **Compliance Costs** | B.1.3 | It is costly to invest in GDPR consultants |
| **Compliance Costs** | B.1.4 | It is costly to invest in new hires to meet the demands of GDPR |
| **Government Support** | B.3.1 | There is a lack of information support from the government bodies in relation to GDPR |
| **Government Support** | B.3.2 | There is a lack of practical guidelines from the government bodies to follow standard procedures correctly |
| **Government Support** | B.3.3 | GDPR does not provide any recommendations regarding the use of technology helping to comply with its requirements |
| **Government Support** | B.3.4 | GDPR does not provide any specific instruments or tools for companies |
| **Regulation Complexity** | B.2.5 | It was challenging to train existing employees about GDPR requirements |
| **Regulation Complexity** | B.2.6 | It is challenging to train new employees about GDPR requirements |
| **Regulation Complexity** | B.2.7 | It was difficult to change the company mindset to ensure that each employee follows GDPR principles |
| **Process Adaptation** | B.4.7 | It is not easy to develop a cyber incident response plan |
| **Process Adaptation** | B.4.10 | It is challenging to apply emergent technologies (artificial intelligence, robotics, cloud computing, blockchain, etc.) to achieve better compliance with the GDPR |
| **Process Adaptation** | B.4.11 | It is complex to execute periodic audits to ensure that all processes are compliant with GDPR |

After the EFA analysis the four questions left for the insufficient government support construct were directed to find out whether there is a lack of information support and practical guidelines from the government bodies about GDPR and to follow standard procedures correctly, respectively. The survey questions for this construct were also directed to find out whether GDPR does not provide any recommendations regarding the use of technology helping to comply with its requirements and whether GDPR does not provide any specific instruments or tools for companies. These findings correlate with Norval et al. (2021) study based on a semi-structured interview on 15 UK tech startups before GDPR came into force as well as with Cochrane et al. (2020) study based on quantitative research on SMEs representatives and semi-structured qualitative interviews with Data Protection Authorities (DPAs), 22 SME Association representatives and 11 SME representatives. This opens the question of what consists of government support that will be dealt with under implication in chapter 6. Moreover, as presented on table 5.6b the lowest mean corresponds with the construct GDPR compliance costs (M=2.9135; SD=1.14266) which shows that respondents are less concerned with GDPR compliance costs although as mentioned earlier respondents still find it costly to invest in GDPR consultants. However, all this analysis must be checked with more quantitative analysis.

In part B of the questionnaire, respondents also completed five multiple choice questions to find out to what the highest GDPR costs of their company are associated with, how much does their company spend on an annual basis for being GDPR compliant, how long did it take their company to achieve GDPR compliance, how many people they had to recruit because of GDPR and who is responsible for GDPR in their company.

1. First multiple-choice question which was framed as follows:

The highest GDPR compliance costs of your company are associated with (chose ONLY ONE answer):

1.- Hiring data protection officer (DPO)

2.- Hiring new employees accountable for data protection

3.- Training employees about GDPR

4.- Acquiring new technology solutions

5.- Modifying processes

6.- Introducing new policies and processes

7.- Monitoring compliance

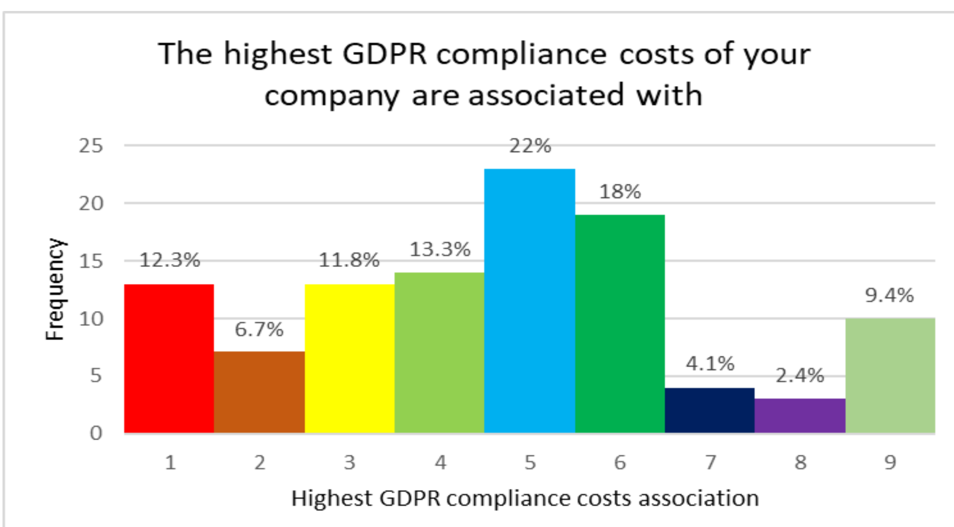
8.- Data protection impact assessment (DPIA)

9.- Risk assessment

10.- Other (specify)

As presented on the histogram figure 5.3 from 106 valid responses, the highest percentage for the highest GDPR compliance costs of the respondents' company is for introducing new polices and processes with 22%, followed by monitoring compliance with 18%, modifying processes with 13.3%, hiring new employees accountable for data protection with 12.3%, acquiring new technology solutions with 11.8%, training employees about GDPR with 6.7%, DPIA with 4.1 % and risk assessment with 2.4% and other with 9.4% in which three of the respondents answered recruitment of external consulting lawyers specialized in GDPR, one respondent answered no acquisition was made, several of the previous answers (3, 5, 7, 8, and 9), one respondent obtained a subsidy, but the cost is relative to the time invested, three of the respondents responded annual contract of the consultant, one respondent answered certification to comply with corporate requirements, one respondent answered that several aspects have influenced and cannot indicate only one.

Figure 5.3 - The highest GDPR compliance costs of startups.



Moreover, for those respondents' company who's highest GDPR compliance costs is for introducing new polices and processes, monitoring compliance and modifying processes, hiring new employees accountable for data protection and acquiring new technology solutions, all these costs are related to the process adaptation challenge since almost 75% of the respondents' company have been established for at least more than four years and therefore established before the GDPR came into force which needed to adapt their existing business model of the company to ensure successful GDPR compliance. This can also be linked to the previous studies of Härting et al. (2021) and Poritskiy et al. (2019) which both recognize that the process adaptation and employees training for micro enterprises with less than 10 employees and small enterprises with 10 to 49 employees is more of a challenge than for medium sized enterprises with 50 to 249 employees and for larger enterprises with 250 employees or more. Moreover, for those respondents' company who's highest GDPR compliance costs are for recruitment of consultants. The results are logical since  can also be linked to the previous study carried out by TrustArc (2017) before GDPR came into force who in their independent report states as a major challenge for organisations to make significant investments on consultants, new hires and technology to meet the GDPR deadline and to the study carried out by Mangini et al. (2020) about their quantitative research on 49 EU executives in which costs and difficulty to implement GDPR without third party consulting came out as major concerns.

2. Second multiple-choice question was framed as follows:

How much does your company spend on an annual basis for being GDPR compliant?

1.- Less than €5,000

2.- €5,000-€10,000

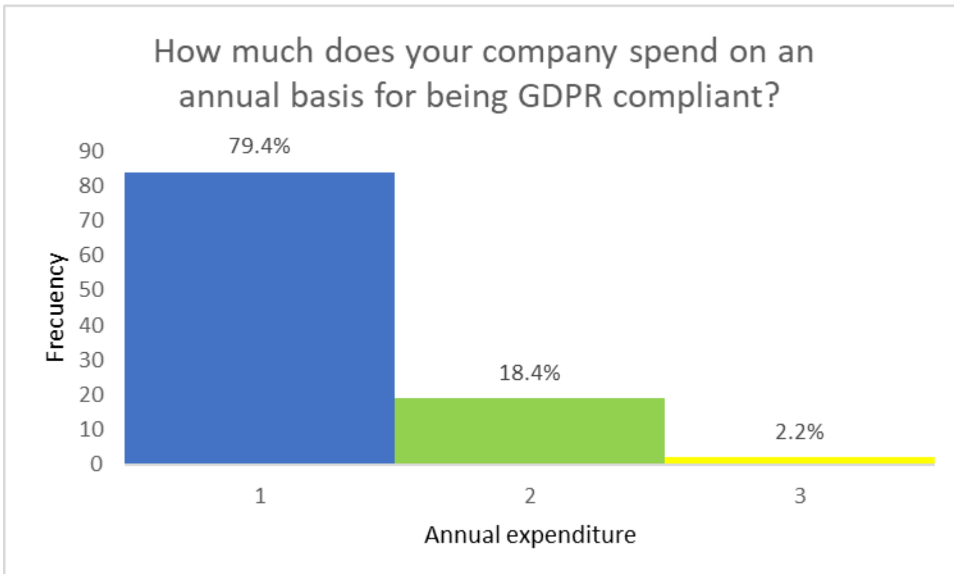
3.- €10,000-€50,000

4.- €50,000-€100,000

5.- More than €100,000.

As presented on the histogram figure 5.4 from 106 valid responses, 84 of the respondents' companies spend less than €5,000 on an annual basis for being GDPR compliant which represents a 79.4%, 19 of the respondents' companies spend between €5,000 and €10,000 which represents a 18.4% and 2 of the respondents' companies spend €10,000 or more which represents a 2.2%.

Figure 5.4 - How much does your company spend on an annual basis for being GDPR compliant?




For those respondents' companies that represent almost 80% of the participants and who have spent less that €5,000 on an annual basis for being GDPR compliant tell the researcher that their size and fewer human and financial resources may have influence their expenditure. The results are logical since can also be linked to the previous works of Freitas & Mira da Silva, (2018), Tikkinen-Piri et al. (2018), Layton & Elaluf-Calderwood (2019), Sirur et al. (2018) and Yeung & Bygrave (2022) show that the implementation of GDPR is a challenge for any company, and in particular for small and medium-sized enterprises (SMEs), since they have fewer human and financial resources to carry out the necessary measures to comply with the regulation. In the research work of Pedroso et al. (2021) and Li, Werner, & Ernst (2019) research work, it was found that while large companies can implement and respond appropriately to the GDPR implementation challenges, SMEs and startups do not always have the expertise and resources to do so. Within the research findings of  Grundstrom et al. (2019) and Nabbosa & Iftikhar (2019), participants also perceived the GDPR compliance process negatively due to its cost.

3. Third multiple-choice question was framed as follows:

How long did it take your company to achieve GDPR compliance?

1.- 3 or less months

2.- 4-6 months

3.- 7-9 months

4.- 10-12 months

5.- 13-18 months

6.- 19-24 months

7.- More than 24 months

8.- We have started but have not yet reached compliance.

As presented on the histogram frequency figure 5.5 from 106 valid responses, 35 of the respondents' companies spent 3 months or less to achieve GDPR compliance which represents 32.9%, 27 of the respondents' companies spent between 4 to 6 months to achieve GDPR compliance which represents 25.3%, 16 of the respondents' companies have started but have not yet reached compliance which represents 14.6%, 10 of the respondents' companies spent between 10 to 12 months which represents 9.5%, 6 of the respondents' companies spent between 13 to 18 months which represents 5.9%, 6 of the of the respondents' companies spent between 7 to 9 months which represents 5.5%, 4 of the respondents' companies spent more than 24 months which represents 3.4% and 3 of the respondents' companies spent 19 to 24 months which represents 3%.

Figure 5.5 - How long did it take your company to achieve GDPR compliance?


The fact that more than 58% of the respondents' companies spent between 3 months or less and 4 to 6 months to achieve compliance tells that they put all their resources together and concentrated on reaching GDPR compliance, that they took it seriously and perhaps the fact that they did not have to change much their business model because of being already compliant with previous data privacy regulations. Moreover, the author finds there is a logic to these results since around 26.5% of the startups that took part in the survey were established after the GDPR came into force in May 2018, these startups had the opportunity to integrate GDPR into their business model from the start as what is known as data privacy by design and regulated under art. 25 of the GDPR which makes it for them less of a challenge in terms of shorting development times Babu et al. (2021).

The fact that there is also a 14.6% of the respondents' companies which had not yet reached compliance tells the big challenge that represents to them and even in a lower scale for the rest of the respondents' companies that took them between 7 to 18 months and the minority that took them between 19 to more than 24 months. The logic for these results can also be related to the fact that these startups did not pay significant prior emphasis on security. Sirur et al. (2018) on their studies confirm that those companies that felt GDPR compliance was onerous had in common the insufficient privacy by design on their business model.

4. Fourth multiple-choice question was framed as follows:

How many people you had to recruit because of GDPR?

1.- None

2.- 1

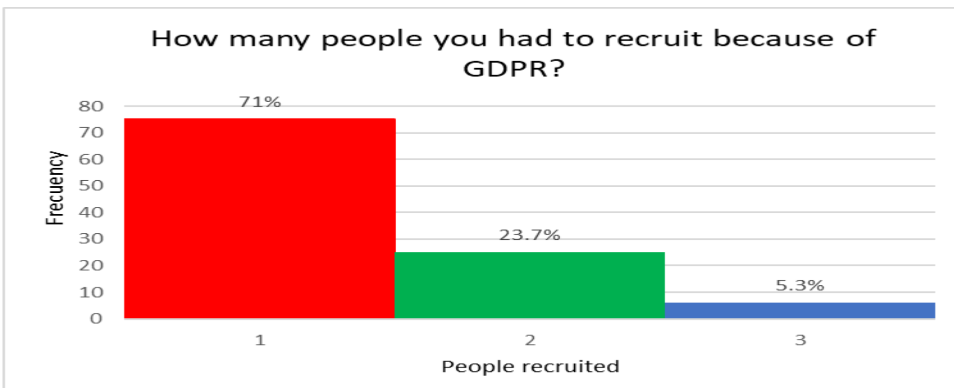
3.- 2-5

4.- 6-10

5.- More than 10.

As presented on the histogram frequency figure 5.6 from 106 valid responses, 75 of the respondents' companies did not recruit any person because of GDPR which represents 71%, 25 of the respondents' companies did recruit between 1 to 5 persons because of GDPR which represents 23.7% and 6 of the respondents' companies did recruit between 6 to 10 persons because of GDPR which represents 5.3%.

Figure 5.6 - How many people you had to recruit because of GDPR?




Withey (2018) addresses the need for European companies to make more investments in the cybersecurity field, namely, in hiring cybersecurity professionals and DPOs. The fact that more than 71% of the respondents' companies did not recruit any person because of GDPR can be linked to the highest GDPR compliance costs, to how much they spend on an annual basis for being GDPR compliant and to who is responsible for GDPR compliance in their company. In terms of the highest GDPR compliance costs only three of the respondents answered recruitment of external consulting lawyers specialized in GDPR and another three of the respondents responded annual contract of the consultant which shows that for the respondents' companies the recruitment of people was not within their priorities specially when almost 80% of the participants have spent less that €5,000 on an annual basis for being GDPR compliant. This could be because the startups have laid out a framework to train their existing and new and future employees or because their founders since they are small companies have decided to train their staff themselves. This can be linked to the question of who is responsible for GDPR compliance in their company.

5. Fifth multiple-choice question was framed as follows:

Who is responsible for GDPR compliance in your company?

1.- Data Protection Officer (DPO)

2.- Chief Protection Officer (CPO)

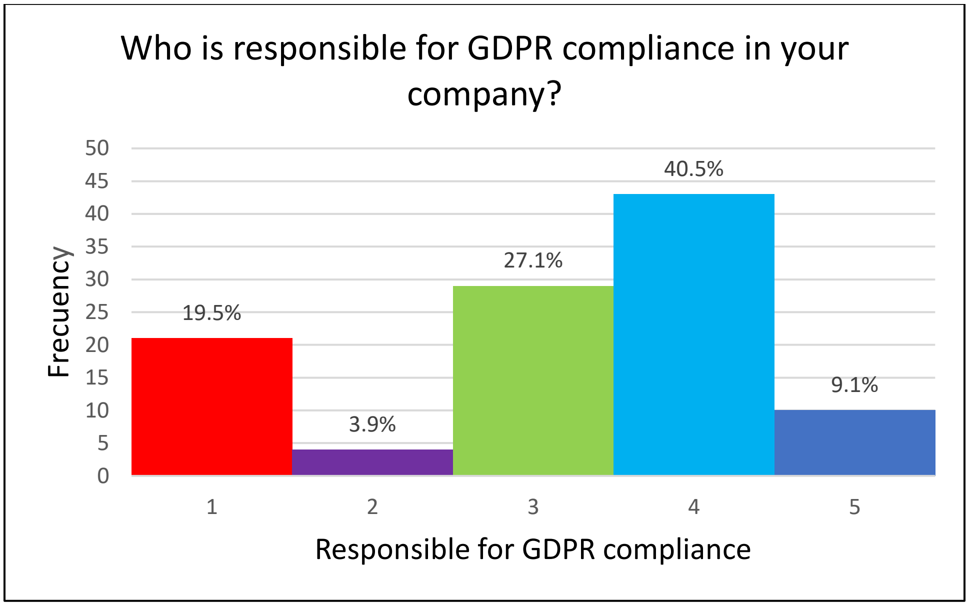
3.- 3rd party consultant

4.- Myself

5.- Other (specify)

As presented on the histogram frequency figure 5.7 from 106 valid responses, 43 of the respondents' companies stated that they were responsible for GDPR compliance in their company which represents 40.5%, 29 of the respondents' companies stated that a third party consultant was responsible for GDPR compliance in their company which represents 27.1%, 21 of the respondents' companies stated that a DPO was responsible for GDPR compliance in their company which represents 19.5%, 4 of the respondents' companies stated that a CPO was responsible for GDPR compliance in their company which represents 3.9% and 9 of the respondents' companies stated other which represents 9.1% and in which each respondent answered; differently: the CTO, the team, the person responsible for communication, the managing director, the company's delegate, the company's administrator, the technical and legal team, the management, and the CFO.

Figure 5.7 - Who is responsible for GDPR compliance in your company?




The fact that 40.5% of the respondents' companies stated that they were responsible for GDPR compliance makes sense because the chances are that they are not required by law to formally appoint a DPO to oversee GDPR compliance and they assign an internal staff member or team of staff responsible for GDPR compliance and even if they are required to appoint a DPO, they can assign an employee within the company, which might be beneficial for the company as it would help focus on GDPR implementation and promote accountability Bräutigam (2016). However, still the big majority of the respondents' companies makes use of a third party consultant, DPO or CPO and this is logical specially for those companies that were established well before the GDPR came into force and as Sirur et al. (2018) identified small companies without significant prior emphasis on security felt GDPR compliance was onerous indicating that there was insufficient privacy by design and being in need of contracting the external services of a DPO or third party consultant.

## 5.4. ANOVA tests

A one-way analysis of variance was performed to compare the effect of independent variables on dependent variables to determine whether startups respondents' perceptions on GDPR challenges differed significantly depending on categorical and scale variables.

**ANOVA test 1** explores the relationship between *the number of new employees recruited to facilitate GDPR compliance versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years of startup established.* Table 5.7 shows these relationships that were measured and reports statistically significant differences in compliance costs and GDPR annual spending depending on the number of new employees recruited to facilitate GDPR compliance. Therefore, the analysis suggests that the null hypothesis 1 is partially accepted.

*$H_o$1: There is no significant relationship between the number of new employees recruited to facilitate GDPR compliance versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years of startup established.*

Table 5.7 Factor unity ratings, standard deviation, and significance depending on the number of new employees recruited to facilitate GDPR compliance.

| Factor | The number of new employees recruited | *M* | *SD* | *F* | *Sig.* | Group Differences |
|---|---|---|---|---|---|---|
| Compliance Costs | None | 3.47 | .85 | 5.464 | .006* | ▪ none vs. 1-5 employees |
| | 1-5 employees | 3.97 | .61 | | | |
| | 6-10 employees | 4.27 | .81 | | | |
| Staff Training | None | 2.71 | 1.04 | 3.039 | .052 | |
| | 1-5 employees | 3.21 | .94 | | | |
| | 6-10 employees | 3.42 | 1.40 | | | |
| Regulation Complexity | None | 3.62 | .93 | 1.544 | .219 | |
| | 1-5 employees | 3.96 | .84 | | | |
| | 6-10 employees | 3.98 | 1.00 | | | |
| Process Adaptation | None | 3.68 | .85 | 2.428 | .093 | |
| | 1-5 employees | 4.09 | .76 | | | |
| | 6-10 employees | 3.99 | 1.09 | | | |
| GDPR annual spending (*in euros*) | None | 3338.09 | 1880.15 | 13.572 | .000* | ▪ none vs. 6-10 employees<br>▪ 1-5 employees vs. 6-10 employees |
| | 1-5 employees | 3672.50 | 2161.82 | | | |
| | 6-10 employees | 8662.48 | 6315.65 | | | |

| | | | | | |
|---|---|---|---|---|---|
| Time to achieve compliance. (*in months*) | None | 10.08 | 10.38 | .114 | .893 |
| | 1-5 employees | 10.85 | 10.15 | | |
| | 6-10 employees | 8.77 | 2.41 | | |
| Number of years the company established | None | 6.10 | 3.08 | .108 | .898 |
| | 1-5 employees | 5.90 | 3.30 | | |
| | 6-10 employees | 5.55 | 2.61 | | |

*. The mean difference is significant at the 0.05 level.

Since a level of significance was found between compliance costs and the number of new employees recruited as well as between GDPR annual spending and the number of new employees recruited and to examine which of the between-subjects factors differed, the multiple post hoc comparisons using Tukey's HSD test were performed and it was found group differences. Starting with compliance costs, those startups that did not employ any person to facilitate GDPR compliance, compliance costs were less of a challenge (M=3.47; SD=.85) compared to those startups that employed between 1 to 5 people (M=3.97; SD=.61). These results mean that the compliance cost increase when a company hires between 1 to 5 employees rather than when it does not hire any employees, but the compliance cost does not increase a lot since the mean difference between then is not so high. The fact that compliance costs mean for those startups that employed between 6 to 10 employees (M=4.27; SD=.81) is higher than the other groups it is just a mere coincidence, since not significance difference has been found between the groups. Withey (2018) addresses the need for European companies to make more investments in the cybersecurity field, namely, in hiring cybersecurity professionals and DPOs. The compliance cost increase when a company hires between 1 to 5 employees rather than when it does not hire any employees could be due to the fact of hiring a DPO or a third-party consultant which may not be within the pay roll of the company but rendering services through a services agreement. Therefore, these results may not be conclusive and therefore will form part of the limitations of this research.

From the literature review the researcher thought it will be worth testing whether there was a significant relationship between staff training and the number of new employees recruited. Tikkinen-Piri et al. (2018) identified that GDPR will demand substantial human resources and that it will also be necessary to offer adequate training to employees to deal with the GDPR requirements. However, the results show that there is no significant relationship between the staff training and the number of new employees recruited. This could be because the startups have laid out a framework to train their existing and new and future employees or because their founders since they are small companies have decided to train their staff themselves.

In terms of process adaptation and the number of new employees recruited the researcher thought that it will be worth checking for any relationship thinking that for the companies to adapt their business model to the GDPR it will be necessary to recruit new employees as also identified by Tikkinen-Piri et al. (2018) and Withey (2018) . However, the results show that there is no significant relationship between process adaptation and the number of new employees recruited. This could be because they have hired external consultants who are not in the payroll of the company to advise them or that their founders and existing employees have done it themselves since they are small startups.

However, when testing the relationship between GDPR annual spending and the number of new employees recruited a significant difference was found among two groups, for those startups that employed between 1 to 5 employees, GDPR annual spending was less of a challenge ($M=3672.50$; $SD= 2161.82$) compared to those startups that employed between 6 to 10 employees ($M=8662.48$; $SD=6315.65$). The results are logical since an increase from none to 1 up to 5 employees recruited to facilitate GDPR compliance; makes compliance costs become more of a challenge for the startups that have had their budgets significantly increased because of GDPR. The same logic we find in the GDPR annual spending which is more of a challenge for those startups who had to increase the number of new employees recruited to facilitate GDPR compliance. This can also be linked to the previous study carried out by TrustArc (2017) before GDPR came into force who in their independent report states as a major challenge for organisations to make significant investments on consultants, new hires and technology to meet the GDPR deadline.

However, the researcher thought it will be worth also testing whether there was a significant relationship between the time to achieve compliance and the number of new employees recruited to facilitate GDPR compliance thinking that it will decrease the time to achieve GDPR compliance. However, the results show that there is no significant relationship between the time to achieve compliance and the the number of new employees recruited to facilitate GDPR compliance. Therefore, hiring new employees is not going to affect the time to achieve compliance and although the external factors are unknown some assumptions can be made such that the time to achieve compliance can be that the startups hire a new employees to facilitate GDPR compliance, but depending on their significant prior emphasis on security indicating sufficient or insufficient privacy by design on their business model may lead to the companies to achieve compliance in a shorter or a longer term.

Moreover, the researcher thought it will be worth also testing whether there was a significant relationship between the number of years the company being established, and the number of new employees recruited to facilitate GDPR compliance thinking that the more the years the company has been established the more new employees will be recruited due to the required process adaptation of their business model and that less new employees will be recruited to facilitate GDPR compliance on those startups created after the GDPR coming into force which will have already applied privacy by design. Sirur et al. (2018) identified that smaller organisations without significant prior emphasis on security felt GDPR compliance was onerous indicating that there was insufficient privacy by design. However, the results show that there is no significant relationship between the number of years the company being established, and the number of new employees recruited to facilitate GDPR compliance. Therefore, the years the company has been established is not going to affect the number of new employees recruited to facilitate GDPR compliance and although the external factors are unknown some assumptions can be made such the fact that the startups independently of the number of years the company has been established they may only hire off the pay roll a DPO or external consultant (Tikkinen-Piri et al. (2018) and still consider it as a new employee which is an already recognised limitation. Moreover, for those startups which are not obligated to designate a DPO for now, they may hire a new employee, or they may nominate a staff member internally which may be beneficial**,** as this would help focus on GDPR implementation and promote accountability Bräutigam (2016). This is the especially the case if a company is looking to grow or make more intensive use of personal data in the future. Building up competencies internally may be an effective strategy compared to hiring a new DPO, as a hands-on employee who knows the business is needed Bräutigam (2016).

**ANOVA test 2,** explores the relationship between *responsible for GDPR compliance in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years startup established.* Table 5.8 shows these relationships that was measured and reports statistically not significant differences. Therefore, the analysis suggests that the null hypothesis 2 is accepted.

*$H_o$2: There is no significant relationship between responsible for GDPR compliance in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years startup established.*

Table 5.8 Factor unity ratings, standard deviation, and significance levels depending on the responsible for the GDPR compliance in a start-up

| Factor | Responsible for GDPR compliance | *M* | *SD* | *F* | *Sig.* |
|---|---|---|---|---|---|
| Compliance Costs | Data Protection Officer (DPO) | 3.71 | .85 | .527 | .716 |
| | Chief Protection Officer (CPO) | 3.61 | .59 | | |
| | 3rd party consultant | 3.70 | .92 | | |
| | Myself | 3.63 | .85 | | |
| | Other | 3.27 | .58 | | |
| Staff Training | Data Protection Officer (DPO) | 3.15 | 1.00 | 1.947 | .108 |
| | Chief Protection Officer (CPO) | 3.24 | 1.09 | | |
| | 3rd party consultant | 2.50 | .84 | | |
| | Myself | 3.02 | 1.12 | | |
| | Other | 2.51 | 1.24 | | |
| Regulation Complexity | Data Protection Officer (DPO) | 3.63 | 1.08 | .827 | .511 |
| | Chief Protection Officer (CPO) | 4.18 | 1.30 | | |
| | 3rd party consultant | 3.88 | .77 | | |
| | Myself | 3.67 | .96 | | |
| | Other | 3.41 | .63 | | |
| Process Adaptation | Data Protection Officer (DPO) | 3.86 | .85 | .067 | .992 |
| | Chief Protection Officer (CPO) | 3.75 | .44 | | |
| | 3rd party consultant | 3.76 | .86 | | |
| | Myself | 3.77 | .86 | | |
| | Other | 3.85 | 1.08 | | |
| GDPR annual spending (*in euros*) | Data Protection Officer (DPO) | 3652.54 | 2158.71 | .497 | .738 |
| | Chief Protection Officer (CPO) | 2875.30 | 1513.34 | | |
| | 3rd party consultant | 4233.11 | 3725.80 | | |

| | | | | | |
|---|---|---|---|---|---|
| | Myself | 3513.97 | 2034.22 | | |
| | Other | 3361.89 | 1994.96 | | |
| Time to achieve compliance. (*in months*) | Data Protection Officer (DPO) | 12.24 | 8.48 | .295 | .881 |
| | Chief Protection Officer (CPO) | 8.48 | 12.41 | | |
| | 3rd party consultant | 9.86 | 9.20 | | |
| | Myself | 9.53 | 10.78 | | |
| | Other | 10.50 | 12.35 | | |
| Number of years the company established | Data Protection Officer (DPO) | 6.60 | 3.67 | 1.021 | .400 |
| | Chief Protection Officer (CPO) | 5.65 | 2.21 | | |
| | 3rd party consultant | 5.33 | 2.59 | | |
| | Myself | 5.95 | 3.02 | | |
| | Other | 7.36 | 3.66 | | |

The researcher thought it will be worth also testing whether there was a significant relationship between responsible for GDPR compliance (the owner, the DPO, the CPO, third party consultant or other) and compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years startup established. From the statistical point of view since there are not significant results it can be established that for the results in general it does not matter who is responsible for GDPR compliance. Compliance costs will be what they must be, staff training will have to be carried out anyway, regulation complexity is not related because it is not going to become less complex depending on who is responsible and the same with process adaptation. In terms of GDPR annual spending the test results show that it does not matter who is going to be responsible and that although the companies are going to have GDPR annual spending it does not show that is necessarily related to whom is responsible for GDPR. So, the main conclusion is that it does not matter who is going to deal with GDPR compliance since it is not going to significantly affect compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and years startup established. This makes sense since there are startups that will hire or contract the services of a DPO, CPO or external consultant to be responsible for GDPR compliance, but there will also be as previously discussed startups which are not obligated to designate a DPO for now, they may nominate a staff member internally which may be an effective strategy compared to hiring a new DPO, as a hands-on employee who knows the business is needed Bräutigam (2016). Therefore, in some cases nominating a competent staff member already working for the company who already knows the business' needs rather than appointing a new DPO may be an effective way to achieve compliance faster.

**ANOVA test 3,** *Total number of employees in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and number of years startup established.* Table 5.9 shows these relationships that were measured and although there is a significant relationship between the GDRP process adaptation, and the number of persons employed on the startup, after running the post hoc tests no significant group differences were found. This means that the significance is very weak, and it must be treated as insignificant because there are not differences between the groups. Therefore, the analysis suggests that the null hypothesis 3 is accepted partially.

*$H_o3$: There is no significant relationship between total number of employees in a startup versus compliance costs, staff training, regulation complexity, process adaptation, GDPR annual spending, months to achieve compliance, and number of years startup established.*

Table 5.9 Factor unity ratings, standard deviation, and significance levels depending on the total number of employees in a startup.

| Factor | Size of a startup | *M* | *SD* | *F* | *Sig.* |
|---|---|---|---|---|---|
| Compliance Costs | 0 to 1 person | 4.02 | .76 | 2.114 | .126 |
| | 2 to 9 persons | 3.62 | .79 | | |
| | 10 to 49 persons | 3.49 | .93 | | |
| Staff Training | 0 to 1 person | 2.43 | .86 | 1.455 | .238 |
| | 2 to 9 persons | 2.95 | 1.01 | | |
| | 10 to 49 persons | 2.91 | 1.20 | | |
| Regulation Complexity | 0 to 1 person | 3.72 | .81 | .091 | .914 |
| | 2 to 9 persons | 3.75 | .91 | | |
| | 10 to 49 persons | 3.66 | 1.02 | | |
| Process Adaptation | 0 to 1 person | 3.95 | .77 | 3.121 | .048* |
| | 2 to 9 persons | 3.91 | .75 | | |
| | 10 to 49 persons | 3.47 | 1.01 | | |
| GDPR annual spending (*in euros*) | 0 to 1 person | 3174.74 | 1770.71 | .345 | .709 |
| | 2 to 9 persons | 3805.87 | 2935.37 | | |
| | 10 to 49 persons | 3726.84 | 2187.37 | | |
| Time to achieve compliance (*in months*) | 0 to 1 person | 15.12 | 13.24 | 2.071 | .131 |
| | 2 to 9 persons | 9.52 | 9.91 | | |

| | | | | | |
|---|---|---|---|---|---|
| | 10 to 49 persons | 9.21 | 8.02 | | |
| Number of years the company established | 0 to 1 person | 5.25 | 3.59 | 1.214 | .301 |
| | 2 to 9 persons | 5.88 | 2.76 | | |
| | 10 to 49 persons | 6.68 | 3.43 | | |

*. The mean difference is significant at the 0.05 level

The fact that process adaptation mean for those startups that have 0 to 1 person employed (M= 3.95; SD= 77) is higher than the other groups is just a mere coincidence, since significance is very weak and not differences have been found between the groups. From the statistical point of view since there are no significant results it can be established that for the results in general it does not matter the number of employees in a company since the process adaptation will have to be carried out anyway.

**NOVA test 4. Part 1,** *The startup business sector versus compliance costs, staff training, regulation complexity and process adaptation.* In this test the foodtech and mobility sectors were not included because the number of respondents from these sectors were not sufficient to carry out statistical tests. Table 5.10 shows these relationships that were measured and that there is statistically significant differences in compliance costs and the startups business sector. Therefore, the analysis suggests that the null hypothesis 4 is accepted partially.

*$H_o4$: There is no significant relationship between startup business sector versus compliance costs, staff training, regulation complexity and process adaptation.*

Table 5.10 Factor unity ratings, standard deviation, and significance levels of the startup business sector (weighted): GDPR challenges.

| Factor | Startup business sector | *M* | *SD* | *F* | *Sig.* | Group Differences |
|---|---|---|---|---|---|---|
| Compliance Costs | ICT | 3.29 | .72 | 2.297 | .018* | ▪ ICT vs. Leisure |
| | Leisure | 4.08 | .64 | | | |
| | Health | 3.54 | .96 | | | |
| | Business Services | 3.80 | .92 | | | |
| | E-commerce & Logistics | 3.79 | 1.11 | | | |
| | Fintech & Insurtech | 4.00 | .00 | | | |
| | Greentech | 3.43 | 1.15 | | | |
| | Fashion & Design | 3.17 | .44 | | | |
| | Edtech | 3.11 | .97 | | | |
| Staff Training | ICT | 2.78 | 1.13 | 1.399 | .193 | |

| | | | | | |
|---|---|---|---|---|---|
| | Leisure | 3.23 | .99 | | |
| | Health | 2.61 | 1.04 | | |
| | Business Services | 2.53 | 1.03 | | |
| | E-commerce & Logistics | 2.70 | 1.09 | | |
| | Fintech & Insurtech | 3.83 | .19 | | |
| | Greentech | 3.05 | 1.30 | | |
| | Fashion & Design | 2.92 | 1.52 | | |
| | Edtech | 2.11 | 1.33 | | |
| Regulation Complexity | ICT | 3.52 | .98 | .882 | .553 |
| | Leisure | 3.96 | .78 | | |
| | Health | 3.45 | .97 | | |
| | Business Services | 3.85 | .67 | | |
| | E-commerce & Logistics | 3.88 | .91 | | |
| | Fintech & Insurtech | 4.00 | 1.16 | | |
| | Greentech | 3.75 | .82 | | |
| | Fashion & Design | 4.38 | .76 | | |
| | Edtech | 3.17 | .28 | | |
| Process Adaptation | ICT | 3.69 | .90 | 2.821 | .004* |
| | Leisure | 4.08 | .64 | | |
| | Health | 3.64 | .78 | | |
| | Business Services | 3.87 | .74 | | |
| | E-commerce & Logistics | 3.95 | .81 | | |
| | Fintech & Insurtech | 3.83 | .19 | | |
| | Greentech | 3.90 | 1.15 | | |
| | Fashion & Design | 4.00 | .99 | | |
| | Edtech | 3.56 | 1.33 | | |

*. The mean difference is significant at the 0.05 level

To examine which of the between-subjects factors differ, the multiple post hoc comparisons using Tukey's HSD test were performed and it was found group differences. Those startups within the ICT business sector compliance costs were less of a challenge (M: 3.29; SD: .72) compared to the startups within the Leisure business sector (M: 4.08; SD: .64).

There is a logic in the relationship between startup business sector compliance costs since those startups that had data privacy security integrated in their business model or those startups that have GDPR by design from the start will become more GDPR compliance cost effective than those startups who did not Babu et al. (2021).

Those startups who did not have data privacy security integrated in their business model will have high compliance costs since they will have to adapt much more their existing business model to ensure successful GDPR compliance as Sirur et al. (2018) identified small companies without significant prior emphasis on security felt GDPR compliance was onerous indicating that there was insufficient privacy by design. Moreover, the ICT-Tourism of Catalonia cluster has been created and promoted by the Department of Business and Labour to improve the competitiveness of companies in the leisure sector, promote their internationalization, attract talent and speed up the incorporation of new technologies (ACCIÓ - Agència per la Competitivitat de l'Empresa, 2022).

However, for staff training and regulation complexity there are not significant results and the fact that process adaptation mean for the startups within the leisure sector (M= 4.08; SD= .64) is higher than the other groups is just a mere coincidence, since significance is very weak and not differences have been found between the groups. From the statistical point of view since there are no significant results it can be established that for the results in general it does not matter the startup's business sector since the process adaptation will have to be carried out anyway.

**ANOVA test 4. Part 2,** *The startup business sector versus GDPR annual spending and months to achieve compliance.* In this test the foodtech and mobility sectors were not included because the number of respondents from these sectors were not sufficient to carry out statistical tests. Table 5.11 shows these relationships that were measured and although there is a significant relationship between the GDRP annual spending, and the startups business sector, after running the post hoc tests no significant group differences were found. This means that the significance is very weak, and it must be treated as insignificant because there are not differences between the groups. Therefore, the analysis suggests that the null hypothesis 5 is accepted partially.

*$H_o$5: There is no significant relationship between startup business sector versus GDPR annual spending and months to achieve compliance.*

Table 5.11 Factor unity ratings, standard deviation, and significance levels of the startup business sector (weighted): GDPR spending and time to achieve compliance.

| Factor | Startup business sector | *M* | *SD* | *F* | *Sig.* |
|---|---|---|---|---|---|
| GDPR annual spending (*in euros*) | ICT | 2672.41 | 932.92 | 8.213 | .000* |
| | Leisure | 3750.00 | 2212.86 | | |
| | Health | 3636.36 | 2155.20 | | |
| | Business Services | 3500.00 | 2142.02 | | |

| | | | | | |
|---|---|---|---|---|---|
| | E-commerce & Logistics | 3026.32 | 1684.07 | | |
| | Fintech & Insurtech | 2500.00 | .00 | | |
| | Greentech | 2500.00 | .00 | | |
| | Fashion & Design | 3750.00 | 2527.03 | | |
| | Edtech | 2500.00 | .00 | | |
| Time to achieve compliance. (*in months*) | ICT | 10.69 | 11.12 | .963 | .480 |
| | Leisure | 12.42 | 11.99 | | |
| | Health | 10.18 | 9.48 | | |
| | Business Services | 4.40 | 3.75 | | |
| | E-commerce & Logistics | 12.37 | 12.39 | | |
| | Fintech & Insurtech | 3.50 | 1.74 | | |
| | Greentech | 6.86 | 10.57 | | |
| | Fashion & Design | 12.00 | 12.71 | | |
| | Edtech | 4.00 | 1.66 | | |

*. The mean difference is significant at the 0.05 level.

The fact that the highest GDPR annual spending (in euros) mean for those startups within the mobility sector (M: 11250; SD: 4221.67) is higher than the other groups is just a mere coincidence, since significance is very weak and not differences have been found between the groups. From the statistical point of view since there are no significant results it can be established that for the results in general it does not matter the startup business sector since they all will have GDPR annual spending.

**ANOVA test 5,** *The respondent's role in a start-up versus compliance costs, staff training, regulation complexity and process adaptation.* Table 5.12 shows these relationships that were measured and reports statistically significant differences in process adaptation and the respondent's role in the startup. Therefore, the analysis suggests that the null hypothesis 6 is accepted partially.

*$H_0$6: There is no significant relationship between respondent's role in a start-up versus compliance costs, staff training, regulation complexity and process adaptation.*

Table 5.12 Factor unity ratings, standard deviation, and significance levels depending on the respondent's role in a startup.

| Factor | Respondent's role | *M* | *SD* | *F* | *Sig.* | Group Differences |
|---|---|---|---|---|---|---|
| Compliance Costs | Founder or member of the board of directors | 3.59 | .91 | .050 | .985 | |
| | CEO, CFO, CMO, Managing Director | 3.54 | .93 | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Manager or Department Manager | 3.57 | .79 | | | |
| | Other | 3.48 | .76 | | | |
| Staff Training | Founder or member of the board of directors | 2.69 | 1.05 | .972 | .409 | |
| | CEO, CFO, CMO, Managing Director | 3.19 | .90 | | | |
| | Manager or Department Manager | 2.83 | 1.29 | | | |
| | Other | 2.87 | 1.16 | | | |
| Regulation Complexity | Founder or member of the board of directors | 3.70 | .97 | .505 | .680 | |
| | CEO, CFO, CMO, Managing Director | 3.86 | .72 | | | |
| | Manager or Department Manager | 3.45 | .85 | | | |
| | Other | 3.70 | .89 | | | |
| Process Adaptation | Founder or member of the board of directors | 3.66 | .77 | 3.267 | .024* | ▪ Founder or member of the board of directors vs. CEO, CFO, CMO, Managing Director |
| | CEO, CFO, CMO, Managing Director | 4.35 | .64 | | | |
| | Manager or Department Manager | 3.74 | 1.01 | | | |
| | Other | 3.93 | 1.03 | | | |

*. The mean difference is significant at the 0.05 level

To examine which of the between-subjects factors differed, the multiple post hoc comparisons using Tukey's HSD test were performed and it was identified group differences. Those respondents with a role as founder or member of the board of directors perceived less of a challenge process adaptation (M: 3.66; SD: .77) compared to those respondents with a role in the company as CEO, CFO, CMO or managing director (M: 4.35; SD: .64). The reason for it could be that the founder who in startups is normally also member of the board of directors perceives process adaptation as a less of a challenge because it is generally seen as a competence or responsibility of the CEO, CFO, CMO and managing director Picken (2017). However, for compliance costs, staff training and regulation complexity there are not significant results.

**ANOVA test 6,** *The respondent's level of education versus compliance costs, staff training, regulation complexity and process adaptation.* Table 5.13 shows these relationships that were measured and although there is a significant relationship between the level of education of the respondents and their perceptions about GDPR staff training and the regulation complexity, after running the post hoc tests no significant differences were found between the groups. This means that the significance is very weak, and it must be treated as insignificant because there are not differences between the groups. Therefore, the analysis suggests that the null hypothesis 7 is accepted partially.

*$H_o7$: There is no significant relationship between respondent's level of education versus compliance costs, staff training, regulation complexity and process adaptation.*

Table 5.13 Factor unity ratings, standard deviation, and significance levels depending on the respondent's level of education.

| Factor | Respondent's level of education | *M* | *SD* | *F* | *Sig.* |
|---|---|---|---|---|---|
| Compliance Costs | High School Diploma | 3.7294 | 1.02071 | 1.744 | .131 |
| | College Degree | 3.9069 | .85955 | | |
| | Professional Degree | 3.8956 | .73628 | | |
| | Bachelor's Degree | 3.2295 | .79938 | | |
| | Master's Degree | 3.5362 | .82994 | | |
| | Doctorate Degree | 3.8737 | .70559 | | |
| Staff Training | High School Diploma | 1.9778 | .42314 | 2.712 | .024* |
| | College Degree | 3.3270 | 1.03496 | | |
| | Professional Degree | 2.8390 | 1.57507 | | |
| | Bachelor's Degree | 2.2786 | 1.00574 | | |
| | Master's Degree | 2.9396 | 1.04034 | | |
| | Doctorate Degree | 2.8567 | .72831 | | |
| Regulation Complexity | High School Diploma | 3.1835 | 1.48824 | 2.484 | .036* |
| | College Degree | 4.1634 | .85106 | | |
| | Professional Degree | 2.8937 | 1.02378 | | |
| | Bachelor's Degree | 3.6868 | .68290 | | |
| | Master's Degree | 3.7160 | .93147 | | |
| | Doctorate Degree | 3.5034 | .74590 | | |
| Process Adaptation | High School Diploma | 4.0665 | 1.42582 | 1.395 | .233 |
| | College Degree | 3.8814 | .65376 | | |
| | Professional Degree | 4.0677 | 1.38044 | | |
| | Bachelor's Degree | 3.8515 | .68283 | | |
| | Master's Degree | 3.5605 | .86357 | | |
| | Doctorate Degree | 4.1461 | .80412 | | |

*. The mean difference is significant at the 0.05 level

The fact that staff training mean and regulation complexity mean for the respondents with a college degree (M= 3.3270; SD= 1.03496) and (M= 4.1634; SD= .85106) respectively is higher than the other groups is just a mere coincidence, since significance is very weak and not differences have been found between the groups. From the statistical point of view since there are no significant results it can be established that for the results in general it does not matter the respondent's level of education since the staff training will have to be carried out anyway and the regulation complexity will not become less complex.

**ANOVA test 7,** *The respondent's field of education versus compliance costs, staff training, regulation complexity and process adaptation.* Table 5.14 shows these relationships that was measured and reports statistically not significant differences. Therefore, the analysis suggests that the null hypothesis 8 is accepted.

*$H_o$8: There is no significant relationship between respondent's field of education versus compliance costs, staff training, regulation complexity and process adaptation.*

Table 5.14 Factor unity ratings, standard deviation, and significance levels depending on the respondent's field of education**.**

| Factors | Respondent's field of education | *M* | *SD* | *F* | *Sig.* |
|---|---|---|---|---|---|
| Compliance Costs | Business & Economics Sciences | 3.57 | .83 | 1.193 | .319 |
| | Engineering & ICT sciences | 3.66 | .85 | | |
| | Health schiences | 3.44 | .86 | | |
| | Law sciences | 4.30 | .61 | | |
| | Other | 3.86 | .85 | | |
| Staff Training | Business & Economics Sciences | 2.76 | 1.03 | 2.125 | .084 |
| | Engineering & ICT sciences | 2.98 | .81 | | |
| | Health schiences | 2.99 | .99 | | |
| | Law sciences | 4.20 | .61 | | |
| | Other | 3.02 | 1.41 | | |
| Regulation Complexity | Business & Economics Sciences | 3.61 | .99 | 1.640 | .171 |
| | Engineering & ICT sciences | 3.91 | .79 | | |
| | Health schiences | 3.38 | .83 | | |
| | Law sciences | 4.15 | .81 | | |
| | Other | 4.09 | .93 | | |
| Process Adaptation | Business & Economics Sciences | 3.54 | .83 | 1.739 | .148 |
| | Engineering & ICT sciences | 3.86 | .78 | | |
| | Health schiences | 4.13 | .68 | | |
| | Law sciences | 4.07 | .64 | | |
| | Other | 3.84 | 1.02 | | |

Other (architecture, design, history, tourism, journalism)

The researcher thought it will be worth also testing whether there was a significant relationship between *the respondent's field of education versus compliance costs, staff training, regulation complexity and process adaptation*. From the statistical point of view since there are not significant results it can be established that for the results in general it does not matter the respondent's field of education in terms of compliance costs, staff training, regulation complexity and process adaptation. Compliance costs will be what they must be, staff training will have to be carried out anyway, regulation complexity is not related because it is not going to become less complex depending on the respondent's field of education and the same with process adaptation. So, the main conclusion is that it does not matter the respondent's field of education since it is not going to significantly affect compliance costs, staff training, regulation complexity and process adaptation.

## 5.5. Independent Sample T-Test

Gender was analyzed using Independent Sample T-Test since it consists of only two categories. The sample consists of 79 males and 28 females, and the test was run to find out if there were significant difference in their perceptions between males and females' respondents in terms of GDPR compliance costs, staff training, regulation complexity and process adaptation.

As presented on table 5.15 no significant difference is found in their perceptions in terms of GDPR challenges. This means that perceptions on GDPR compliance costs, staff training, regulation complexity and process adaptation do not depend on gender and the differences on each of the factors may just be a coincidence. Therefore, the analysis suggests that the null hypothesis 9 is accepted.

*$H_o$9: There is no significant difference between males and females in their perceptions of GDPR compliance costs, staff training, regulation complexity and process adaptation.*

Table 5.15 T-Test - Independent Samples Test.

| Factor | Gender | Mean | SD. | F. | Sig. |
|---|---|---|---|---|---|
| MeanCost | Male | 3.5591 | .89157 | .354 | .553 |
| | Female | 3.6071 | .86092 | | |
| MeanStaff | Male | 2.8177 | 1.02466 | 1.516 | .221 |
| | Female | 2.7381 | 1.22510 | | |
| MeanRegul | Male | 3.6797 | .88606 | 1.250 | .266 |
| | Female | 3.7143 | .99934 | | |
| MeanProcess | Male | 3.8194 | .80014 | 2.457 | .120 |
| | Female | 3.7381 | .95735 | | |
| | Male | | | | |

## 5.6. Correlation analysis

A correlation analysis (scale) descriptive statistic was carried out and the means of the constructs are presented on Table 5.16.

Table 5.16 Correlation analysis (scale) descriptive statistics.

**Descriptive Statistics**

| | Mean | Std. Deviation | N |
|---|---|---|---|
| MeanCost | 3.5717 | .87987 | 107 |
| MeanStaff | 2.7969 | 1.07524 | 107 |
| MeanRegul | 3.6888 | .91232 | 107 |
| MeanProcess | 3.7981 | .84015 | 107 |

Table 5.17. Pearson's R Correlation Coefficient.

**Correlations**

| | MeanCost | MeanStaff | MeanRegul | MeanProcess |
|---|---|---|---|---|
| MeanCost | 1 | .439** | .183 | .204* |
| | | .000 | .059 | .035 |
| | 107 | 107 | 107 | 107 |
| MeanStaff | .439** | 1 | .406** | .416** |
| | .000 | | .000 | .000 |
| | 107 | 107 | 107 | 107 |
| MeanRegul | .183 | .406** | 1 | .388** |
| | .059 | .000 | | .000 |
| | 107 | 107 | 107 | 107 |
| MeanProcess | .204* | .416** | .388** | 1 |
| | .035 | .000 | .000 | |
| | 107 | 107 | 107 | 107 |

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

The researcher carried out a Pearson’s correlation 2-tailed significant test for the sample of 107 respondents. From the Pearson’s R Correlation Coefficient matrix results presented in Table 5.17, the researcher makes the following observations on the relationship between the independent variables mean compliance cost, mean staff training, mean regulation complexity and mean process regulation:

1.- Between compliance costs and staff training there is a moderate positive correlation with an acceptable level of error and vice versa. Between compliance costs and regulation complexity there is no correlation and between compliance costs and process adaptation there is a weak positive correlation with an acceptable level of error and vice versa.

2.- Between staff training and compliance costs there is a moderate positive correlation with an acceptable level of error. Between staff training and regulation complexity there is a moderate positive correlation with an acceptable level of error. Between staff training and process adaptation there is also a moderate positive correlation with an acceptable level of error.

3.- Between regulation complexity and compliance costs there is a weak positive correlation with an acceptable level of error. Between regulation complexity and staff training there is a moderate positive correlation with an acceptable level of error. Between regulation complexity and process adaptation there is also a moderate positive correlation with an acceptable level of error.

4.- Between process adaptation and compliance costs there is a weak positive correlation with an acceptable level of error. Between process adaptation and staff training there is also a moderate positive correlation with an acceptable level of error. Between process adaptation and regulation complexity there is also a moderate positive correlation with an acceptable level of error.

The next step is to determine which of these variables is qualified to be included in the regression analysis which are significant and have at least moderate relationship between variables. In this research for the given sample, only compliance costs, staff training and process adaptation qualify for further regression analysis with the qualitative variable month to achieve compliance.

## 5.7. Regression analysis

The aim of the correlation analysis was to check how the scale variables relate to each other. The next step was to build regression models and hypothesis to understand the variables relationships found in the correlation analysis and to find out which variables are dependent and which variables are independent. For the regression test a linear regression analysis was performed on SPSS.

For interpreting the results for each of the four linear regression models table 5.20 has been created which includes the extracted relevant values from the model summary, ANOVA and Coefficients table.

**Model 1.-** Costs = a + $b_1$Staff Training + $b_2$Regulation Complexity+$b_3$Process

The hypothesis 10 to be tested are as follows:

- $H_{o1}$: Compliance costs are not affected by staff training, regulation complexity and process adaptation
- $H_{A1}$: Compliance costs are affected by staff training, regulation complexity and process adaptation

As presented on table 5.18 the R-value is .440, the R square .194 and the adjusted R square .170. The Sig. value is .000 which is less than the 0.05 making the result significant. The value for F-ratio is 8.245 which is greater than 1 for F ratio yield efficient model. The Sig. values of the coefficients compliance costs and staff training is .000 which is less than the acceptable value of 0.05. With a 1% increase in the staff training, the mean cost will increase by 351 (B value). Moreover, since the Sig. values of the coefficients regulation complexity and process adaptation are .989 and .799, respectively then the null hypothesis 10 is accepted partially. Costs = 2.491 + .351 x Staff Training.

Although, the study research carried out by Tikkinen-Piri et al. (2018) claim that GDPR will demand substantial financial and human resources and that will also be necessary to offer adequate training to employees to deal with the GDPR requirements. They do not go further within the research in terms of finding whether there is any relationship between compliance costs, staff training and regulation complexity. The author finds that there is a logic in the relationship between compliance costs and staff training since it is challenging to train existing and new employees about GDPR requirements and the startups recognizing the complexity of the regulation has had to invest time and money in training an existing member of the staff or recruiting a new one to dedicate mainly to GDPR compliance which also includes the training of the staff Bräutigam (2016). Some other startups have had to invest in GDPR consultants or DPOs. The role of DPO within the organization covers a wide range of tasks as required by Article 39 of the GDPR. The main tasks are to monitor, inform and advise the controller or processor on GDPR compliance, provide advice such as data protection impact assessments, cooperate with the supervisory authority and act as a contact point, as well as provide training and awareness raising.

Table 5.18 Summary, ANOVA and Coefficient

| Model | | R | R Square | Adjusted R Square | F | Sig. | B | Sig. |
|---|---|---|---|---|---|---|---|---|
| 1 | Model Summary | .440a | .194 | .170 | | | | |
| | ANOVA | | | | 8.245 | .000b | | |
| | Coefficients | | | | | | | |
| | (Constant) | | | | | | 2.491 | .000 |
| | MeanStaff | | | | | | .351 | .000 |
| | MeanRegul | | | | | | -.001 | .989 |
| | MeanProcess | | | | | | .027 | .799 |

a. Predictors: (Constant), MeanProcess, MeanRegul, MeanStaff

b. Dependent Variable: MeanCost

**Model 2.-** Staff training = a + $b_1$Regulation + $b_2$Process

The hypothesis 11 to be tested are as follows:

- $H_{o1}$: Staff training is not affected by regulation complexity and process adaptation.
- $H_{A1}$: Staff training is affected by regulation complexity and process adaptation.

As presented on table 5.19 the Sig. values of the coefficients regulation complexity and process adaptation is .002 and .001, respectively which is less than the acceptable value of 0.05.

With a 1% increase in the regulation complexity and process adaptation, the staff training will increase by .340 and .389 (B value), respectively, then the null hypothesis 11 is accepted partially. Staff training = .340 x Regulation + .389 x Process.

Table 5.19 Summary, ANOVA and Coefficient

| Model | | R | R Square | Adjusted R Square | F | Sig. | B | Sig. |
|---|---|---|---|---|---|---|---|---|
| 1 | Model Summary | .493a | .243 | .229 | | | | |
| | ANOVA | | | | 16.735 | .000b | | |
| | Coefficients | | | | | | | |
| | (Constant) | | | | | | **.066** | **.891** |
| | MeanRegul | | | | | | .340 | .002 |
| | MeanProcess | | | | | | .389 | .001 |

a. Predictors: (Constant), MeanProcess, MeanRegul

b. Dependent Variable: MeanStaff

Although, the report research carried out by TrustArc (2018) that underlines as top challenge GDPR complexity, lack of expertise, qualified staff and GDPR technology and tools and the research study carried out by Tikkinen-Piri et al. (2018) that identifies that GDPR will demand substantial human resources and that it will also be necessary to offer adequate training to employees to deal with the GDPR requirements. They do not go further within the research in terms of finding whether there is any relationship between staff training and regulation complexity and process adaptation. The author finds there is a logic in the relationship between staff training and regulation complexity and process adaptation since GDPR is complex and difficult to understand the existing and new employees must be trained about GDPR requirements. Moreover, the fact that the startups need to adapt their existing business model to ensure successful GDPR compliance once these changes have been implemented the staff will also need to be trained to know how to proceed with their daily tasks with the already adapted GDPR compliance business model.

**Model 3.-** Process = a + $b_1$Staff training + $b_2$Regulation + $b_3$GDPR annual spending

The hypothesis 12 to be tested are as follows:

- $H_{o1}$: Process adaptation is not affected by staff training, regulation complexity and GDPR annual spending.
- $H_{A1}$: Process adaptation is affected by staff training, regulation complexity and GDPR annual spending.

As presented on table 5.20 the Sig. values of the coefficients process regulation complexity and staff training are .006 and .003, respectively which is less than the acceptable value of 0.05. With a 1% increase in the regulation complexity and staff training, the process adaptation will increase by .250 and .232 (B value), respectively, then the null hypothesis 12 is accepted partially. Process = 2.159 + .232 x Staff training + .250 x Regulation.

Table 5.20.- Summary, ANOVA and Coefficient

| Model | | R | R Square | Adjusted R Square | F | Sig. | B | Sig. |
|---|---|---|---|---|---|---|---|---|
| 1 | Model Summary | .483a | .233 | .210 | | | | |
| | ANOVA | | | | 10.419 | .000b | | |
| | Coefficients | | | | | | | |
| | (Constant) | | | | | | 2.159 | .000 |
| | MeanRegul | | | | | | .250 | .006 |
| | MeanStaff | | | | | | .232 | .003 |
| | GDPR annual spending (euros) | | | | | | .000 | .577 |

a. Predictors: (Constant), GDPR annual spending (euros), MeanRegul, MeanStaff

b. Dependent Variable: MeanProcess

Although Härting et al. (2021) and Poritskiy et al. (2019) which both recognize process adaptation and employees training as a challenge specially for micro enterprises with less than 10 employees and small enterprises with 10 to 49 employees, both authors do not go further within their research in terms of finding whether there is any relationship between process adaptation and employees training. The author finds there is a logic in the relationship between process adaptation and regulation complexity and staff training since the startups must adapt their existing business model to ensure successful GDPR compliance, a regulation that is of mandatory compliance, complex and difficult to understand and that requires to train their existing and new employees so that they can integrate the GDPR guidelines into their daily work routines.

**Model 4.-** Months to achieve compliance = a + $b_1$Staff training + $b_2$Process + $b_3$Costs + Year Co established

The hypothesis 13 to be tested are as follows:

$H_{o1}$: Months to achieve compliance are not affected by staff training, process adaptation, compliance costs and year company established.

$H_{A1}$: Months to achieve compliance are affected by staff training, process adaptation, compliance costs and year company established.

As presented on table 5.21 the Sig. value is .022 which is less than the 0.05 making the result significant. With a 1% increase in the process adaptation, the months to achieve compliance will increase by 2.854 (B value). Moreover, since the Sig. values of the coefficients staff training, compliance costs and regulation complexity are .440, .744 and .591, respectively; the null hypothesis is partially accepted. Months to achieve compliance = 2.854 x Process.

Table 5.21.- Summary, ANOVA and Coefficient

| Model | | R | R Square | Adjusted R Square | F | Sig. | B | Sig. |
|---|---|---|---|---|---|---|---|---|
| 1 | Model Summary | .324a | .105 | .070 | | | | |
| | ANOVA | | | | 2.987 | .022b | | |
| | Coefficients | | | | | | | |
| | (Constant) | | | | | | -6.748 | .259 |
| | MeanProcess | | | | | | 2.854 | .032 |
| | MeanStaff | | | | | | .870 | .440 |
| | MeanCost | | | | | | .401 | .744 |
| | MeanRegul | | | | | | .650 | .591 |

a. Predictors: (Constant), MeanRegul, MeanCost, MeanProcess, MeanStaff

b. Dependent Variable: Months to achieve compliance.

The author finds there is a logic in the relationship between months to achieve GDPR compliance and process adaptation since those startups that had data privacy security integrated in their business model or those startups that have GDPR by design from the start will become GDPR compliance in a shorter term than those startups who did not Babu et al. (2021).

Those startups who did not have data privacy security integrated in their business model will require more months to achieve GDPR compliance since they will have to adapt much more their existing business model to ensure successful GDPR compliance as Sirur et al. (2018) identified small companies without significant prior emphasis on security felt GDPR compliance was onerous indicating that there was insufficient privacy by design.

## 5.8. Summary

The analysis's results have been described and discussed. Starting with the respondent, company profile and the startups by sectors by describing the demographic profile of the respondents, the number of years the company's respondents have been established, the number of years the respondent has been employed in the company and the weighted frequencies of the respondents by business sectors. Followed by the descriptive statistics analysis, the eight ANOVA test results analysis, the independent sample T-test analysis, the correlation test results analysis and the four regression models analysis results. Finally, the summary of the key research findings concerning the research aim and questions, the results and their implications, the strategy recommendations, the study's limitations, contributions, and proposed recommendations for future research are presented in chapter 6.

# CHAPTER 6 IMPLICATIONS, RECOMMENDATIONS, AND MAIN CONCLUSIONS

## 6.1. Introduction

This chapter will conclude the study by reflecting on the research aim and objectives, discussing the research contribution to the body of knowledge, presenting the practical implications of the research results, detailing the implications of the research for the key stakeholders, presenting policy recommendations, reviewing the research limitations, and proposing recommendations for future research studies.

## 6.2. Reflection on the research aim and objectives

The research aimed to gather data on the startups' respondents personal familiarity with the GDPR, to identify the key challenges faced by technology startups in Catalonia resulting from the enforcement of the GDPR as of May 2018, and if there is an association between these key challenges with compliance costs, regulation complexity, insufficient government support or process adaptation, and the existence or not of a relationship between the challenges and the number and type of employees recruited, size, business sector, year of establishment; as well as GDPR annual spending and time to achieve compliance.

The objective was to collect data to carry out both 'descriptive' and 'inferential' statistical analysis, generalize and draw conclusions from the sample to find out the level of GDPR knowledge of the startups' respondents, to identify a series of quantitative GDPR implementation challenges and the existence or not of a relationship between the challenges and the number and type of employees recruited, size, business sector, year of establishment; as well as GDPR annual spending and time to achieve compliance and also to provide recommendations to help to increase technology startups' awareness in Catalonia to address and overcome the challenges to comply with GDPR and for the Catalan government to support technology startups with challenges of implementing GDPR. Although the results cannot be generalised to all technology startups in Catalonia because of not having reached the required minimum sample size of the population for representativeness, the research questions will be answered based on the Catalonian technology startups that participated in the survey.

In relation to **RQ 1**: How familiar are technology startups in Catalonia with the GDPR?

The literature research highlighted a gap in how familiar Catalan technology startups are with the GDPR, and it was addressed in part A of the questionnaire in which respondents completed eight knowledge questions items with answer options true/false/ I don't know to find out their perceptions and familiarity with the GDPR. The model questionnaire for this part A was adopted from the model presented by the authors (Hartman et al., 2020) which was also used to assess the respondents' existing knowledge and views about data practices. The descriptive statistical analysis showed mixed results in terms of familiarity and understanding of the GDPR: 97,3% of the sample correctly answered a question on the main purpose, and only 30,4% gave correct answers to a question on data portability. These results might be explained by the lack of the respondents' GDPR awareness and insufficient training, which is also evidenced by the research by Tikkinen-Piri et al. (2018). Concerning personal data, respondents appeared most knowledgeable, with more than 7 out of 10 answering these questions correctly. However, concerning open data, respondents were least knowledgeable, with 48.2% and 37% answering these questions correctly. These results might be explained by the respondents' lack of knowledge of the type of data that are freely available to everyone to use and republish for their purposes. Three years later, there is still a considerable amount of GDPR lack of familiarity among the technology startups that participated in the survey, reinforcing the need to increase awareness and training in the workplace.

In relation to **RQ 2**: What are the key challenges of the GDPR implementation faced by technology startups in Catalonia?

The literature research helped the author decide on an appropriate structure for the conceptual framework and highlighted a gap in the challenges faced by startups from enforcing the GDPR as of May 2018. Thirty-two challenges were identified related to GDPR and grouped into four constructs/categories: Compliance costs, regulation complexity, government support and process adaptation. These challenges were also confirmed by the researcher's interviews with three Catalan startups registered in the Agency for Business Competitiveness (ACCIÓ) and addressed in part B of the questionnaire in which 107 respondents completed thirty-two scale questions items with a five-point Likert scale, ranging from '1.- strongly disagree' to '5 – strongly agree' to identify the challenges they have faced from the enforcement of the GDPR as of May 2018. Respondents appeared most concerned with the risk of being accountable when there are no clear GDPR guidelines to follow and with the complexity of executing periodic audits to ensure that all processes comply with GDPR. Respondents are also concerned with difficulty in developing a cyber incident response plan, the cost of investing in GDPR consultants and the lack of information support from the government bodies concerning GDPR.

In relation to **RQ 2.1**: Are the key challenges associated with compliance costs, regulation complexity, insufficient government support or process adaptation?

This research question was also addressed in part B of the questionnaire, and the key challenges were confirmed by the descriptive statistical analysis results of the mean and standard deviation for each scale question and construct. The resulting insufficient government support is the highest challenge for the Catalonian startups that participated in the survey because they agree that there is a lack of information support and practical guidelines from the government bodies about GDPR and to follow standard procedures correctly, respectively. They also agree that GDPR does not provide any recommendations regarding the use of technology to help them to comply with its requirements and that GDPR does not provide any specific instruments or tools for them.

In relation to **RQ 2.2**: Is there any relationship between the challenges faced by technology startups and the number and type of employees recruited, size, business sector, year of establishment, GDPR annual spending and time to achieve compliance?

This research question was addressed in parts B and C of the questionnaire, the last part dedicated to the company and respondent profile. The researcher carried out a correlation analysis, a one-way ANOVA test and a linear regression analysis to explore the relationship between the four challenges, compliance costs, regulation complexity, insufficient government support and process adaptation, and the variables number of new employees recruited, responsible for GDPR compliance, size, business sector, GDPR annual spending, year of establishment, time to achieve compliance, respondent's role, level of education and field of education.

For compliance costs, a significant relationship with the number of new employees recruited to facilitate GDPR compliance was found because a significance level of less than .005 was found, and the post hoc test was performed to find group differences. However, the compliance cost increase when a company hires between 1 to 5 employees rather than when it does not hire any employees could be due to the fact of hiring a DPO or a third-party consultant who may not be within the payroll of the company but rendering services through a services agreement. Therefore, these results may not be conclusive and will form part of the limitations of this research.

A significant relationship with the startup business sector was found for compliance costs, and the post hoc test was performed, finding group differences. Compliance costs were less challenging for those startups within the ICT business sector compared to those within the Leisure business sector. There is a logic in the relationship between the startup business sector and compliance costs since those startups that had data privacy security integrated into their business model or those startups that have GDPR by design from the start will become more GDPR compliance cost-effective than those startups who did not Babu et al. (2021).

For regulation complexity and staff training, no relationship with the variables was found because there are no significant results; therefore, regulation complexity is not related to any of the variables because it is not going to become less complex depending on the variables and the same with staff training which will have to be carried out anyway.

Only a significant relationship with the respondent's role was found for process adaptation because a significance level was found, and the post hoc test was performed to find group differences. For example, those respondents with a role as founder or member of the board of directors perceived less of a challenge process adaptation than those with a role in the company as CEO, CFO, CMO or managing director. The reason for it could be that the founder, who in startups is usually also a member of the board of directors, perceives process adaptation as less of a challenge because it is generally seen as the competence or responsibility of the CEO, CFO, CMO and managing director Picken (2017).

In relation to **RQ 3**: What recommendations can be provided to help technology startups in Catalonia overcome the challenges resulting from the GDPR?

This research question is further addressed in this chapter with the help of the literature research, the researcher's interviews with three Catalan startups registered in the Agency for Business Competitiveness (ACCIÓ) and the questionnaire.

The recommendations, in general, will be the following:

- To invest in hiring the services of an expert in GDPR to assess the company's actual state in terms of GDPR compliance and to follow the advice. Without the advice of an expert regularly, the startups will not be able by themselves to deal with the complexity of the regulation and with the GDPR training that is required to be given to the employees.

- It is crucial that the IT experts of the company work together with the GDPR expert to facilitate the GDPR compliance process in terms of adapting the existing business model of the organisation, providing the company's stakeholders access to their data, to have established a straightforward procedure to delete an individual's data, to ensure the portability of personal data, to perform the processing if a data subject opts out automated process, to quickly know where all the personal data of their stakeholders is stored, to apply emergent technologies to achieve better compliance with GDPR and to execute periodic audits to ensure that all processes are compliant with GDPR.

- IT experts who lack expertise on the legal aspects of GDPR will require the assistance of a GDPR expert such as a DPO, a CPO or a third-party consultant expert. Therefore, it is essential that when appointing a person as GDPR responsible, this person have sufficient expertise on GDPR.

- It is also essential to hire the services of a cybersecurity expert to have implemented a cyber incident response plan to comply with the 72 hours for the startup to report the incident.

## 6.3. Contribution to the body of knowledge

The study contributes to research and practice in several ways, and the unique and significant contribution of the research is outlined below:

From the research perspective, it is among the first empirical studies on Catalan technology startups' GDPR compliance efforts and contributes to the literature on data privacy research. It analyses and discusses the prior literature on the GDPR challenges faced by companies, and by using the academic search engine, Scopus decides on an appropriate structure for the framework and aggregates the main challenges in implementing the GDPR. This synthesis makes it possible to identify and evaluate the relative relevance and effect of the challenges faced by the startups in Catalonia. This information is also relevant to understanding how the startups in Catalonia look at the challenges of implementing the GDPR. Additionally, this study provides relevant theoretical input and research implications, summarizing the key challenges in implementing the GDPR. Finally, this study is among the first empirical studies on technology startups' GDPR challenges that have conducted advanced statistical analysis techniques starting with ANOVA, followed by independent sample T-test, correlation analysis and regression analysis, which supports the findings.

From the practical perspective, it makes a practical contribution by providing recommendations that help increase technology startups' awareness of the different types of challenges they must address and overcome to comply with GDPR. The thesis contributes to the Catalan government boosting startup GDPR implementation. Proper understanding of GDPR implementation helps companies to be better prepared for the legal compatible EU structure Knill et al. (1998). The proper understanding of GDPR implementation challenges and factors and their application enhances the proper usage of norms and thus conveys the Catalan economy's more sustainable economic development. The thesis also raises awareness of a better explanation and understanding of the current GDPR implementation ambiguity whereby the EU policymakers and hence the parliament can apply different strategies to help companies adapt adequately Toshkov (2010).

## 6.4. Practical implications and recommendations

The literature research shows that the previous studies carried out on the GDPR challenges faced by technology startups are minimal. For example, in their study, NOR. On the other hand, in their research study, Poritskiy et al. (2019) adopt a quantitative methodology based on a survey conducted with 286 Portuguese IT companies of all sizes which dealt with the enforcement of the GDPR. However, it does not examine the types of challenges at each stage of GDPR adoption and does not consider the specifics of the activities undertaken by each company. Therefore, this study adds to the field of GDPR challenges faced by technology startups in Catalonia by making the Catalonian technology startups that participated in the survey realise the need to increase GDPR awareness and training in the workplace and become aware of the existing implementation challenges and how relevant it is to hire the services of a GDPR expert and a cybersecurity expert or to train an existing team who already knows how the company operates to comply with GDPR since the benefits outweigh the costs.

This study also adds to the GDPR challenges faced by technology startups in Catalonia by making the Catalan government aware of their vital role in boosting GDPR implementation among the technology startups. They are rising in Catalonia and often work on the development and application new technologies (AI/ML, blockchain, IoT, among others). However, small attention has been paid to the way startups working at the forefront of the latest technologies deal with privacy Norval et al. (2021). Already Norval et al. (2021) argued that the actions of technology startups have the potential for far-reaching implications in the broader data protection landscape, potentially with systemic consequences and that addressing problems sooner rather than later plays a major part in combating bad practices and misunderstandings is used to improve privacy practices more broadly.

Proper understanding of the GDPR challenges helps organisations to be better prepared to be GDPR compliant. Furthermore, the proper understanding of GDPR implementation challenges and factors and its application enhances the proper usage of norms and thus conveys a more sustainable economic development of the Catalan economy. Finally, the thesis raises awareness of a better explanation and understanding of the current GDPR implementation ambiguity. As a result, the EU policymakers and parliament can apply different strategies to help companies adapt adequately.

### 6.4.1 Implications for key stakeholders

The GDPR defines a comprehensive set of rules which involves and affects major stakeholders and their relationships. Huth et al. (2018) come up with five key stakeholders in the GDPR by defining entities with at least three relationships with other entities (active or passive). The five main stakeholders are the data subject whose personal data is being collected and whose rights are strengthened by the GDPR, the controller responsible for lawful data processing, the processor not involved in a direct communication with the data subject, the data protection officer as an entity within a processing or control body and the national supervisory authority Huth et al. (2018). Huth et al. (2018) evidenced that the centre of activity in the GDPR revolves around the data subject and the controller and between the controller and the supervisory authority and concludes that the leading actor in the GDPR is the data controller.

This research study is useful for the controller, the processor, the data protection officer, the supervisory authority, and regional government's agency authorities, but it is most useful for the data controller and the national supervisory and regional government agency authorities specially for the Catalan technology companies and for ACCIÓ and Barcelona Activa**.** In Spain the Data Protection Authority (DPA) is the Agencia Española de Protección de Datos (AEPD) and in Catalonia is the Autoritat Catalana de Protecció de Dades (APDCAT). The study concentrates on the AEPD since the APDCAT has not, within their competencies, the private companies which do not carry out activities for the government.

The implications for the two main key stakeholders in this research, technology startups and the government are presented as follows and shown under figure 6.1.

**Implications for data controllers: technology startups.**

Technology startups should be more proactive on privacy approaches. In general, they seem to benefit from becoming more aware of the objectives and intentions of the GDPR. There is more that technology startups could do to advocate the regulation as an opportunity to evaluate, consider and implement processes to improve privacy practices Norval et al. (2021). If it is not clear how to achieve compliance, advice should be sought (or other actions taken) to ensure they are best able to demonstrate their ability to meet their GDPR obligations. If the appropriate course of action is inherently unclear, there is some evidence that companies should not pursue any particular path until they have a clearer strategy for coping with the privacy issues at stake Norval et al. (2021). This may include the introduction of alternative technologies or technical approaches, such as the need to increase awareness and training in the workplace.

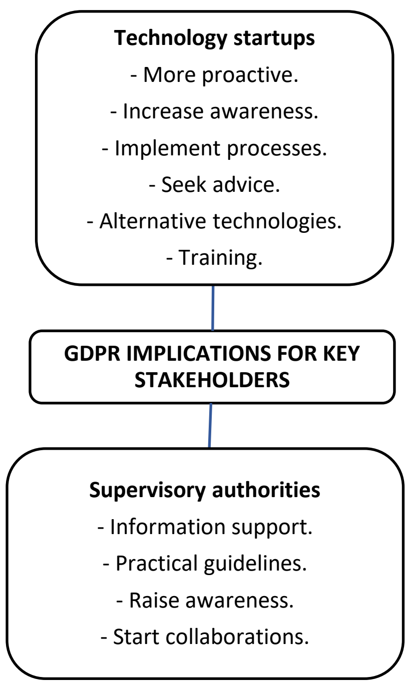



Fig. 6.1 GDPR implications for key stakeholders.

**Implications for the national supervisory authority: the government**

Based on the questionnaire results, the Catalonian technology startups that participated in the survey claim a lack of information support and practical guidelines on GDPR compliance from the government bodies. Information support and practical guidelines that need to be specifically tailored for technology startups. Consequently, the AEPD has failed to reach out to those startups that participated in the survey about GDPR compliance. There is an apparent extent to how much the AEPD can meet the needs of startups in Catalonia, and the following questions remain:

- How to reconcile the AEPR's position with the disappointment of the support received by the Catalonian startups that participated in the survey? and
- How can the AEPD aid the Catalonian startups that participated in the survey with precise and targeted guides that could ease their GDPR journey?

For the answer to these questions, it will be considered the three interviews carried out with three tech startups in Catalunya. There is good reason to believe that ACCIÓ could play an important role in supporting the AEPD to aid the startups in Catalonia. ACCIÓ is the Catalan government agency for business competitiveness and is part of the Ministry of Economy and Employment (ACCIÓ Strategy and Competitive Intelligence Unit, 2022a). It is the organisation open to the public that works to contribute to the transformation of Catalan companies. It works with public and private institutions to build tomorrow's business today. ACCIÓ is driven by three main objectives: to increase the productivity of Catalan companies, to accompany them in their transformation and global positioning challenges, and finally to strengthen Catalonia's attractiveness as a destination for high-quality foreign investments. These goals should have a positive effect on economic growth and job creation (ACCIÓ Strategy and Competitive Intelligence Unit, 2022a).

In terms of the benefits ACCIÓ can bring, first, ACCIÓ engages in activities with interests that overlap with the obligations of the AEPD to increase understanding of the GDPR among startups. There seems to be an issue of the decentralised information especially between the two agencies. Nevertheless, close cooperation between the AEPD and ACCIÓ could lead to a co-creation of practical guidelines and relevant information and recommendations for startups.

Second, ACCIÓ has open channels of communication with startups that can be leveraged to raise understanding of GDPR and facilitate compliance. For example, one of the standard channels can be the member mailing list. Otherwise, the AEPD could also collect and use the startup contact details for dissemination of guidance materials since the model of 'we publish it, you find it' is concerning guidance it appears not to be effective (Cochrane et al., 2020).

In the case of the startups in Barcelona, Barcelona Activa could also cooperate with ACCIÓ and the AEPD. Barcelona Activa is Barcelona City Council's economic development agency. It supports Barcelona entrepreneurs and new startups from the business idea stage to consolidation by offering business advice, training, spaces, connection to the entrepreneurial ecosystem and access to finance needed to develop successful companies.

Practical guidance, yet not necessarily legally binding compliance advice, is essentially what startups in Catalonia are looking for, which means that a close and cooperative interaction between the AEPD and the startups based on vagueness will not be appreciated by the startups. A collaboration between the AEPD and ACCIÓ or between the AEPD and the startups will require financial, human resources and structures to facilitate the initial collaboration, resources that the European Union could partially fund. A collaboration between the AEPD and ACCIÓ will provide an opportunity to quickly and effectively understand the unique needs of startups across a range of technology industries.

In Europe, some of the data protection authorities have already started to work more closely and proactively with certain associations, such as the Belgian DPA, which launched an awareness-raising project with associations representing the fintech industry in Belgium ("Belgium Data Protection Authority," n.d.) or the Italian DPA who has been collaborating with SME associations in Italy and Bulgaria within the SME DATA II project, which aims to improve the practical application of the GDPR through awareness raising, multiplication of training and sustainable capacity building for SMEs ("SMEDATA II Poject," n.d.).

## 6.4.2 Policy recommendations

From the descriptive statistical analysis results of the mean and standard deviation for each scale question and construct, the insufficient government support came up as the highest challenge for the Catalonian startups that participated in the survey. This opens the question of what consists of government support.

Art. 51 of the GDPR states that the primary responsibility of Data Protection Authorities (DPAs) concerns the oversight and reliability of their application 'to defend the fundamental rights and freedoms of individuals with respect to processing and to enable the free flow of personal data within the Union' (Cochrane et al., 2020). To achieve this goal, art. 57 of the GDPR lists 22 tasks from enforcers, ombudsmen, auditors, advisers to policy advisors, negotiators, and educators (Cochrane et al., 2020).

To help in a generalised way the compliance of managers, the AEPD has published, since the approval of the GDPR, numerous guides, help manuals and designed free applications available on its website specifically Facilita-Emprende (Agencia Española Protección de Datos, n.d.), which facilitate those responsible for and in charge of the startup of its activity in compliance with the data protection regulations and the evaluation of the risks generated. Likewise, the AEPD makes available to everyone on its website a catalogue of frequently asked questions where you can find answers to the most common problems detected in the application and compliance with data protection regulations. In addition, a relevant supporting tool known in Spanish as Facilita is designed for companies that process low-risk personal data, and it is about creating the minimum documents required for GDPR compliance.

The Instruction (*Instruction 1/2021, of November 2, of the Spanish Data Protection Agency, which establishes guidelines regarding the advisory function of the Agency, in accordance with Regulation (EU) 2016/679, of the European Parliament and of the Council of April 27, 2*, n.d.) in its third preamble states that *" (…) The AEPD will not develop individualised consultative functions aimed at controllers and processors, because it is not provided for in the RGPD or the LOPDGDD. Furthermore, it is not consistent with the principle of proactive responsibility. It may* *generate a perception of a lack of impartiality when the AEPD must exercise its powers of investigation and supervision over treatments in which it has previously performed an advisory or consultative function.*

*On the other hand, it is the reiterated criterion of this Agency not to attend to queries that may be raised by law firms or consultants whose functions are, precisely, the interpretation of the law and advice to their clients. (…) to help in a general way the compliance of those responsible and in charge, the AEPD has published, since the approval of the RGPD, numerous guides, help manuals and designed free applications and available on its website (www.aepd.es), which facilitate the responsible and in charge of the startup of its activity concerning data protection regulations and the evaluation of the risks generated. Likewise, the AEPD makes available to everyone on its website a catalogue of frequently asked questions where answers can be found to the most common problems detected in the application and compliance with the data protection regulations (…)."*

For the construct of government support, the highest mean, 4.0104, is for the component that there is a risk of being accountable when there are no clear GDPR guidelines to follow. As is well known, the GDPR is a principle-based regulation that is technology-neutral and often criticised for being too vague and triggering legal uncertainty (Härting et al., 2021). It appears that if the measures for supporting startups by the Catalonian government are in place, why are the technology startups still experiencing difficulties, what is missing and what might be improved? There is a role for the government in exploring more innovative support mechanisms, and regulatory sandboxes already being used within the financial sector are an example of what the Catalonian government can do for the technology startups Finck (2018). A regulatory sandbox is a formal regulatory initiative to test innovation on a time and scale limited basis in the live market to determine the appropriate regulatory treatment/status before the innovation can be fully deployed in the marketplace. The use of regulatory sandboxes are suitable mechanisms to help the technology startups from different sectors, finance, healthcare, legal services, aviation, transport and logistics, and energy, often including the application of new, emerging technologies – such as artificial intelligence (AI) and blockchain/distributed ledger technologies

(DLT) – or the innovative application of existing technologies (Union, 2020), to test their innovations which was already noted back in November 2020 through the conclusions of the European Council on regulatory sandboxes and experimentation clauses, which advocate for them as instruments for an innovation-friendly, future-proof and resilient regulatory framework that meets and underlines the disruptive challenges of the digital age (Truby, Brown, Ibrahim, & Parellada, 2022), so that the EU can emerge stronger from the COVID-19 crisis, which has had a severe impact on the majority of businesses in the EU, especially small and medium-sized enterprises (SMEs), including micro-enterprises and startups (Union, 2020), need the EU regulatory framework to be as competitive, effective, efficient, coherent, predictable, innovation-friendly, future-proof, sustainable and resilient as possible (Union, 2020). It needs to be evidence-based and has to protect and support citizens and businesses in the context of a fully functioning EU Single Market without imposing new unnecessary burdens and while reducing existing burdens (Union, 2020). Already in the proposition for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain legal provisions of the union (European Parliament and the Council of the European Union, 2021), the regulatory sandboxes are regulated under article 53 (1) "AI regulatory sandboxes established by one or more Member States competent authorities or the European Data Protection Supervisor shall provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan. This shall take place under the direct supervision and guidance by the competent authorities with a view to ensuring compliance with the requirements of this Regulation and, where relevant, other Union and Member States legislation supervised within the sandbox." AI goals include regulatory sandboxes, fostering AI innovation by establishing controlled and safe experimentation and testing environments in the advancement and pre-commercialization phases, ensuring legal certainty for innovators and oversight and interpretation of emerging opportunities by those in charge public authorities to improve risks and effects of AI use and expedite market access, comprising by removing obstacles for small and medium-sized enterprises (SMEs) and startups (European Parliament and the Council of the European Union, 2021).

## 6.5. Research limitations

The following limitations were identified in relation to the research:

- Lacking well-documented previous studies in the same evolving and narrow field.

- Difficulty in the data collection. The heavy workload and lack of personnel of the startups and the COVID pandemic crisis limited the number of responses since many were concentrating their efforts on applying for funding from government institutions, working with minimum personnel, and others had to close their activity.

- The results cannot be generalised to all startups in Catalonia because of not reaching the required minimum sample size for representativeness; 116 responses were collected compared to the 314 needed to reach the sample size. Therefore, since the sample size does not represent the population, it is impossible to generalise the finding for all startups in Catalonia and only make inferences about the respondents (survey participants). Therefore, other researchers must base the same study on a larger sample size to produce more accurate results.

- The mobility and food tech sectors that received only two respondents were not considered for the ANOVA test business sectors. Therefore, other researchers must base the study on a larger sample size that receives sufficient respondents from each technology sector to conduct the ANOVA test.

- The Startup Act that came into force on the 22nd of December 2022 provides a startup definition. Still, this study considers the definition of a startup provided by ACCIÓ since the researcher uses the data base provided by ACCIÓ, the theoretical framework was defined and the data was collected from May 2021 to November 2021. Therefore, other researchers must base the study on the definition of startup provided by the Startup Act.

## 6.6. Future research

- To explore the challenges for ACCIÓ and Barcelona Activa for engaging to offer guidance for Catalan technology startups. The researcher has in mind to conduct qualitative research via interviews with a representative group of people from these two different Catalan institutions to produce recommendations.

- To explore the challenges for the Catalan, the rest of the Spanish and European Union technology startups in implementing GDPR by reaching the required minimum sample size for representativeness. The present research aims, and objectives are to explore the challenges and any relationship among them and produce recommendations.

- To explore the challenges for the AEPD and institutions to offer guidance for Spanish and European Union technology startups. This research could involve representatives from the AEPD and other Spanish regional institutions to explore the challenges and relationships among them and produce recommendations.

- To explore whether it has been more of a challenge for the US technology startups than for the EU technology startups or vice versa in terms of GDPR implementation and compliance. Researchers could conduct a qualitative or quantitative research study using the challenges already found in the present research and the variables also identified to explore the challenges, any relationship among them and produce recommendations.

## 6.7. Summary

A reflection on the research aim and objectives has been carried out while answering the research questions based on the Catalonian technology startups that participated in the survey, followed by a discussion of the research contribution to the body of knowledge from the research and practical perspective, presenting the practical implications of the research results, detailing the implications of the research for the key stakeholders, presenting policy recommendations, reviewing the research limitations, and proposing recommendations for future research studies.

## References


ACCIÓ, & Generalitat de Catalunya. (2020). *La ciberseguretat a Catalunya | Píndola tecnològica*. Retrieved March 28, 2023 from https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/eic-la-ciberseguretat-a-catalunya.

ACCIÓ Strategy and Competitive Intelligence Unit. (2022a). *The Agency*. ACCIÓ. Retrieved March 28, 2023 from https://www.accio.gencat.cat/en/accio/agencia/

ACCIÓ Strategy and Competitive Intelligence Unit. (2022b). The ICT-Turisme de Catalunya Cluster is born, made up of 24 companies and agents with a turnover of 253 million euros. Retrieved March 28, 2023, from https://www.accio.gencat.cat/ca/accio/premsa-comunicacio/cercador-premsa-actualitat/article/20220328-neix-cluster-tic-turisme

Agarwal, S. (2016). Towards dealing with GDPR uncertainty. *11th IFIP Summer School on Privacy and Identity Management*.

Agencia Española Protección Datos. (n.d.). *Facilita Emprende*. AEPD. Retrieved March 29, 2023, from https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQ2NDc1NDkxNjgwMTYwNDYxMzM3?updated=true

Ahmed, J., Yildirim, S., Nowostawski, M., Abomhara, M., Ramachandra, R., & Elezaj, O. (2020). Towards blockchain-based GDPR-compliant online social networks: challenges, opportunities and way forward. In *Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC), Volume 1* (113-129). Springer. https://doi.org/10.1007/978-3-030-39445-5_10.

Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, *21*(4), 402-418. https://doi.org/10.1108/DPRG-01-2019-0007.

Babu, M. S., Raj, K. B., & Devi, D. A. (2021). Data security and sensitive data protection using privacy by design technique. In *2nd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing: BDCC 2019* (177-189). Springer. https://doi.org/10.1007/978-3-030-47560-4_14.

Baldwin, A., Birks, M., Mills, J., & Budden, L. (2014). Putting the philosophy into PhD. *Working Papers in the Health Sciences*, 1-4.

Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the ground: driving corporate behavior in the United States and Europe*. MIT Press.

Bankman, J., & Gilson, R. J. (1999). Why start-ups? *Stanford Law Review*, 289-308.

Belgium Data Protection Authority. (n.d.). *Page d'accueil citoyen*. Autorité de protection des données. Retrieved March 19, 2023, from https://www.autoriteprotectiondonnees.be/

Bessen, J. E., Impink, S. M., Reichensperger, L., & Seamans, R. (2020). GDPR and the Importance of Data to AI Startups. *NYU Stern School of Business*. https://dx.doi.org/10.2139/ssrn.3576714

Bräutigam, T. (2016). *What should SME's do to prepare for the upcoming General Data Protection Regulation?* Bird & Bird. Retrieved March 29, 2023, from https://www.twobirds.com/en/insights/2016/global/what-should-smes-do-to-prepare-for-the-upcoming-gdpr

Brodin, M. (2019). A framework for GDPR compliance for small-and medium-sized enterprises. *European Journal for Security Research*, *4*, 243-264.https://doi.org/10.1007/s41125-019-00042-z

Burrell, G., & Morgan, G. (1979). Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life (2nd ed.). Routledge. https://doi.org/10.4324/9781315609751

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy regulation and market structure. *Journal of Economics & Management Strategy*, *24*(1), 47-73.https://doi.org/10.1111/jems.12079.

Catalan Data Protection Authority. (2020). *Artificial Intelligence. Automated decision-making in Catalonia*. Catalan Data Protection Authority.

Cochrane, L., Jasmontaite-Zaniewicz, L., & Barnard-Wills, D. (2020). Data Protection Authorities and Their Awareness-Raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-Size Enterprises. *European Data Protection Law Review*, *6*, 352.https://doi.org/10.21552/edpl/2020/3/6.

Cohen, J. (2013). Statistical power analysis for the behavioral sciences: Routledge.

Cordero, J. A. V. (2021). Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos. *IDP. Revista de Internet, Derecho y Política*, (33). https://doi.org/10.7238/IDP.V0I33.376366.

Cramer, D., & Howitt, D. L. (2004). *The Sage dictionary of statistics: a practical resource for students in the social sciences*. Sage. https://doi.org/10.4135/9780857020123.

Creswel, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage.

Creswell, J.W. (2014). *Research Design: Qualitative, quantitative and mixed Method Approaches.* Sage.

Creswell, Jhone .W, & Clark, V. P. (2017). *Designing and conducting mix method research*. (3rd ed.). Sage.

Crotty, M. J. (1998). The foundations of social research: Meaning and perspective in the research process. *The foundations of social research*, 1-256. Sage.

Cunliffe, A. L. (2010). Retelling tales of the field: In search of organizational ethnography 20 years on. *Organizational Research Methods*, *13*(2), 224-239. Sage. https://doi.org/10.1177/1094428109340041

D'ACCIÓ, U. d'Estratègia i I. ligenci. C. (2022). L'economia digital a Catalunya. *ACCIÓ*. Barcelona.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer law & security review*, *32*(2), 179-194. https://doi.org/10.1016/j.clsr.2016.02.006.

Denman DC, Baldwin AS, Betts AC, McQueen A, Tiro JA. (2018) Reducing "I Don't Know" Responses and Missing Survey Data: Implications for Measurement. Medical Decision Making. 2018;38(6):673-682. Sage. https://doi.org/10.1177/0272989X18785159

Determann, L. (2020). *Determann's field guide to data privacy law: International corporate compliance*. Edward Elgar Publishing.

Dillman, D. A. (2007). *Mail and Internet Surveys: The Tailored Design Method* -- 2007 Update with New Internet, Visual, and Mixed-Mode Guide. Wiley.

Doane, D. P., & Seward, L. E. (2011). Measuring skewness: a forgotten statistic? *Journal of statistics education*, *19*(2). https://doi.org/10.1080/10691898.2011.11889611.

European Commission. (2020). *Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*. European Commission.

European Parliament & Council of the European Union. (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). *European Parliament & Council of the European Union*. Retrieved March 29, 2023, from EUR-Lex website: https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament & Council of the European Union (2021). Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. *European Parliament & Council of the European Union.*

Fähnrich, N., & Kubach, M. (2019). Enabling SMEs to comply with the complex new EU data protection regulation. *Open Identity Summit 2019*.

Field, A. (2009) *Discovering statistics using SPSS* (3rd ed.). Sage.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics.* Sage.

Finck, M (2018). Blockchains and the GDPR. Oxford Business Law Blog Round-Up: Top 20 Most

Read Posts. *Oxford Legal Studies Research Paper*, (4-5) http://dx.doi.org/10.2139/ssrn.3442001

Flick, U. (2022). *An introduction to qualitative research* (7th. ed.). Sage.

Fowler Jr, F. J. (2013). Survey research methods. *Applied Social Research Methods Series* (5th ed.). Sage.

Freitas, M. D. C., & Mira da Silva, M. (2018). GDPR compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*, *3*(4), 1–7. https://doi.org/10.20897/jisem/3941.

Furman, J., & Seamans, R. (2019). AI and the Economy. *Innovation policy and the economy*, *19*(1), 161-191. https://doi.org/10.1086/699936.

George, D. (2011). *SPSS for windows step by step: A simple guide and reference, 17.0 update* (10th ed.). Pearson.

Goldberg, S., Johnson, G., & Shriver, S. (2019). Regulating privacy online: The early impact of the GDPR on European web traffic & e-commerce outcomes. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3421731.

Grundstrom, C., Väyrynen, K., Iivari, N., & Isomursu, M. (2019). Making sense of the General Data Protection Regulation—Four categories of personal data access challenges. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, *6*, 5039–5048. https://doi.org/10.24251/hicss.2019.605.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). Multivariate data analysis (6th ed.). Prentice Hall.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th ed.). Pearson.

Hair, J.F., Hult, G.T.M., Ringle, C.M., & Sarstedt, M. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage.

Härting, R. C., Kaim, R., Klamm, N., & Kroneberg, J. (2021). Impacts of the New General Data Protection Regulation for small-and medium-sized enterprises. In *Proceedings of Fifth International Congress on Information and Communication Technology 2020, London, Volume 1* (238-246). Springer. https://doi.org/10.1007/978-981-15-5856-6_23

Härting, R. C., Kaim, R., & Ruch, D. (2020). Impacts of the implementation of the General Data Protection Regulation (GDPR) in SME business models—An empirical study with a quantitative design. In a*gents and multi-agent systems: Technologies and Applications 2020: 14th KES International Conference, KES-AMSTA 2020, June 2020 Proceedings* (pp. 295-303). Springer. https://doi.org/10.1007/978-981-15-5764-4_27.

Hartman, T., Kennedy, H., Steedman, R., & Jones, R. (2020). Public perceptions of good data management: Findings from a UK-based survey. *Big Data & Society*, *7*(1).

https://doi.org/10.1177/2053951720935616.

Hinz, A., Michalski, D., Schwarz, R., & Herzberg, P. Y. (2007). The acquiescence effect in responding to a questionnaire. GMS *Psycho-Social Medicine*, *4*, *Doc 7*.

Holman, R., Glas, C. A., Lindeboom, R., Zwinderman, A. H., & de Haan, R. J. (2004). Practical methods for dealing with "not applicable" item responses in the AMC Linear Disability Score project. *Health and Quality of Life Outcomes*, (2), 29. https://doi.org/https://doi.org/10.1186/1477-7525-2-29.

Houser, K. A., & Voss, W. G (2018). GDPR: The end of Google and Facebook or a new paradigm in data privacy? *Richmond Journal of Law & Technology*, *XXV*(1), 1–109.

Hurdík, J. (2018). The right to be forgotten in the Czech Republic. *The Lawyer Quarterly*, *8*(4), 423-433.

Huth, D., Faber, A., & Matthes, F. (2018). Towards an understanding of stakeholders and dependencies in the EU GDPR. *Multikonferenz Wirtschaftsinformatik*, *2018-March*, 338–344.

*Instruction 1/2021, of November 2, of the Spanish Data Protection Agency, which establishes guidelines regarding the advisory function of the agency, in accordance with Regulation (EU) 2016/679, of the European Parliament and of the Council of April 27, 2*. (n.d.).

Intelligence Unit, A. strategy and competitive. (2022). *The digital economy in Catalonia sector snapshot*. ACCIÓ.

Jantti, M. (2020). Studying data privacy management in small and medium-sized IT companies. *Proceedings of the 2020 14th International Conference on Innovations in Information Technology, IIT 2020*, 57–62. https://doi.org/10.1109/IIT50501.2020.9299050.

Johnson, D.R., & Creech, J. C. (1983). Ordinal measures in multiple indicator models: A simulation study of categorization error. *American Sociological Review*, (48), 398–407.

Jonas, J. (2018). *Finding the missing link in GDPR compliance.* Senzing.

Kapoor, K., Renaud, K., & Archibald, J. (2018). Preparing for GDPR: helping EU SMEs to manage data breaches. In *2018 AISB Convention: Symposium on Digital Behaviour Intervention for Cyber Security* (pp. 13-20). Society for the Study of Artificial Intelligence and Simulation for Behaviour (AISB).

Kline, R. B. (2011). *Principles and practice of structural equation modeling. Methodology in the social sciences* (3rd ed.). Guilford Press.

Knill, C., & Lenschow, A. (1998). Coping with Europe: The impact of British and German administrations on the implementation of EU environmental policy. *Journal of European Public Policy,* 5(4), 595-614. https://doi.org/10.1080/13501769880000041.

Kollmann, T., Jung, B. P., Kleine-Stegemann, L., Ataee, J., & de Cruppe, K. (2020). *Deutscher startup monitor 2020* (B. D. S. e. V., Ed.). Retrieved February 7, 2023, from https://deutscherstartupmonitor.de/.

Koops, B. J. (2014). The trouble with European data protection law. *International Data Privacy Law*, *4*(4), 250–261. https://doi.org/10.1093/idpl/ipu023.

Kortum, S., & Lerner, J. (2000). Assessing the contribution of venture capital to innovation. *RAND Journal of Economics*, *31*(4), 674-692. https://doi.org/10.2307/2696354.

Krasteva, S., Sharma, P., & Wagman, L. (2015). *The 80/20 rule: Corporate support for innovation by employees*. *International Journal of Industrial Organization*, (*38)*, 32-43. https://doi.org/10.1016/j.ijindorg.2014.11.002.

Krishnaiah, P. R., Mudholkar, G. S., & Subbaiah, P. (1980). 21 Simultaneous test procedures for mean vectors and covariance matrices. *Handbook of statistics*, 1, 631-671. Elsevier. https://doi.org/10.1016/S0169-7161(80)80051-4.

Lachaud, E. (2014). Should the DPO be certified? *International Data Privacy Law*, *4*(3), 189–202. https://doi.org/10.1093/idpl/ipu008.

Landau, S., Leese, M., Stahl, D., & Everitt, B. S. (2011). *Cluster analysis*. Wiley.

Layton, R., & Elaluf-Calderwood, S. (2019). A social economic analysis of the impact of GDPR on security and privacy practices. *2019 12th CMI Conference on Cybersecurity and Privacy, (CMI)* (1-6). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/CMI48017.2019.8962288.

Li, Z. S., Werner, C., & Ernst, N. (2019). Continuous requirements: An example using gdpr. In *2019 IEEE 27th International Requirements Engineering Conference Workshops (REW)* (pp. 144-149). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/REW.2019.00031.

Lindgren, P. (2018). GDPR regulation impact on different business models and businesses. *Journal of Multi Business Model Innovation and Technology*, *4*(3), 241–254. https://doi.org/10.13052/jmbmit2245-456X.434.

Mangini, V., Tal, I., & Moldovan, A. N. (2020). An empirical study on the impact of GDPR and right to be forgotten - Organisations and users perspective. ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security, 37, 1-9. Association for Computing Machinery. https://doi.org/10.1145/3407023.3407080.

Mansfield-Devine, S. (2016). Data protection: prepare now or risk disaster. *Computer Fraud & Security*, *2016*(12), 5–12. https://doi.org/10.1016/S1361-3723(16)30098-7.

Marsh, H. W., Balla, J. R., & McDonald, R. P. (1988). Goodness-of-fit indexes in confirmatory factor analysis: The effect of sample size. *Psychological bulletin*, *103*(3), 391.

Martínez-Martínez, D. F. (2018). Unification of personal data protection in the European Union: Challenges and implications. *Profesional de la Informacion*, *27*(1), 185–194. https://doi.org/10.3145/epi.2018.ene.17.

Mayring, P. (2000). Qualitative content analysis. *Forum Qualitative Social Research, 1(2)*, (Art.20).

McAdam, R., & Galloway, A. (2005). Enterprise resource planning and organisational innovation: a management perspective. *Industrial Management & Data Systems*, *105*(3), 280–290. https://doi.org/10.1108/02635570510590110.

McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, *4*(1), 2053951716686994. https://doi.org/10.1177/2053951716686994.

Morse, J. M. (2003). Principles of mixed methods and multimethod research design. *Handbook of mixed methods in social and behavioral research*, 1, 189-208. Sage.

Nabbosa, V. L., & Iftikhar, R. (2019, August). Digital retail challenges within the EU: fulfillment of holistic customer journey post GDPR. In *Proceedings of the 2019 3rd International Conference on E-Education, E-Business and E-Technology* (pp. 51-58). https://doi.org/10.1145/3355166.3355170

Norman, G. (2010). Likert scales, levels of measurement and the “laws” of statistics. *Advances in health sciences education*, *15(5)*, 625–632. Springer.

Norval, C., Janssen, H., Cobbe, J., & Singh, J. (2021). *Data protection and tech startups: The need for attention, support, and scrutiny. Policy & Internet*. Wiley. https://doi.org/10.1002/poi3.255

Oster, S. M. (1999). Modern competitive analysis. *Oxford University Press Catalogue.*

Pedroso, L. M., Araújo, V. M., Cota, M. P., & Magalhães, J. P. (2021, June). How can GDPR fines help SMEs ensuring the privacy and protection of processed personal data. In *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). Institute of Electrical and Electronics Engineers. https://doi.org/10.23919/CISTI52073.2021.9476620.

Perrault, R., Shoham, Y., Brynjolfsson, E., Clark, J., Etchemendy, J., Grosz Harvard, B., & Niebles, J. C. (2019). The AI index 2019 annual report. In *AI Index Steering Committee, Human-Centered AI Institute*. Stanford university.

Perry, R. (2019). GDPR – project or permanent reality? *Computer Fraud & Security*, *2019*(1), 9–11. Elsevier. https://doi.org/10.1016/S1361-3723(19)30007-7.

Picken, J. C. (2017). From founder to CEO: An entrepreneur’s roadmap. *Business Horizons*, *60*(1), 7–14. Elsevier. https://doi.org/10.1016/j.bushor.2016.09.004.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), 1–20. Oxford Academic. https://doi.org/10.1093/cybsec/tyy001.

Pollman, E. (2019). Startup Governance. *University of Pennsylvania Law Review, 168, 155.* https://dx.doi.org/10.2139/ssrn.3352203

Polykalas, S. E., & Prezerakos, G. N. (2019). When the mobile app is free, the product is your personal data. *Digital Policy, Regulation and Governance*, *21*(2), 89–101. https://doi.org/10.1108/DPRG-11-2018-0068.

Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, *21*(5), 510–524. https://doi.org/10.1108/DPRG-05-2019-0039.

Presthus, W., & Sønslien, K. F. (2021). An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management*, *9*(1), 38–53. https://doi.org/10.12821/ijispm090102.

Ramayah, T., Soto-Acosta, P., Colomo-Palacios, R., Gopi, M., & Popa, S. (2014). Explaining the adoption of Internet stock trading in Malaysia: comparing models. *Asian Journal of Technology Innovation*, *22*(1), 131–151. https://doi.org/10.1080/19761597.2013.873110.

Raschke, P., Küpper, A., Drozd, O., & Kirrane, S. (2018). Designing a GDPR-compliant and usable privacy dashboard. *Privacy and Identity Management. The Smart Revolution. Privacy and Identity 2017. IFIP Advances in Information and Communication Technology*, vol 526. Springer. https://doi.org/10.1007/978-3-319-92925-5_14.

Rhahla, M., Allegue, S., & Abdellatif, T. (2021). Guidelines for GDPR compliance in Big Data systems. *Journal of Information Security and Applications*, *61*(June), 102896. https://doi.org/10.1016/j.jisa.2021.102896.

Ries, E. (2011), *The lean startup: How today's entrepreneurs use continuous innovation to create radically successful businesses*. (1st ed.) Crown Business.

Rodotà, S. (2009). Data protection as a fundamental right. In *reinventing data protection?* (77–82). Springer. https://doi.org/10.1007/978-1-4020-9498-9_3.

Ryan, P., Crane, M., & Brennan, R. (2021, May). GDPR Compliance tools: best practice from RegTech. In *Enterprise Information Systems: 22nd International Conference, ICEIS 2020, Virtual Event, May 5–7, 2020, Revised Selected Papers* (905-929). Springer. https://doi.org/10.1007/978-3-030-75418-1_41.

Sarkar, S., Banatre, J. P., Rilling, L., & Morin, C. (2018, July). Towards enforcement of the EU GDPR: enabling data erasure. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (222-229). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/Cybermatics_2018.2018.00067.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students.* (7th ed.). Pearson.

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research Methods for Business Students Eight Edition. *Qualitative Market Research: An International Journal*.

Saunders, M., & Tosey, P. (2013). *The layers of research design*. Rapport 30 58-9. The

Association for Neuro Linguistic Programming.

Secretaría de Estado de Comunicación. Consejo de Ministros. The Spanish Startup Act 28/2022. *Consejo de Ministros, Energía, Turismo y Agenda Digita*l.

Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2018). An analysis of economic impact on IoT industry under GDPR. *Mobile Information Systems*, *2018*, 1-6. https://doi.org/10.1155/2018/6792028.

Shapiro, S. S., & Wilk, M. B. (1965). An analysis of variance test for normality (complete samples). *Biometrika*, *52*(3/4), 591-611. https://doi.org/10.1093/biomet/52.3-4.591.

Sirur, S., Nurse, J. R., & Webb, H. (2018, January). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (88-95). https://doi.org/10.1145/3267357.3267368.

SMEDATA II Poject. (n.d.). Retrieved July 30, 2022, from https://smedata.eu/

Sørensen, J. B., & Fassiotto, M. A. (2011). Organizations as fonts of entrepreneurship. *Organization Science*, *22*(5), 1322–1331. https://doi.org/10.1287/orsc.1100.0622.

Startup Heatmap Europe. (2021). *The power of the ecosystem startup heatmap europe report 2021*. Startup Heatmap Europe. Retrieved July 30, 2022, from https://startupsandplaces.com/wp-content/uploads/2021/03/SHM2021_ThePowerofTheEcosystem.pdf

StartupBlink. (2021). *Global startup ecosystem index*. StartupBlink.

Strategic and Competitive Intelligence Unit ACCIÓ. (2021). *Barcelona & Catalonia startup hub, 2021 analysis*. ACCIÓ. Retrieved July 30, 2022, from http://startups.catalonia.com/.

Sue, V.M., & Ritter, L. A. (2012). *Conducting online surveys.* (2nd ed.). Sage.

Sullivan, G. & Artino Jr., A. R. (2013). Analyzing and interpreting data from likert-type scales. *Journal of Graduate Medical Education.*, *5(4)*, 541–542. https://doi.org/10.4300/JGME-5-4-18.

Supyuenyong, V., Islam, N., & Kulkarni, U. (2009). Influence of SME characteristics on knowledge management processes: The case study of enterprise resource planning service providers. *Journal of Enterprise Information Management*, *22*(1/2), 63–80. https://doi.org/10.1108/17410390910922831.

Tabachnick, B. G., & Fidell, L. S. (2006). *Using multivariate statistics.* (5th ed.). Allyn & Bacon.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 34(1), 134-153. https://doi.org/10.1016/j.clsr.2017.05.015.

Toshkov, D. (2010). Taking stock: A review of quantitative studies of transposition and implementation of EU law. *Institute for European Integration Research, 25-26.*

Truby, J., Brown, R. D., Ibrahim, I. A., & Parellada, O. C. (2022). A sandbox approach to regulating high-risk artificial intelligence applications. *European Journal of Risk Regulation*, *13*(2), 270–294. https://doi.org/10.1017/err.2021.52.

TrustArc. (2017). *Privacy and the EU GDPR. US and UK Privacy Professional.*TrustArc.

TrustArc. (2018). *GDPR compliance status: A comparison of US, UK and EU companies*. TrustArc.

Union, C. of the E. (2020). *Council conclusions on regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age Delegations* (Vol. 2020).

Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: Providing a competitive advantage for U.S. companies. *American Business Law Journal*, 56(2), 287-344. https://doi.org/10.1111/ablj.12139.

Withey, V. (2018). *The impact of GDPR on the technology sector*. Retrieved July 21, 2022 from https://www.grcworldforums.com/gdpr/the-impact-of-gdpr-on-the-technology-sector/152.article

Yeung, K., & Bygrave, L. A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, *16*(1), 137-155. https://doi.org/10.1111/rego.12401.

Yin, R. K. (2017). *Case study research and applications design and methods* (6th ed.). Sage.

Zumbo, B. D., & Zimmerman, D. W. (1993). Is the selection of statistical methods governed by level of measurement? *Canadian Psychology/Psychologie canadienne*, *34*(4), 390. https://doi.org/10.1037/h0078865

# APPENDICES

## APPENDIX A

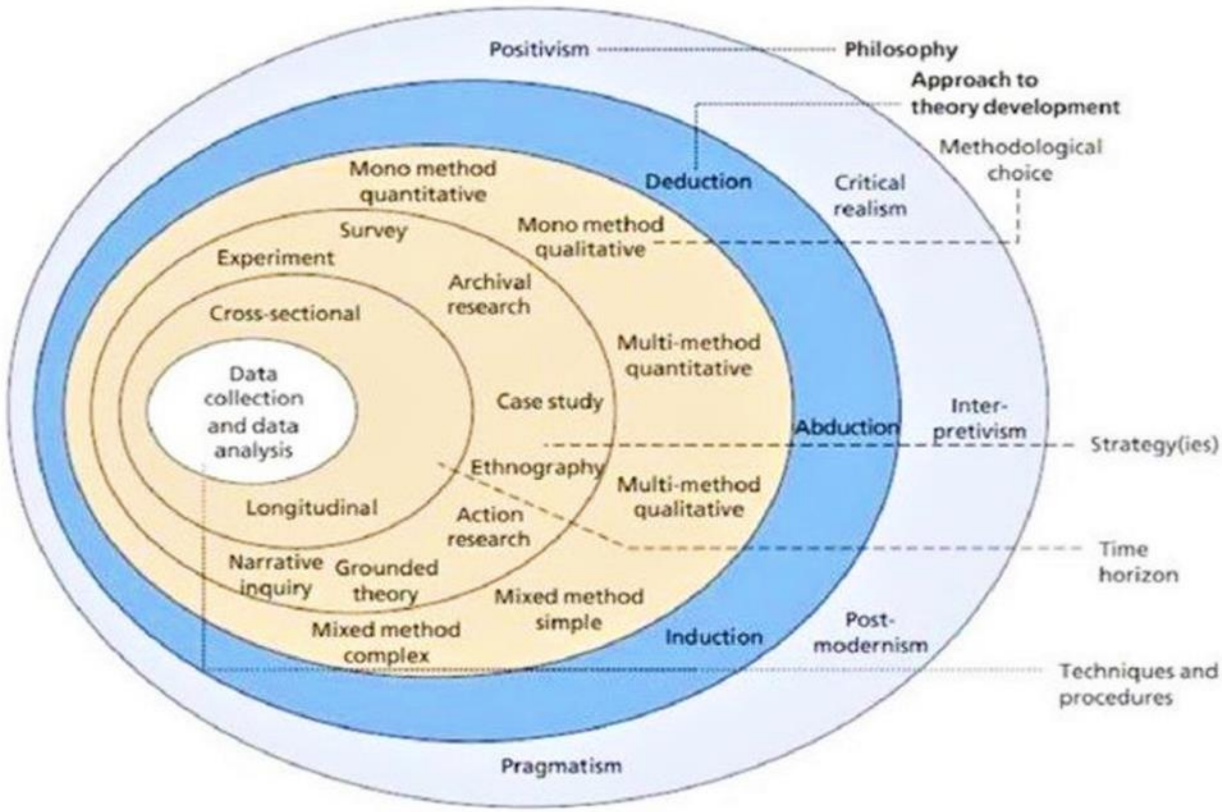



Figure A.1: The research onion framework by Saunders, Lewis, and Thornhill (2016)

In the following sections, each layer of the research onions is discussed with reference to the prior framework to illustrate the philosophical approach and the steps taken to guarantee that the study research design and survey techniques were relevant.

### Research philosophy

The first layer of the research onion refers to the philosophical approach of the researchers. To make sure they have a believable design, scholars must be aware first of their own views and how they influence their decisions. Saunders et al. (2019, p.130) refer to research philosophy as “a system of beliefs and assumptions about the development of knowledge”**,** and Creswell and Clark (2018, p. 34) likewise emphasize the relevance of: Researchers should be aware of their assumptions about knowledge acquisition during their studies. These assumptions influence the investigation and study procedures. Saunders et al. (2019) recommended that before considering the various research philosophies, scholars should be able to differentiate and comprehend their ontological, epistemological, and axiological assumptions, and proposed that objectivism and subjectivism can be viewed as two extremes. Table A.1 illustrates the types of assumption about normal questions and continua of objectivism and subjectivism.

Table A.1: Philosophical assumptions (Saunders et al., 2019)

| Assumption type | Questions | Continua with two sets of extremes | | |
|---|---|---|---|---|
| | | **Objectivism** | ⇔ | **Subjectivism** |
| **Ontology** | • What is the nature of reality?<br>• What is the world like?<br>• For example:<br>– What are organisations like?<br>– What is it like being in organisations?<br>– What is it like being a manager or being managed? | Real | ⇔ | Nominal/decided by convention |
| | | External | ⇔ | Socially constructed |
| | | One true reality (universalism) | ⇔ | Multiple realities (relativism) |
| | | Granular (things) | ⇔ | Flowing (processes) |
| | | Order | ⇔ | Chaos |
| **Epistemology** | • How can we know what we know?<br>• What is considered acceptable knowledge?<br>• What constitutes good-quality data?<br>• What kinds of contribution to knowledge can be made? | Adopt assumptions of the natural scientist | ⇔ | Adopt the assumptions of the arts and humanities |
| | | Facts | ⇔ | Opinions |
| | | Numbers | ⇔ | Narratives |
| | | Observable phenomena | ⇔ | Attributed meanings |
| | | Law-like generalisations | ⇔ | Individuals and contexts, specifics |
| **Axiology** | • What is the role of values in research? How should we treat our own values when we do research?<br>• How should we deal with the values of research participants? | Value-free | ⇔ | Value-bound |
| | | Detachment | ⇔ | Integral and reflexive |

All research philosophies make at least three main types of assumption: ontology, which deals with assumptions about the nature of the world and reality, axiology which relates to the role of values and ethics in the research process and epistemology, which according to Burrell and Morgan (1979, p.xii) addresses assumptions about knowledge – how we know what we say we know, what constitutes acceptable, valid, and legitimate knowledge, and how we can impart knowledge to those around us. Finally, epistemological assumptions determine what contribution research can make to knowledge (Saunders et al., 2019). According to Baldwin et. al (2014), in business studies as a branch of philosophy, epistemology can be engraved as the study of the criteria by which the researcher classifies what constitute knowledge and what does not.

The researcher also completed the Heightening your Awareness of your Research Philosophy (HARP) designed by A. Bristow and M.N.K. Saunders (Saunders et al., 2019) and after questioning research beliefs and assumptions and becoming familiar with the main research philosophies in business and management and the research design used to conduct the research, he has come to the conclusion, that the epistemological research philosophy is the one that resonates with the researcher. This research is about accepted knowledge, measurable facts and not opinions because this research accepts noticeable phenomena based on data and facts as information, the research philosophy of positivism.

## Research approach

The second layer of the research onion looks at whether an abductive, deductive, or inductive technique is chosen. The following section provides an overview of each term and the reasons for the choice:

**Deduction**: The approach usually begins with a theory, often derived from your reading of the scholarly literature Saunders et al. (2019, p.153).

**Induction:** Saunders et al. (2019, p.153) suggested that this approach is relevant when your investigation begins by gathering information to research a phenomenon and developing or building theories (frequently in the type of a conceptual framework).

**Abduction:** Saunders et al. (2019, p.153) suggested that the approach is relevant when you gather information to study a phenomenon, associate topics and illustrate patterns, in order to develop a recent theory or alter an existing theory, which you then test through further information gathering. Table A.2 shows how they illustrated the research approaches. Since this research starts with a conceptual framework developed from the researcher's reading of the academic literature, anecdotal evidence, and interviews with several representatives of startups in Catalonia, the research approach is deductive.

Table A.2: Deduction, induction and abduction: from reason to research - (Saunders et al., 2019)

| | Deduction | Induction | Abduction |
|---|---|---|---|
| Logic | In a deductive inference, when the premises are true, the conclusion must also be true | In an inductive inference, known premises are used to generate untested conclusions | In an abductive inference, known premises are used to generate testable conclusions |
| Generalisability | Generalising from the general to the specific | Generalising from the specific to the general | Generalising from the interactions between the specific and the general |
| Use of data | Data collection is used to evaluate propositions or hypotheses related to an existing theory | Data collection is used to explore a phenomenon, identify themes and patterns and create a conceptual framework | Data collection is used to explore a phenomenon, identify themes and patterns, locate these in a conceptual framework and test this through subsequent data collection and so forth |
| Theory | Theory falsification or verification | Theory generation and building | Theory generation or modification; incorporating existing theory where appropriate, to build new theory or modify existing theory |

# APPENDIX B

Doña Melany Delgado Phillips, Traductora-Intérprete Jurada de inglés nombrada por el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, certifica que la que sigue es traducción fiel y completa al español de un documento redactado en inglés.

MELANY DELGADO PHILLIPS
Traductora-Intérprete Jurada de INGLÉS
N.º 10606

-----------------------------------------------------------*Comienzo de la traducción*------------------

## ENCUESTA SOBRE LOS RETOS DEL RGPD

*Esta encuesta se lleva a cabo como parte del estudio de investigación realizado en nombre de la Geneva Business School de Barcelona. El objeto del estudio es identificar los retos a los que se enfrentan las empresas de nueva creación (startups) tecnológicas de Barcelona a raíz de la aplicación del Reglamento General de Protección de Datos (RGPD) a partir de mayo de 2018.*

*La información que proporcione, así como sus respuestas, son estrictamente confidenciales. La identificación de la empresa es necesaria solo para fines estadísticos. Los resultados del estudio se presentarán en forma de datos agregados.*

### PARTE A: Entender el Reglamento General de Protección de Datos (RGPD)

*En la sección siguiente, elija una de las respuestas sugeridas en relación con sus percepciones personales y su conocimiento sobre el Reglamento General de Protección de Datos (RGPD)*

| N.º | Preguntas | Opciones de respuesta | Respuesta correcta |
|---|---|---|---|
| A.1 | El Reglamento General de Protección de Datos (RGPD) regula el tratamiento de los datos personales (recogida, almacenamiento y uso) | Verdadero / Falso / No sé | ***VERDADERO*** |
| A.2 | Toda información que pueda utilizarse para identificar a una persona es un dato personal | Verdadero / Falso / No sé | ***VERDADERO*** |
| A.3 | Los datos de localización recogidos por su teléfono móvil no son datos personales | Verdadero / Falso / No sé | ***FALSO*** |
| A.4 | El Reglamento General de Protección de Datos (RGPD) no le da derecho a acceder a los datos personales que las organizaciones tienen sobre usted | Verdadero / Falso / No sé | ***FALSO*** |
| A.5 | Todavía no existen sanciones económicas para las empresas que no cumplan con el Reglamento General de Protección de Datos (RGPD) | Verdadero / Falso / No sé | ***FALSO*** |
| A.6 | El Reglamento General de Protección de Datos (RGPD) permite la «portabilidad de datos», lo que significa que puede tomar sus datos de una organización y dárselos a otra | Verdadero / Falso / No sé | ***VERDADERO*** |
| A.7 | Los datos abiertos (*open data*) no suelen incluir datos personales | Verdadero / Falso / No sé | ***VERDADERO*** |
| A.8 | Los datos abiertos (*open data*) solo pueden utilizarse, modificarse y compartirse con fines no comerciales | Verdadero / Falso / No sé | ***FALSO*** |

### PARTE B: Retos del Reglamento General de Protección de Datos (RGPD)

*B.1 Valore en una escala de 10 puntos (donde 1 = totalmente en desacuerdo ... y 10 = totalmente de acuerdo) las afirmaciones que figuran a continuación sobre los costes de cumplimiento del Reglamento General de Protección de Datos (RGPD).*

| Concepto | N.º | Pregunta | Escala de Likert de 10 puntos (totalmente en desacuerdo – totalmente de acuerdo) | No sé | No procede |
|---|---|---|---|---|---|
| Costes de Cumplimiento | B.1.1 | Cumplir con el RGPD es costoso | 1-10 | | |
| | B.1.2 | El presupuesto de la empresa ha aumentado de manera considerable debido al RGPD | 1-10 | | |
| | B.1.3 | Es costoso invertir en consultores de RGPD | 1-10 | | |
| | B.1.4 | Es costoso invertir en nuevas contrataciones para cumplir con las exigencias del RGPD | 1-10 | | |
| | B.1.5 | Tuvimos que adquirir nuevas soluciones tecnológicas para cumplir con el RGPD | 1-10 | | |
| | B.1.6 | Fue costoso invertir en tecnología nueva | 1-10 | | |
| | B.1.7 | Estamos dedicando mucho tiempo a cumplir con el RGPD | 1-10 | | |
| | B.1.8 | Estamos gastando importantes recursos económicos para cumplir con el RGPD | 1-10 | | |

B.1.9 Los **costes <u>más elevados</u>** de cumplimiento del RGPD de su empresa están relacionados con (elija SOLO UNA respuesta):

- o Contratación del delegado de protección de datos (DPO)
- o Contratación de nuevos empleados responsables de la protección de datos
- o Formación de los empleados acerca del RGPD
- o Adquisición de nuevas soluciones tecnológicas
- o Modificación de procesos
- o Introducción de nuevas políticas y procesos
- o Control del cumplimiento
- o Evaluación de impacto relativa a la protección de datos (EIPD)
- o Evaluación de riesgos
- o Otros (especifique) ________

B.1.10 ¿Cuánto gasta su empresa anualmente para cumplir con el RGPD?

- o Menos de 5000 €
- o 5000 € – 10 000 €
- o 10 000 € – 50 000 €
- o 50 000 € – 100 000 €
- o Más de 100 000 €

MELANY DELGADO PHILLIPS
Traductora-Intérprete Jurada de
INGLÉS
N.º 10606

*B.2 Valore en una escala de 10 puntos (donde 1 = totalmente en desacuerdo ... y 10 = totalmente de acuerdo) las afirmaciones que figuran a continuación sobre la complejidad del Reglamento General de Protección de Datos (RGPD).*

| Concepto | N.º | Pregunta | Escala de Likert de 10 puntos (totalmente en desacuerdo – totalmente de acuerdo) | No sé | No procede |
|---|---|---|---|---|---|
| **Complejidad del Reglamento** | B.2.1 | El RGPD es complejo y difícil de entender | 1-10 | | |
| | B.2.2 | El RGPD carece de precisión y claridad | 1-10 | | |
| | B.2.3 | Nuestra empresa tuvo dificultades para entender e interpretar el RGPD | 1-10 | | |
| | B.2.4 | Es difícil garantizar que nuestros proveedores/suministradores/vendedores sigan la normativa en materia de protección de datos personales (RGPD) | 1-10 | | |
| | B.2.5 | Supuso un reto formar a los empleados existentes acerca de los requisitos del RGPD | 1-10 | | |
| | B.2.6 | Supone un reto formar a los nuevos empleados acerca de los requisitos del RGPD | 1-10 | | |
| | B.2.7 | Fue difícil cambiar la mentalidad de la empresa para garantizar que cada empleado siguiera los principios del RGPD | 1-10 | | |

*B.3 Valore en una escala de 10 puntos (donde 1 = totalmente en desacuerdo ... y 10 = totalmente de acuerdo) las afirmaciones que figuran a continuación sobre la ayuda prestada por el gobierno en relación con el cumplimiento del Reglamento General de Protección de Datos (RGPD).*

| Concepto | N.º | Pregunta | Escala de Likert de 10 puntos (totalmente en desacuerdo – totalmente de acuerdo) | No sé | No procede |
|---|---|---|---|---|---|
| **Apoyo del Gobierno** | B.3.1 | Hay una falta de apoyo informativo por parte de los organismos gubernamentales en relación con el RGPD | 1-10 | | |
| | B.3.2 | Faltan directrices prácticas de los organismos gubernamentales para seguir correctamente los procedimientos estándar | 1-10 | | |
| | B.3.3 | El RGPD no ofrece ninguna recomendación sobre el uso de tecnología que ayude a cumplir sus requisitos | 1-10 | | |

| | | | | | |
|---|---|---|---|---|---|
| | B.3.4 | El RGPD no proporciona ningún instrumento o ninguna herramienta específicos para las empresas | 1-10 | | |
| | B.3.5 | Existe el riesgo de tener que rendir cuentas cuando no existen directrices claras que seguir en materia de RGPD | 1-10 | | |
| | B.3.6 | Las multas impuestas por el gobierno por incumplimiento del RGPD son demasiado elevadas | 1-10 | | |

*B.4 Valore en una escala de 10 puntos (donde 1 = totalmente en desacuerdo … y 10 = totalmente de acuerdo) las afirmaciones que figuran a continuación sobre la adaptación de los procesos de la empresa para cumplir del Reglamento General de Protección de Datos (RGPD).*

| **Concepto** | **N.º** | **Pregunta** | **Escala de Likert de 10 puntos (totalmente en desacuerdo – totalmente de acuerdo)** | **No sé** | **No procede** |
|---|---|---|---|---|---|
| **Adaptación de Procesos** | B.4.1 | Fue difícil adaptar el modelo de negocio existente de la empresa para garantizar el cumplimiento satisfactorio del RGPD | 1-10 | | |
| | B.4.2 | Supone un reto proporcionar a nuestras partes interesadas (clientes, empleados, proveedores, gobierno, etc.) el acceso a los datos personales | | | |
| | B.4.3 | No es fácil establecer un procedimiento claro para eliminar los datos de una persona | | | |
| | B.4.4 | Supone un reto tratar volúmenes de datos crecientes de una forma rápida | | | |
| | B.4.5 | Es difícil garantizar la portabilidad de los datos personales | | | |
| | B.4.6 | No podemos contar con una persona que realice el tratamiento si un interesado rechaza el tratamiento automatizado | | | |
| | B.4.7 | No es fácil elaborar un plan de respuesta ante incidentes cibernéticos | | | |
| | B.4.8 | No es fácil saber dónde se almacenan todos los datos personales de nuestras partes interesadas | | | |
| | B.4.9 | Supone un reto responder a las consultas de datos dentro del plazo obligatorio de 30 días | | | |
| | B.4.10 | Supone un reto aplicar las tecnologías emergentes (inteligencia artificial, robótica, computación en la nube, *blockchain*, etc.) para lograr un mejor cumplimiento del RGPD | | | |
| | B.4.11 | Es complejo llevar a cabo auditorías periódicas para garantizar que todos los procesos cumplen con el RGPD | | | |

B.4.12 ¿Cuánto tiempo ha tardado su empresa en cumplir con el RGPD?

- o 3 meses o menos
- o 4-6 meses
- o 7-9 meses
- o 10-12 meses
- o 13-18 meses
- o 19-24 meses
- o Más de 24 meses
- o Hemos empezado, pero todavía no hemos alcanzado el cumplimiento

MELANY DELGADO PHILLIPS
Traductora-Intérprete Jurada de
INGLÉS
N.º 10606

B.4.13 ¿Cuántas personas han tenido que contratar a causa del RGPD?

- o Ninguna

○ 1
○ 2-5
○ 6-10
○ Más de 10

B.4.14 ¿Quién es el responsable del cumplimiento del RGPD en su empresa?
○ Delegado de protección de datos (DPO)
○ Jefe de protección de datos (CPO)
○ Consultor externo
○ Yo mismo/a
○ Otros (especifique) _______________

**PARTE C: PERFIL DE LA EMPRESA Y DE LA PERSONA ENCUESTADA**

C.1 Indique el nombre de su empresa:

_____________________

*(Tenga en cuenta que el nombre de su empresa se necesita solo con fines estadísticos para EVITAR <u>un seguimiento innecesario de la encuesta</u>)*

C.2 ¿Cuándo se creó la empresa?

_____________________

*(mes y año)*

C.3 ¿Cómo se posiciona su empresa?
○ Nueva creación (*startup*)
○ Microempresa
○ Pequeña empresa
○ Mediana empresa

C.4 ¿Cuántas personas trabajan en su empresa?
○ De 0 a 1 persona
○ De 2 a 9 personas
○ De 10 a 49 personas
○ De 50 a 249 personas

C.5 ¿En qué área se especializa su empresa?
○ Tecnología financiera (*Fintech*)
○ Tecnología en el sector inmobiliario (*Proptech*)
○ Salud digital (*Ehealth*)
○ Biotecnología (*Biotech*)
○ Movilidad
○ Tecnología publicitaria (*Adtech*)
○ Jobtech
○ Moda
○ Comercio electrónico (B2B)
○ Comercio electrónico (B2C)
○ Internet de las cosas (IoT)
○ Ciudades inteligentes
○ Impacto social
○ Otros (especifique) _____________

C.6 ¿Cuál es su función en la empresa?
○ Fundador
○ Miembro del consejo de administración
○ Administrador
○ Director
○ Delegado de protección de datos (DPO)
○ Jefe de protección de datos (CPO)
○ Responsable de la normativa de protección de datos
○ Responsable, en parte, de la normativa de protección de datos
○ Departamento de tecnología de la información
○ Otros (especifique) _________________

C.7 Especifique su sexo:
○ Masculino
○ Femenino

MELANY DELGADO PHILLIPS
Traductora-Intérprete Jurada de
INGLÉS
N.º 10606

C.8 ¿Cuál es su nivel de estudios MÁS ALTO?

- o Título de Bachillerato
- o Título universitario
- o Título profesional
- o Licenciatura/Grado
- o Máster
- o Doctorado
- o Otros (especifique) ______________

C.9 Especifique el campo de estudio asociado a su nivel de estudios MÁS ALTO:

____________________

**¡Gracias por su contribución a la ciencia!**

---------------------------------------------------------------*Fin de la traducción*---------------------------------------------------------------

Esta traducción consta de cinco (5) páginas, numeradas, fechadas, firmadas y selladas por la traductora-intérprete jurada, registradas bajo el número TIJ_03_2021_00046 de su registro, con una copia adjunta del documento original, fechada y sellada por la traductora-intérprete jurada.

Certificación

Doña Melany Delgado Phillips, Traductora-Intérprete Jurada de inglés nombrada por el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, certifica que la que antecede es traducción fiel y completa al español de un documento redactado en inglés.

En Las Palmas de Gran Canaria (España), a 31 de marzo de 2021.

Traductora-Intérprete Jurada de inglés n.º 10606
Socio profesional ASETRAD n.º 2550

MELANY DELGADO PHILLIPS
Traductora-Intérprete Jurada de
INGLÉS
N.º 10606

## APPENDIX C

### QUESTIONNAIRE ON GDPR CHALLENGES

*This survey is conducted as part of the research study carried out on behalf of Geneva Business School, Barcelona. The aim of the study is to identify challenges faced by technological startups in Barcelona resulting from the enforcement of the General Data Protection Regulation (GDPR) as of May 2018.*

*The information you provide, and your answers are strictly confidential. Company identification is needed for statistical purposes only. The results of the study will be presented in the form of aggregate data.*

**PART A: Understanding the General Data Protection Regulation (GDPR)**

*In the section below, please choose one of the suggested answers regarding your personal perceptions and familiarity with the General Data Protection Regulation (GDPR)*

| No. | Question Items | Answer Options | Correct Answer |
|---|---|---|---|
| A.1 | The General Data Protection Regulation (GDPR) governs the processing of personal data (collection, storage, and use) | True / False / I don't know | ***TRUE*** |
| A.2 | Any information that can be used to identify an individual is personal data | True / False / I don't know | ***TRUE*** |
| A.3 | Location data collected by your mobile phone is not personal data | True / False / I don't know | ***FALSE*** |
| A.4 | The General Data Protection Regulation (GDPR) does not give you the right to access the personal data organizations hold about you | True / False / I don't know | ***FALSE*** |
| A.5 | There are still no financial penalties for companies that do not comply with the General Data Protection Regulation (GDPR) | True / False / I don't know | ***FALSE*** |
| A.6 | The General Data Protection Regulation (GDPR) allows for 'data portability' meaning that you can take your data from one organization and give it to another | True / False / I don't know | ***TRUE*** |
| A.7 | Open data does not generally include personal data | True / False / I don't know | ***TRUE*** |
| A.8 | Open data can only be used, modified, and shared for non-commercial purposes | True / False / I don't know | ***FALSE*** |

**PART B: Challenges of the General Data Protection Regulation (GDPR)**

*B.1 Please rate on a 10-point scale (where 1 = strongly disagree ... and 10 = strongly agree) the statements below regarding the General Data Protection Regulation (GDPR) compliance costs.*

| Construct | No. | Question Item | 10-point Likert Scale (strongly disagree – strongly agree) | I don't know | Not Applicable |
|---|---|---|---|---|---|
| Compliance Costs | B.1.1 | GDPR is expensive to comply with | 1-10 | | |
| | B.1.2 | The company budget has been significantly increased because of GDPR | 1-10 | | |
| | B.1.3 | It is costly to invest in GDPR consultants | 1-10 | | |
| | B.1.4 | It is costly to invest in new hires to meet the demands of GDPR | 1-10 | | |
| | B.1.5 | We had to acquire new technology solutions to comply with GDPR | 1-10 | | |
| | B.1.6 | It was costly to invest in new technology | 1-10 | | |
| | B.1.7 | We are spending a lot of time to be GDPR compliant | 1-10 | | |
| | B.1.8 | We are spending significant financial resources to be GDPR compliant | 1-10 | | |

B.1.9 The **highest** GDPR compliance **costs** of your company are associated with (chose ONLY ONE answer):

- O Hiring data protection officer (DPO)
- O Hiring new employees accountable for data protection
- O Training employees about GDPR
- O Acquiring new technology solutions

MELANY DELGADO PHILLIPS
Traductora-Intérprete Jurada de
INGLÉS
N.º 10606

o Modifying processes
o Introducing new policies and processes
o Monitoring compliance
o Data protection impact assessment (DPIA)
o Risk assessment
o Other (specify) ________

MELANY DELGADO PHILLIPS
Traductora-Intérprete Jurada de
INGLÉS
N.º 10606 31 MAR 2021

B.1.10 How much does your company spend on an annual basis for being GDPR compliant?

o Less than €5,000
o €5,000 – €10,000
o €10,000 – €50,000
o €50,000 – €100,000
o More than €100,000

*B.2 Please rate on a 10-point scale (where 1 = strongly disagree ... and 10 = strongly agree) the statements below regarding the complexity of the General Data Protection Regulation (GDPR).*

| **Construct** | **No.** | **Question item** | **10-point Likert Scale (strongly disagree – strongly agree)** | **I don't know** | **Not Applicable** |
|---|---|---|---|---|---|
| **Regulation Complexity** | B.2.1 | GDPR is complex and difficult to understand | 1-10 | | |
| | B.2.2 | GDPR lacks precision and clarity | 1-10 | | |
| | B.2.3 | Our company had difficulties with understanding and interpreting GDPR | 1-10 | | |
| | B.2.4 | It is difficult to ensure that our providers / suppliers / vendors follow the regulation for personal data protection (GDPR) | 1-10 | | |
| | B.2.5 | It was challenging to train existing employees about GDPR requirements | 1-10 | | |
| | B.2.6 | It is challenging to train new employees about GDPR requirements | 1-10 | | |
| | B.2.7 | It was difficult to change the company mindset to ensure that each employee follows GDPR principles | 1-10 | | |

*B.3 Please rate on a 10-point scale (where 1 = strongly disagree ... and 10 = strongly agree) the statements below regarding the government support in relation to the compliance with the General Data Protection Regulation (GDPR).*

| **Construct** | **No.** | **Question item** | **10-point Likert Scale (strongly disagree – strongly agree)** | **I don't know** | **Not Applicable** |
|---|---|---|---|---|---|
| **Government Support** | B.3.1 | There is a lack of information support from the government bodies in relation to GDPR | 1-10 | | |
| | B.3.2 | There is a lack of practical guidelines from the government bodies to follow standard procedures correctly | 1-10 | | |
| | B.3.3 | GDPR does not provide any recommendations regarding the use of technology helping to comply with its requirements | 1-10 | | |
| | B.3.4 | GDPR does not provide any specific instruments or tools for companies | 1-10 | | |
| | B.3.5 | There is a risk of being accountable when there are not clear GDPR guidelines to follow | 1-10 | | |
| | B.3.6 | Government fines for GDPR incompliance are too high | 1-10 | | |

*B.4 Please rate on a 10-point scale (where 1 = strongly disagree ... and 10 = strongly agree) the statements below regarding the adaptation of company processes to comply with the General Data Protection Regulation (GDPR).*

| Construct | No. | Question item | 10-point Likert Scale (strongly disagree – strongly agree) | I don't know | Not Applicable |
|---|---|---|---|---|---|
| **Process Adaptation** | B.4.1 | It was difficult to adapt the existing business model of the company to ensure successful GDPR compliance | | | |
| | B.4.2 | It is challenging to provide our stakeholders (customers, employees, suppliers, government, etc.) with the access to personal data | 1-10 | | |
| | B.4.3 | It is not easy to establish a clear procedure to delete an individual's data | | | |
| | B.4.4 | It is challenging to process growing data in a quick way | | | |
| | B.4.5 | It is hard to ensure portability of personal data | | | |
| | B.4.6 | We are not able to have a person performing the processing if a data subject opts out of automated processing | | | |
| | B.4.7 | It is not easy to develop a cyber incident response plan | | | |
| | B.4.8 | It is not easy to know where all the personal data of our stakeholders is stored | | | |
| | B.4.9 | It is challenging to respond to data enquiries within a 30-day obligation period | | | |
| | B.4.10 | It is challenging to apply emergent technologies (artificial intelligence, robotics, cloud computing, blockchain, etc.) to achieve better compliance with the GDPR | | | |
| | B.4.11 | It is complex to execute periodic audits to ensure that all processes are compliant with GDPR | | | |

B.4.12 How long did it take your company to achieve GDPR compliance?

- O 3 or less months
- O 4-6 months
- O 7-9 months
- O 10-12 months
- O 13-18 months
- O 19-24 months
- O More than 24 months
- O We have started but have not yet reached compliance

B.4.13 How many people you had to recruit because of GDPR?

- O None
- O 1
- O 2-5
- O 6-10
- O More than 10

B.4.14 Who is responsible for GDPR compliance in your company?

- O Data Protection Officer (DPO)
- O Chief Protection Officer (CPO)
- O 3rd party consultant
- O Myself
- O Other (specify) _______________

MELANY DELGADO PHILLIPS
Traductora-Intérprete Jurada de
INGLÉS
N.º 10606 31 MAR 2021

## PART C: COMPANY AND RESPONDENT PROFILE

C.1 Specify the name of your enterprise:

____________________

*(Please note that the name of your enterprise is needed only for statistical purposes to AVOID unnecessary survey follow-up)*

C.2 When was the enterprise established?

____________________

*(month and year)*

C.3 How your enterprise is positioned?

- o Startup
- o Microenterprise
- o Small business
- o Medium business

C.4 How many persons are employed on your enterprise?

- o 0 to 1 person
- o 2 to 9 persons
- o 10 to 49 persons
- o 50 to 249 persons

C.5 What is the area of specialization of your enterprise?

- o Fintech
- o Proptech
- o Ehealth
- o Biotech
- o Mobility
- o Adtech
- o Jobtech
- o Fashion
- o eCommerce (B2B)
- o eCommerce (B2C)
- o Internet of things
- o Smart cities
- o Social impact
- o Other (specify) ____________

C.6 What is your role in the company?

- o Founder
- o Member of the board of directors
- o Director
- o Manager
- o Data Protection Officer (DPO)
- o Chief Protection Officer (CPO)
- o Responsible for data protection regulations
- o Partly responsible for data protection regulations
- o IT department
- o Other (specify) ________________

C.7 Specify your gender:

- o Male
- o Female

C.8 What is your HIGHEST level of education

- o High School Diploma
- o College Degree
- o Professional Degree
- o Bachelor's Degree
- o Master's Degree
- o Doctorate Degree
- o Other (specify) ______________

MELANY DELGADO PHILLIPS
Traductora-Intérprete Jurada de
INGLÉS
N.º 10606 31 MAR 2021

C.9 Specify your study field associated with your HIGHEST education:

____________________

**Thank you for your contribution to science!**