ESTIMATING THE GDPR IMPACT ON STARTUPS IN UPTEC

Ricardo Schlatter Hasenack

Dissertation

Masters in Innovation and Technological Entrepreneurship

Supervised by

Manuel de Sousa Aroso

2023

Abstract

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for collecting, processing, and storing personal information from residents of the European Union (EU). The regulation applies to all companies, of any magnitude, that collect or handle information from European Citizens. This work aims to understand how the GDPR might negatively affect startups in UPTEC by either raising costs, hindering innovation, or placing barriers to the accelerated growth this type of company usually seeks. Using an online questionnaire, we inquired startup founders, c-level managers, and senior managers about the experience of their companies regarding the road to compliance with the GDPR and its impact on their business. We conclude, given the limitations of the study, that the regulation tends to create additional costs for startups, although not at a very significant level. In the innovation spectrum, the conclusion is that management often weighs the need to comply with the GDPR when ideating new products or services - the tendency, however, is not to discard any ideas exclusively because of the risk of non-compliance. Regarding growth, the GDPR is not seen as a blocker for growth for most companies, either because they tend to build compliant products from the ground up or because the risk of non-compliance is not high enough and the companies chose to develop the business without taking the regulation into account.

Keywords: GDPR, Data Regulation, Startups, Technology, Privacy

Resumo

O Regulamento Geral de Proteção de Dados (GDPR) é um quadro legal que estabelece diretrizes para a recolha, processamento e armazenamento de informações pessoais de residentes da União Europeia (UE). O regulamento aplica-se a todas as empresas, de qualquer magnitude, que recolham ou manipulem informações de cidadãos europeus. Este trabalho tem como objetivo entender como o GDPR pode afetar negativamente as startups no Norte de Portugal, quer aumentando os custos, dificultando a inovação, ou colocando barreiras ao crescimento acelerado que este tipo de empresa geralmente busca. Usando um questionário online, inquirimos fundadores de startups, gestores de alto nível e gerentes seniores sobre a experiência das suas empresas no caminho para a conformidade com o GDPR e o seu impacto nos seus negócios. Concluímos, dadas as limitações do estudo, que a regulamentação tende a criar custos adicionais para as startups, embora não a um nível muito significativo. No espectro da inovação, a conclusão é que a gestão geralmente pesa a necessidade de cumprir o GDPR ao idealizar novos produtos ou serviços - a tendência, no entanto, não é descartar quaisquer ideias exclusivamente por causa do risco de não conformidade. No que diz respeito ao crescimento, o GDPR não é visto como um obstáculo para o crescimento da maioria das empresas, ou porque elas tendem a construir produtos conformes desde o início, ou porque o risco de não conformidade não é alto o suficiente e as empresas optam por desenvolver o negócio sem levar a regulamentação em conta.

Palavras-chave: GDPR, Regulamento de Dados, Privacidade, Startups, Technology

Index

1. Introduction

On the 25th of May 2018, the General Data Protection Regulation (GDPR) was put into effect by the European Union, affecting organizations anywhere that target or collect data related to people inside the EU. This new data privacy and security law is composed of hundreds of pages of requirements for organizations across the globe and imposes significantly high fines for ones that don't comply with the rules.

Over the last 25 years, technology has transformed lives in ways that were hard to picture in advance. The scale of the collection and sharing of personal data has increased immensely - the technology available today allows both private companies and public authorities to make use of personal data on an unprecedented scale to pursue their activities. While we use the internet daily for our personal and professional lives, information that was once private or known by a few companies is now accessible to thousands of companies. The European Union historically took big steps to regulate the usage of this data to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, and the GDPR is the latest proof of this effort.

"This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."

Recital 2 from the GDPR

Recent cutting-edge releases in the Generative Artificial Intelligence (AI) spectrum, represented by, among others, Large Language Models such as Open AI's Chat GPT and prompt-based image generation products such as Midjourney and Stable Diffusion have resurfaced the discussion about Data Privacy and how it should be regulated. Generative AI is built by training the models over millions of pages of text and images, and whether the way the companies that own these models handle this data is compliant or not is currently a hot topic that has even led to temporary bans on the tool by some European countries such as Italy (McCallum, 2023).

The issue of data anonymization, for instance, is an essential topic in this area. As AI develops in strength, there is an increasing chance that it may be able to interpret anonymized data, undermining the layers of security surrounding sensitive data. To ensure ethical data

usage and respect for privacy in this situation, generative AI models must be built per GDPR regulations.

Generative AI is just one example of emerging technologies that must be designed and implemented in compliance with GDPR to ensure ethical data usage and maintain respect for privacy. As detailed in Recital 13 of the GDPR to ensure a consistent level of protection to the users in the European Union the regulation applies to micro, small, and medium-sized enterprises (with a derogation to organizations with less than 250 employees regarding record-keeping, as stated in article 30-5). That means that any company, regardless of its size, must make a considerable effort to comply with the regulations to reduce the risk of penalties. Large corporations can likely absorb these costs, but startups and SMEs have more limited resources while facing similar challenges as major companies.

It is crucial not to undervalue the extent of these difficulties. The regulation is extensive, in a way that even before the implementation process, it is a difficult challenge to comprehend the complexity of compliance with the GDPR. The road to compliance includes, for instance, mapping and auditing all data processing activities within an organization, ensuring proper consent mechanisms are in place, instituting robust data security practices, and upholding data subjects' rights. Additionally, GDPR mandates immediate responses to data breaches and calls for crystal-clear consent methods for data gathering, placing heavy demands on a small business's time, resources, and skills.

1.1. Motivation

As someone who has recently relocated to Europe for work, I have been bombarded with disclaimers about how each business handles my personal information - from having to accept and reaccept terms & conditions to needing to choose the way I want my cookies stored in virtually every single website. While I am, personally, not overly concerned with how my individual data is stored and handled, I am confident that every person should have the right to their privacy, which is becoming increasingly difficult in this day and age.

What I encountered previously at the start of my career as an APS software consultant by ingesting and handling various companies' data was a considerate preoccupation with sensitive information regarding production methods, costs, and financial data. The project would hardly ever include ingesting or processing personal data - and when it did, there was no preoccupation about who could see personal information, how the data was stored, or how or if it was deleted after an employee left the company. At my current occupation, however, worrying about Personal Identifiable Information (PII) information and how it can

and should be handled has become part of my daily routine. When creating new data models or simply adding new columns to an existing table in the database, which often should take only a few hours to be completed can often take months blocked due to bureaucratic processes related to the GDPR restrictions. Valuable information required to take important business decisions is sometimes unavailable or has visibility restricted to a single person or team due to privacy concerns. Whole multidisciplinary teams, with engineers, lawyers, and data scientists are formed to handle these issues across the multiple data sources and datasets existent across the whole business. Software suppliers must go through rigorous bureaucratic processes to guarantee they are also complying with the existing privacy regulations.

I firmly believe that these laws come for good - businesses detain immense amounts of information about users, and it can certainly be misused or mishandled. Regulations are there to protect these from abuses out of their control - nonetheless, from personal experiences, I have, however, wondered how these constraints might impact business development and affect companies, both directly – by, for instance, raising costs due to the necessity for new data governance and privacy departments - and indirectly - by hindering the data ingestion and processing initiatives that might affect innovation or growth of a product or service. My curiosity is to explore if this negative impact in fact exists and its magnitude. In bigger and established companies this cost is probably relatively easily absorbed. In Startups fighting to release a product and depending on a thin upper edge on what the product delivers or strong marketing to get ahead of the competition before money runs out, the impact of extra costs and extra bureaucracy and development times might be fatal. How much does the GDPR increase startup costs, if so? Are the products worse or do they take more time to improve because of these regulations? How does the impact on startups compare to established tech businesses? Can we measure this impact when comparing companies from the EU, where these regulations are stricter than in other regions? How can businesses effectively manage data privacy concerns and ensure compliance with the GDPR without hindering innovation and development?

Answering these questions can provide valuable insights into the impact of the GDPR on businesses and help identify strategies to minimize their detrimental effects while still protecting individuals' privacy. The analysis of these questions can also highlight the importance of balancing the need for data privacy protection with the need for businesses to innovate and grow in a rapidly evolving technological landscape.

1.2. Background Concepts

Data privacy, as a concept, has its roots in the broader context of information privacy, which can be traced back to the early days of recorded history. The right to privacy emerged as a response to the increasing power of the state and various institutions to collect, store, and use personal information (Solove, D., 2008). The advent of new technologies, such as the printing press and photography, raised concerns about privacy and the need to protect individuals from unwarranted intrusion into their lives. (Solove, D., 2008).

The Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which were adopted in 1980, served as the foundation for the creation of privacy laws in the European Union (EU) (OECD, 2002). Aiming to standardize data protection laws across EU member states and ensure the protection of individuals' personal data and privacy, the EU Data Protection Directive (Directive 95/46/EC) was developed in 1995 in large part thanks to these principles (European Parliament and Council, 1995). After the Directive went into effect, several EU members created their own national data protection laws, which varied greatly in terms of their reach and methods of enforcement. Inconsistencies in privacy laws and their enforcement caused by this fragmentation forced the creation of a more thorough and consistent legal framework (Kuner et al., 2020).

The GDPR, which was adopted by the European Parliament and Council on April 27, 2016, was created to address these anomalies. The Data Protection Directive was officially replaced by the GDPR on the 25th of May 2018, making it the primary data protection regulation in the EU (European Parliament and Council, 2016). The GDPR has received plaudit for placing a strong emphasis on defending people's right to privacy while also establishing a more unified and uniform approach to data protection across the EU (Kuner et al., 2020). Strong privacy laws are essential in a world that is becoming more linked and data-driven because of the regulation's worldwide reach and extraterritorial applicability to companies that process the personal data of EU citizens (Voigt et. al., 2017).

The GDPR is a comprehensive set of privacy regulations that grants privacy rights and protections to individuals and correspondingly prescribes restrictions on how organizations must treat personal data. This regulation applies to any organization collecting personal data from anyone inside the EU, so even companies that are based outside the European Union are subject to fines of up to 20 million Euros or 4% of the annual revenue.

Article 5.1-2 of the official document outlines the seven protection and accountability principles:

Lawfulness, fairness, and transparency: Processing must be lawful, fair, and transparent to the data subject.

Purpose limitation: You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.

Data minimization: You should collect and process only as much data as necessary for the purposes specified.

Accuracy: You must keep personal data accurate and up to date.

Storage limitation: You may only store personally identifying data for as long as necessary for the specified purpose.

Integrity and confidentiality: Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g., by using encryption).

Accountability: The data controller is responsible for being able to demonstrate GDPR compliance with all these principles.

The GDPR in the way it applies to Startups can be divided into four main groups of ideas.

Principles (Articles 4–11)

Pseudonymization, openness, data minimization, and minors' (children's) consent are some of the significant principles that the GDPR establishes concerning the processing of personal data. The term *pseudonymization* refers to the processing of personal data to prevent the link to a specific individual without the use of supplementary information (which must be stored separately and safeguarded). When compared to previous regulations, such as DIR95, GDPR adds the requirement of transparency concerning the data subject. According to both DIR95 and GDPR, the personal data used in the processing must be suitable, relevant, and required considering the purposes for which they are processed.

The Data Subject's Rights (Articles 12–23)

The rights of access, rectification, erasure, restriction of processing, and objection are significant for the data subject. According to the GDPR, the data processor must additionally inform the data subject of the legal basis for processing, the length of time the data will be retained, the source of the data, and the data subject's rights. When it comes to the right to

erasure (also known as the right to be forgotten), the GDPR favors the data subject and makes it less difficult to be forgotten when compared to previous regulations – for instance, personal data can (and must, if requested) be deleted under GDPR even if it is not complete, accurate, or processed in compliance with the rules. Additionally, information must be deleted if it is no longer required for the purposes for which it was obtained, consent has been revoked, a data subject objects, or no other valid legal basis exists. The Right to Data Portability is also a new right introduced by the GDPR, allowing individuals to receive and reutilize their personal data across multiple services where processing is automated and consent or a contract is the legal basis. Data must be provided in a machine-readable, structured format that is widely utilized.

Processor and Controller (Articles 24-43)

Regarding the obligations of controllers and processors, there are several significant ramifications. They must first start with the guiding idea of data protection by design and default. This means that data security safeguards must be enabled as a standard and included in every piece of software development. Additionally, when a controller processes personal data, they must take organizational and technical precautions to guarantee that only the personal information required for each individual processing purpose is processed. In the event of a data breach, the controller is required to notify the data subject and notify the supervisory authority within 72 hours.

For most SMEs, a data protection impact assessment (DPIA) should be conducted before beginning any processing when the processing of data poses a significant danger to the rights and liberties of natural people. Some SMEs are also required to appoint a Data Protection Officer (DPO) if their primary activities include processing activities that demand extensive, routine monitoring of data subjects; processing sensitive personal data; or processing personal data of criminal convictions and offenses.

Transfers of Personal Data to International Organizations or Third Countries (Articles 44–50)

The GDPR has tightened the guidelines for sending personal data outside of the EU. This is only permitted under restricted circumstances. In cases where the Commission has determined that the region (country, territory, or sector within the country) or organization

in question provides an acceptable level of protection, the judgment is known as an *adequacy decision*. If the controller or processor has implemented suitable measures and there are enforceable rights and viable legal remedies available to data subjects, a transfer may take place in the absence of a sufficient decision. Binding corporate regulations are an option for businesses that were created in the EU or that are part of an international group of businesses that are based outside of the EU. These are the guidelines that a group of businesses creates to control how their personal data is processed internationally.

If none of the aforementioned circumstances apply, personal data may still be transferred with the approval of a court or tribunal in a third country, or if a particular circumstance arises, such as when the data subject has expressly consented to the proposed transfer, the transfer is required by (a) a contract with the data subject or for their benefit, (b) the protection of the data subject's vital interests, (c) the defense of legal claims, (d) the transfer is necessary because the data is public.

Small and medium enterprises represent over 99% of the businesses in the EU, employing over 100 million people and accounting for over half of the European Union's GDP (The European Commission 2019). As cited by Brodin (2018), studies by Hashim (2015) and Schulze (2018) claim that many small- and medium-sized enterprises (SMEs) do not have the resources or knowledge to manage the changes required to comply with privacy regulations by themselves. These types of companies also have a lack of standardization of processes (Supyuenyong et al., 2009), while full control and registration of every process that handles data is required per the GDPR. Innovation frequently acts as a crucial differentiator for startups, allowing them to compete with bigger, more firmly established firms in the market (Drucker, 1999). Established companies, to remain competitive and keep up with changing consumer preferences and technological advancements, must also constantly innovate (Tushman & O'Reilly, 2004).

In a 2018 study, before the implementation of the GDPR, Sirius concluded that the GDPR was a positive step that would finally encourage businesses to review their approach to data protection. However, this same flexibility of interpretation ran the risk of alienating smaller businesses, which lacked the resources needed to manage the additional overhead.

The evolution of privacy laws, from the most fundamental to the intricate regulations of GDPR, has been essential in preserving people's privacy in a world that is becoming more and more digital. The GDPR distinguishes out because it harmonizes these laws between

nations while putting a special emphasis on the rights of individuals. It holds businesses accountable for how they handle personal data, even those outside the EU.

2. Literature review

2.1. Introduction

In order to find relevant research regarding the topic and knowledge gaps that can help to identify the most relevant research question, a thorough search was made. Firstly, to explore the general topic of GDPR, a simple search in Scopus was initially made with the term GDPR. The search results served as the base data to build Relational Bibliometrics studies. The map shows relationships among scientific publications, and in this work was used to understand other relevant topics and keywords to help in finding relevant work. The map is displayed in Figure 1.

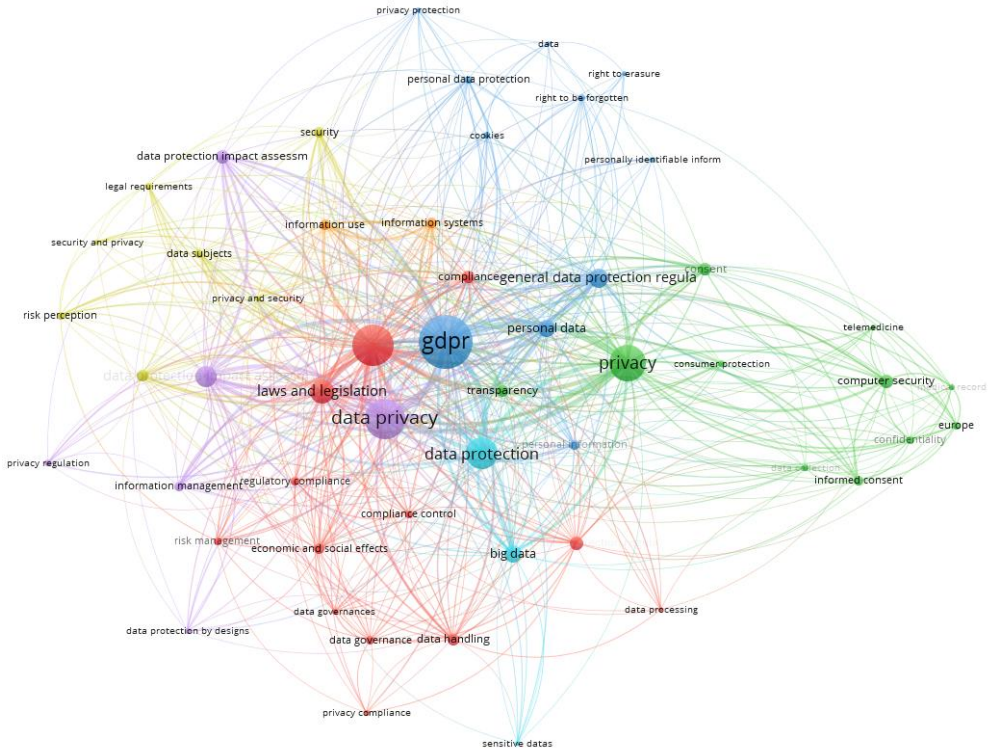


Figure 1. Bibliometrics Map used to find relevant keywords.

After carefully studying the map that showed connections between different GDPR research papers, several important words that helped guide the search were found. These words included "data privacy", "personal data protection", "data protection", "privacy", "cybersecurity", "data controllers", and "data subjects". To further narrow the result to the desired topics, words such as “startup” and “SMEs” were also added to the search. These words guided us through the large amount of GDPR research and helped us find areas that need more study.

2.2. Literature Review

The types of data organizations use, how they use it, and how they relate to end users vary greatly, and thus data protection regulations don't have a regular impact on companies (Martin et al, 2019). Chen (2022) and Peuker (2022) claim, for instance, that in the technological services spectrum, the GDPR was considerably more prejudicial to smaller companies when compared to tech giants such as Google or Amazon. The average impact on profits caused by the GDPR for tech companies in general was a reduction of 8% in profits, mainly to an increase in costs to comply with the regulations, but also a 2% reduction in sales (Chen et al, 2022). Chen states that in small companies this impact is doubled. While earlier research (Aridor et al., 2020; Jia et al., 2021) examined the effects of privacy regulation on online behavior and technology ventures, there is little systematic data on how businesses have fared and adapted to the GDPR outside of the technology sector.

The GDPR also seems to have had an important impact in reducing the likelihood of companies receiving money from venture capital (Kircher et al, 2021) and this has a direct effect on startups that tend to receive money from these means. This study was, however, the only one to clearly conclude this relationship between investment rounds and the GDPR. In addition, it focused only on United States-based startups.

There are a considerable number of studies (considering the novelty of the topic) that analyze the impact of the GDPR on AI technology and training. AI has become the main buzzword in the tech world recently, and the GDPR might present limitations on the development of the technology (Wallace et al, 2018). In a 2020 study, Bessen concludes that the reduced access to training data to run sophisticated algorithms, such as neural networks and ensemble learning, hinders the ability of some AI startups to prosper. His study also indicated an increased cost generated by the need to comply with regulations, which increases the difficulty for the long-term success of new companies in this field.

Another area that was explored by other researchers regarding this topic was the approach that startups have been using to ensure compliance with the GDPR. Li (2022) has deeply dived into the routines of a German startup to understand their approach and to identify issues the company and others face. There were identified three main issues: Reliance on manual tests, lack of awareness and knowledge of the privacy regulations, and balancing GDPR compliance with a business that relies on data.

Martin (2019) focused on how the implementation might impact innovation in startups, finding both positive and negative aspects related to the process of complying with the

GDPR. According to the research, despite the GDPR bringing innovation-constraining effects to the businesses such as abandonment, entrepreneurial discouragement, and data minimization, it can also result in some innovation-stimulating effects: compliance innovation, regulation-exploiting innovation, and "buying European".

Examining the complexities of GDPR compliance within small businesses, Li, Z. S. et al. (2022) identified three key challenges: a heavy dependence on manual GDPR testing procedures, a broad lack of knowledge concerning privacy obligations, and the ongoing struggle to maintain GDPR compliance in the highly competitive data market. Li's study draws parallels with the research conducted by Martin, N. et al. (2019), who explored how GDPR can simultaneously inspire and impede innovation within startup ecosystems. Both research projects underscore the need for broader and more diverse research in this realm.

Härting, R. et al. (2020) extended these findings by scrutinizing the variables that sway the integration of the GDPR into pre-existing business models of small and medium-sized enterprises (SMEs). The author highlights the challenges SMEs face when adapting to the regulation, such as high costs, insufficient provision of information, and the difficulty in adapting to the process.

Research conducted by Norval, C. et al. (2021) homed in on the readiness of tech startups – particularly those innovating at the cutting-edge and pushing the boundaries of technology - in managing data protection issues. This type of tech companies, typically lack established data protection best- practices (Norval et al. 2021). Their findings, resonating with the stress placed by Härting et al. 2020, on the importance of GDPR knowledge, demonstrated opportunities for these startups to enhance their GDPR compliance. Accordingly, they suggest that future research should delve into the practical implementation of 'data protection by design', offering guidelines for best practices and gauging the effectiveness of proposed solutions.

Friedewald, M. et al. (2022) further unpacked the concept of data protection by operationalizing Data Protection Impact Assessments with various stakeholders, spanning from startups and SMEs to corporations. This research builds upon the recommendations of Norval et al. (2021), offering a tangible tool to evaluate data protection strategies across various types of organizations. In parallel, Freitas, M. et al. (2022) explored the challenges SMEs encounter when ensuring GDPR compliance within their supplier network, revealing a profound knowledge gap and highlighting the demanding time commitment necessary to manage GDPR compliance.

Shifting the focus toward the impact of GDPR on AI, Wallace et al., (2018) expressed apprehension over the limitations imposed by the GDPR on AI advancement. The article proposes that the need to comply with the GDPR will:

1. Reduce AI accuracy and power
2. Raise the costs of AI development
3. Constraint innovation
4. Increase general regulatory risks for companies that aim to innovate in the field

This analysis was substantiated by Bessen et al. (2020) who conducted surveys to explore how the GDPR impacts the development of AI technologies, especially in terms of access to and usage of training data. The majority of the firms indicate that their training data is somehow affected by the GDPR, whereas companies located in the EU suffer a higher impact, since they often deal with more data from inside the European Union which is directly contemplated in the regulations (Bessen et al. 2020). For US firms, the need to comply with European Regulations may offer a barrier to reaching a customer base outside of the US (Bessen et al. 2020).

The influence of the GDPR on startup financing was the subject of Kircher et al. (2021) research. They conducted an empirical study on US-based app startups, finding a slight dip in venture capital transactions for these enterprises. As a limitation, their research underscores the need for future investigations that utilize more reliable data and offer a more comprehensive description of the businesses involved.

Peukert et al. (2020) observed the impact of GDPR on HTTP requests performed by websites, finding that the GDPR not only reduced the number of third-party entities receiving these requests but also reduced the market share of smaller firms. This effect aligns with the concerns raised by Johnson, G. et al. (2020), who discovered that the GDPR led to a concentration of personal data ownership and increased market power, opening new avenues for future research on the equilibrium between privacy and antitrust laws.

Research in this area is in its nascent stages, given that it's been less than four years since the GDPR was implemented. Companies, especially smaller ones, are still navigating through the adaptation process. According to Chen et al. (2022), smaller firms have experienced twice the decrease in profits and sales compared to larger corporations operating in the EU. This highlights the disproportionate effect of GDPR on SMEs, reinforcing the urgency for continued, detailed research in this area.

The journey to GDPR compliance is undoubtedly filled with hurdles, with issues ranging from reliance on manual testing to a significant lack of GDPR awareness. Nonetheless, a few studies, such as Martin et al. (2019), suggest that the GDPR might also spur innovative solutions to these challenges. Initial investigations have shed some light on the GDPR's impact on AI development, startup financing, and the competitive disadvantage of smaller web service providers. However, the full scope of GDPR's influence remains somewhat elusive.

It is pertinent to consider the geographical limitations of existing research, with many studies concentrated in the US and Germany. Additionally, the timing of these studies, many of which were conducted less than a year post-GDPR, also needs to be factored in. As the market matures in its understanding and adaptation to privacy regulations, revisiting and reassessing these initial findings will be crucial. The continual evolution of the privacy regulations landscape underscores the importance of comprehensive and ongoing research in this domain.

3. Methodology

3.1. Introduction

Given the existing literature and the knowledge gap identified, this research aims to understand how the need to comply with the GDPR hinders the development of technology startups that act in the EU. The research question proposed is:

How does the need to comply with the GDPR limit the development of technology startups in UPTEC?

The analysis and scope were developed using an iterative process as proposed by Hevner et. al., 2018. The adapted framework shown in Figure 2 displays the proposed Design Science methodology that was used to refine the research question and build the methodology.

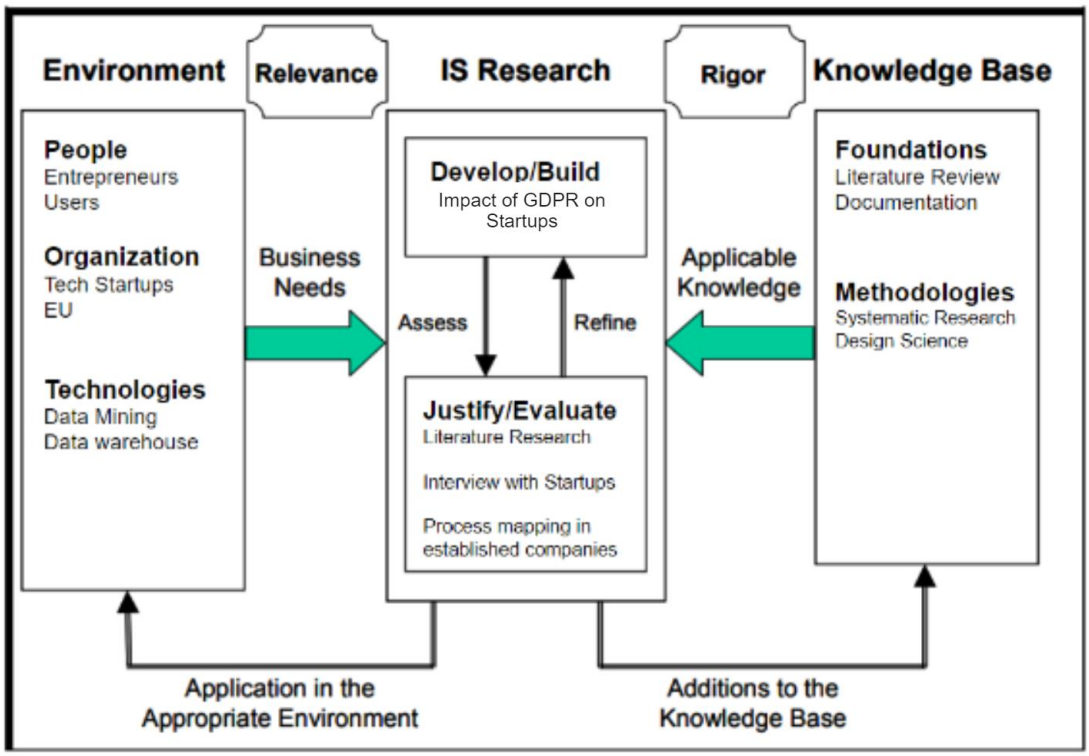


Figure 2. Design Science iterative process based on Hevner et al., 2018

The approach was defined be to lay the knowledge foundation by further thoroughly reading existing literature on the topic and the official documentation of the GDPR. The research method defined was quantitative research, based on a questionnaire run by startup founders, c-level and middle management, to validate the hypothesis to be explored.

This study explores three hypotheses with the selected businesses to understand how the GDPR affects its results and development.

3.2. Hypothesis

3.2.1. Costs

There are several ways the need to comply with the GDPR might increase company costs, especially if it collects or processes significant amounts of personal data. This can lead, for instance, to additional hiring costs for the company or the need for regular GDPR training for employees, since the GDPR requires companies to ensure that all employees who process personal data are adequately trained in data protection.

According to the Art. 37, companies can be required to have a DPO, independently of their size if:

1. The data processing is carried out by a public authority or body.
2. The organization's core activities require regular and systematic monitoring of individuals on a large scale.
3. If the organization's core activities involve the processing of special categories of data on a large scale, such as data related to racial or ethnic origin, political opinions, religious or philosophical beliefs.

Having an extra resource dedicated to this issue, especially for early-stage startups, might represent a significant rise in operational costs. Established companies, however, can most likely easily absorb this cost.

Additionally, companies may need to invest in new technologies to ensure compliance with the GDPR. For instance, they may need to update their data storage and security systems to ensure that personal data is adequately protected. Implementing data procedures for collecting and processing data adequately and having an overall compliant infrastructure might require significant work and extra costs for the company. Developing all the agreement procedures to obtain explicit consent from the user, as the GDPR states in Art. 7 can also be a time-consuming activity for any startup.

Art. 35 also lays the rules for the need for a Data Protection Impact Assessment (DPIA), which is needed for processing activities that are likely to result in a high risk to the rights and freedoms of individuals. This includes:

1. Evaluation or scoring, including profiling and predicting, especially if based on sensitive data or using new technological means.
2. Automated decision-making with legal or similarly significant effects.

3. Systematic monitoring of a publicly accessible area on a large scale.
4. Processing special categories of data on a large scale, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation.
5. Large-scale processing of personal data relating to criminal convictions and offenses.

Carrying DPIAs can incur significant extra costs and increase the time to market for a startup product. The fines imposed by the GDPR are very significant, including fines of 4% of the company's annual turnover. Any company must either have an appropriate legal team in place to ensure compliance or accept an increased risk of being fined.

The first hypothesis to be validated is that compliance with the GDPR creates significant extra costs for startups, which might hinder their development.

3.2.2. Innovation

The second hypothesis proposed suggests that the implementation of the GDPR may have an impact on the development and launch of new products in startups. Specifically, the hypothesis posits that startups may be deterred from pursuing certain product ideas due to the increased challenges and compliance requirements imposed by the GDPR.

One potential manifestation of this impact is the creation of additional obstacles for startups seeking to process large amounts of personal data in the development of their products. As the GDPR requires a significant number of resources and time to ensure compliance with its privacy regulations, startups may be faced with a more arduous task in launching a product that requires collecting and processing personal data. The extra effort required may prove to be too great for some startups, leading them to abandon the idea altogether.

This phenomenon may further exacerbate the already challenging situation that startups face when launching new products. Startups often operate under resource constraints and tight timelines, and the GDPR may introduce an additional layer of complexity and uncertainty that could negatively impact their ability to bring products to market. This may result in missed opportunities for innovation and economic growth, as startups opt to avoid the GDPR's requirements and pursue alternative product ideas that do not require the processing of personal data.

3.2.2. Growth

In line with the GDPR's restrictions, the third hypothesis of this study explores the potential challenges faced by entrepreneurs when they expand their line of already-available products or services. Startups looking to scale their businesses may face additional challenges as a result of the GDPR's clear requirements for consent, transparency, and user rights, particularly if the existing products and services significantly rely on the collecting of personal data.

In order to collect and process personal data about individuals, businesses must first obtain their express and informed consent, according to the GDPR. Users must be informed as to exactly what information is being collected, why it is being gathered, how it will be used, and, if at all, with whom it will be shared. Startups must have effective data handling procedures and transparent communication plans to meet these transparency requirements. These procedures and approaches may need to change in accordance with the product's growth, which could be challenging for startups as they frequently lack resources and have narrow profit margins.

The GDPR also emphasizes people's rights to control their personal data, including the ability to view their data, correct errors, request erasure, object to processing, and more. These data rights may impose extra obligations as companies develop and scale their businesses and as the volume of data processed and users subject to this regulation increases. Building and maintaining the infrastructure necessary to enable such significant data management may be difficult for startups, especially during their development phase.

When a product is expanded, it may also be necessary to work with new suppliers or third-party services, each of which has its own GDPR compliance obligations. Startups may find it difficult to ensure GDPR compliance across an expanding network of suppliers since it takes time and money that could be used for development and innovation.

The threat of non-compliance is yet another possible GDPR barrier to product expansion. The amount of data a product processes increases along with its usage, which increases the risk of data breaches and improper handling. The GDPR has severe penalties for non-compliance, which puts startups at serious financial risk. As a result, entrepreneurs may be discouraged from aggressively scaling their businesses or may be forced to devote resources to risk-reduction measures.

The third hypothesis investigates the many obstacles that the GDPR may present to the expansion of startups' current goods. The GDPR compliance process may reveal new

challenges for the growth and scaling phase of a startup's product or service, increasing complexity, resource requirements, and risk.

3.3. Research Design

To validate the three hypotheses, this work involved running a quantitative questionnaire with startups that might be directly or indirectly impacted by the GDPR. The approach used was based on suggesting the hypotheses to the respondents and collecting data to understand if these hypotheses can be validated by owners and managers of Portuguese startups. The target audience for the inquiry was predominantly CEOs and CTOs of startups, but also employees with upper-management roles. This demographic was defined to obtain a view on the hypothesis raised by the decision-makers of the companies, with the assumption that these have a better knowledge of how the GDPR and how it affects the business. To reach this target audience, the work was focused on startups incubated at UPTEC, the biggest incubator in the UPTEC. The audience was approached via Linkedin or personal messages to founders that were related to the researcher and the tutor. The survey was administered online with a questionnaire build on Tally in April and May of 2023.

The questionnaire was built with four main objectives in mind: company and respondent characterization; personal opinion on the GPDR impact on costs, innovation, and growth; general compliance of the company with the privacy regulation; and specifically inquiring the companies about the relevance of each of the hypotheses. This structure was defined to allow the observation of correlations between the views and opinions of the company's area of operation, size, and the respondent's role.

To achieve this goal, the questionnaire was divided into 6 sections, defined as follows.

Section #1 aimed to categorize the company and the respondent. The goal was to gather some basic information about the company, such as size and area of operation, allowing a better analysis of the company's experience with the GDPR. In addition, this section included questions to understand the position of the participant in the company and its general knowledge of the regulation and how it applies to the company in question. For this, each respondent was required to classify, on a scale from one to five, their general knowledge about the GDPR (at a personal level) and their specific knowledge about the GDPR's impacts on their companies.

The second section was built to obtain a more personal view of the respondents regarding the regulation. The objective was to understand if the respondents view the GDPR positively or negatively (concerning its impact on the companies and the users) and understand their level of agreement in relation to the three hypotheses raised by exposing each participant to statements that explicated each of the hypotheses. All the questions for these two first parts of the questionnaires were required of all respondents.

The following four sections were shown only to users that responded with a value of 2 or higher (on a scale from 1 to 5) to the following question in Section #1: "How familiar are you with how the GDPR affects your company's activity?". This was determined to exclude respondents that claimed to have very little or no knowledge at all about the regulations from answering more specific questions about how it affects their companies. The goal was to ensure that the facts brought by the respondent were in fact aligned with the company's real experience with the regulations.

The third segment of the questionnaire was designed with the intention of deciphering the companies' overall compliance status, the maturity of their compliance efforts, and their diligence in addressing the key aspects of the GDPR regulation. This included inquiries into whether the companies had appointed a DPO as stipulated by the law, whether they sought explicit user consent for data collection and processing, and whether they provided users with the option to request data erasure. This section served as a general survey of the operational terrain, situating the companies' GDPR adherence practices within the broader context of data privacy norms and obligations.

In an attempt to probe the potential influences of the GDPR on the business landscape, the succeeding three sections each targeted a distinct hypothesis introduced in this study.

Section four aimed to address the first hypothesis – that of GDPR precipitating increased costs. To explore this proposition, the section was designed to obtain insights into the respondents' experiences in their company, focusing particularly on whether the GDPR introduced significant additional costs for their startups by, for instance, raising legal consulting costs, demanding additional hires such as a DPO, or needing extra employee training. The intent was not only to gauge the financial implications of the regulation but also to derive a deeper understanding of how these costs might impact the overall sustainability and growth prospects of these young companies.

The fifth section of the survey turned its attention to the second hypothesis – the potential inhibiting effect of the GDPR on innovation. This segment sought to unearth the degree to

which the respondent's company had found the GDPR to be a significant point of consideration during the ideation process for new products or services. The goal here was to understand if the privacy regulations were seen as an obstruction, stifling creativity, and innovation, forcing products to be discarded due to elevated risk of non-compliance or whether they could be navigated in a manner conducive to growth and innovation.

Finally, **the sixth section** focused on the third hypothesis – the possibility that the GDPR creates additional hurdles to the expansion of a product or service. This final segment aimed to harvest insights into the real or perceived barriers that GDPR might impose on the path to business growth and scalability. The goal was to paint a clearer picture of how the landscape of startup growth and product development might be altered by these relatively new data protection regulations.

Table 1 presents a summary of each section as a quick-reference guide. In Appendix 1, the transcript of the questionnaire can be found, as well as a flowchart identifying the flow of the questionnaire for each participant.

Table 1: Questionnaire Overview

Section #	Content	Answers
1	Respondent/company characterization: • What's the area of operation and size of the company? • What's the level of personal knowledge of the respondent about the GDPR and how well it knows about its implementation in the company?	16
2	Personal View: • How does the respondent view the importance of the GDPR • From a personal perspective, how does the respondent think the GDPR might affect a startup in costs, product ideation and product growth	16
3	Company GDPR general compliance: • What's the maturity of the company regarding compliance with the GDPR? • Does the company fulfill basic GDPR requirements, such as having a DPO, explicitly requiring user consent for handling data, among others.	16
4	Costs: • Does the need to comply with the GDPR generate increased costs to the company and to what extent?	13
5	Product Innovation • Does the need to comply with the GDPR appear as a topic when ideating new products? • Does it hinder the development of new products or services in any way?	13
6	Product Growth	13

Section #	Content	Answers
	• Does the GDPR place and extra barrier for startups when growing a product or Service	

The questionnaire had a total number of 16 responses, with 3 respondents going over just the first two sections due to a lack of knowledge of how the regulation affects the companies they work own or work for. It is important to highlight that the small scale of this survey does not present statistically relevant results and should not be perceived as a definitive conclusion on the impacts of the GDPR on startups. Nonetheless, it can provide important insights on the topic.

Given the limited number of responses received, the approach to data analysis was defined accordingly, focusing primarily on descriptive analysis and qualitative interpretations. The following steps outline the methodology to be used for data analysis:

A study of the responses' descriptive content will follow. This procedure involves providing an accessible summary of each question's responses. For categorical responses, frequencies and percentages will be determined; for ordinal or interval responses, central trends like mean or median will be used.

Following this, the data will go through an exploratory analysis to find any patterns or trends. This step will include comparing results from various questionnaire parts and respondent groups, which will be distinguished by elements such as corporate characteristics and respondent responsibilities.

Graphical representations of the results will be produced to facilitate interpretation and communication. These include bar graphs, pie charts, or other visualizations that efficiently summarize and convey the survey results.

The results of this investigation will then be compared to previous works of literature. Due to the small sample size, a statistical comparison might not be possible, but qualitative parallels or differences can be identified. With the use of this exercise, the data may be interpreted in context, and links between the study's conclusions and the broader academic conversation can be made.

This strategy guarantees that the acquired data is carefully analyzed to uncover important insights while respecting the limitations of a limited sample size. The conclusions will act as an exploratory study and establish the foundation for subsequent research using larger samples.

4. Results Overview

4.1. Introduction

This section aims to explore the results obtained from the questionnaire sent to startup founders, c-level managers, and upper management. The questionnaire had a total of 16 responses. Company size ranged from small companies, with 1 to 5 employees, to relatively large enterprises, with over 100 employees, as suggested by Figure 4. The companies that took part in the survey were from various areas of operation, as indicated by Figure 7.1, with close to one-third being from IT and Software.

4.2. Company and respondent characterization

Figure 5 indicates the responses to the degree of indication of understanding of the GDPR at an individual level (vertical axis) and at a company level (horizontal axis), on a scale from one to five. Respondents that identify themselves as founders or C-level employees have a higher knowledge of the regulations for both universes. Three of the respondents had a very low score (<2) for both questions and thus only took part in the first two sections of the questionnaire.

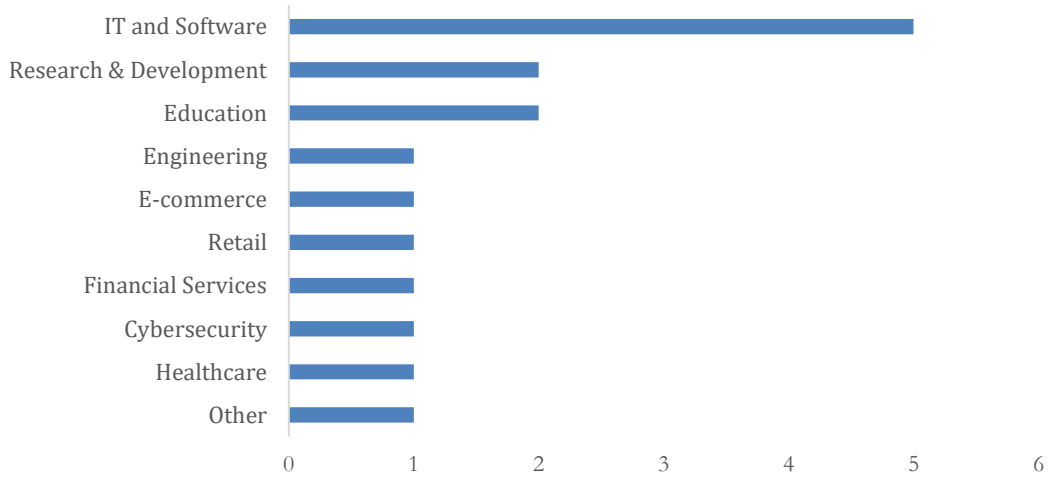


Figure 3. Companies' area of operation

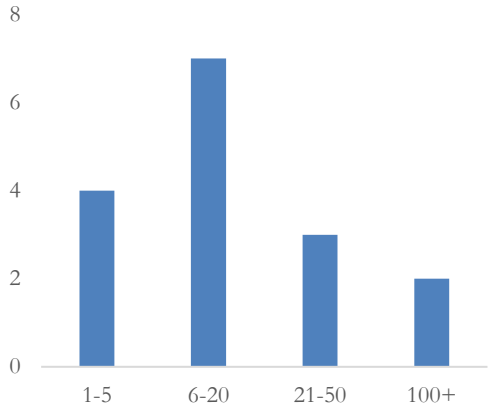


Figure 4. Company Size Distribution

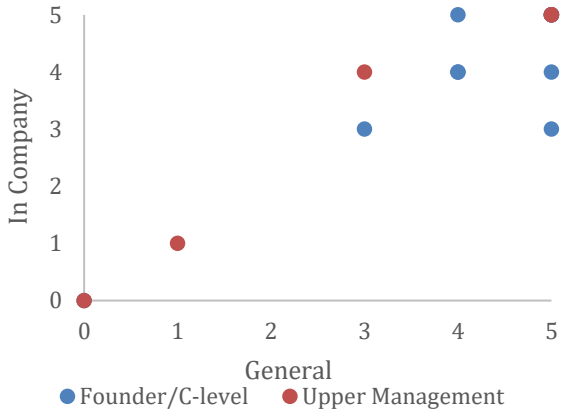


Figure 5. General knowledge of GDPR

For the second section of the questionnaire, the goal was to understand the personal view of the respondents on the GDPR and the three hypotheses raised. Figure 5 shows the vision of the 16 participants regarding the importance of every employee in the company having a general understanding of the data regulations. This is an important marker to better understand the characteristics of the respondents – the expectation is that companies that value the knowledge of the employee about the regulations might also allocate more resources to compliance training, for instance.

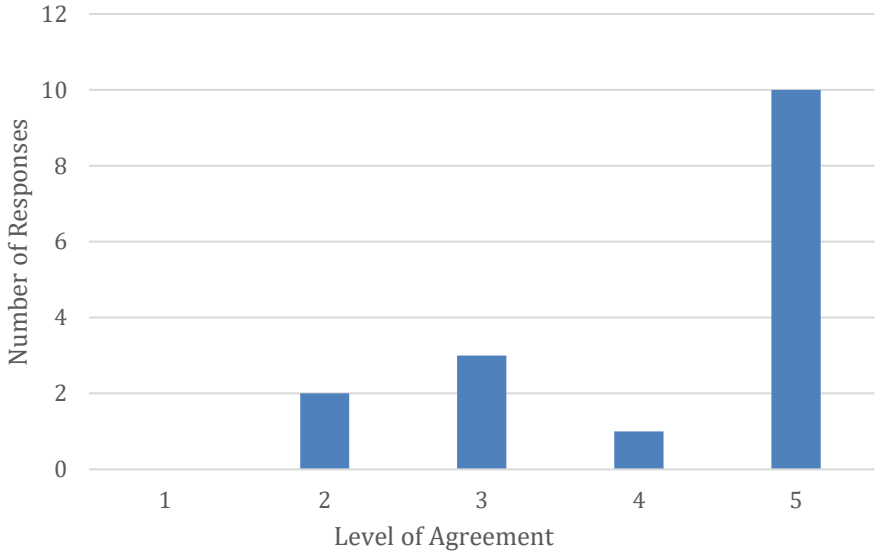


Figure 6. Responses to the question "how important do you think it is for a general employee to be aware of the GDPR and its impacts on the company?"

Regarding personal opinion on the first hypothesis – that the GDPR might increase costs in Startups in a relevant way, over 60% have a view that complying with the regulation generate slightly increased costs, but that are not relevant to the company's financials. Two interviewees suggested that the increased costs are high enough to be relevant, although one of them belongs to the group with very low knowledge of the regulation. When asked to indicate, on, a scale of one to five, the level of agreement with the statement "The GPDR is a burden to startups due to the extra costs it generates", the group that indicated that it has a big impact had a higher average (3.5), while the group that indicated that it has no impact had the lowest average (1.5), with the remaining group responding with an average value of 2.5.

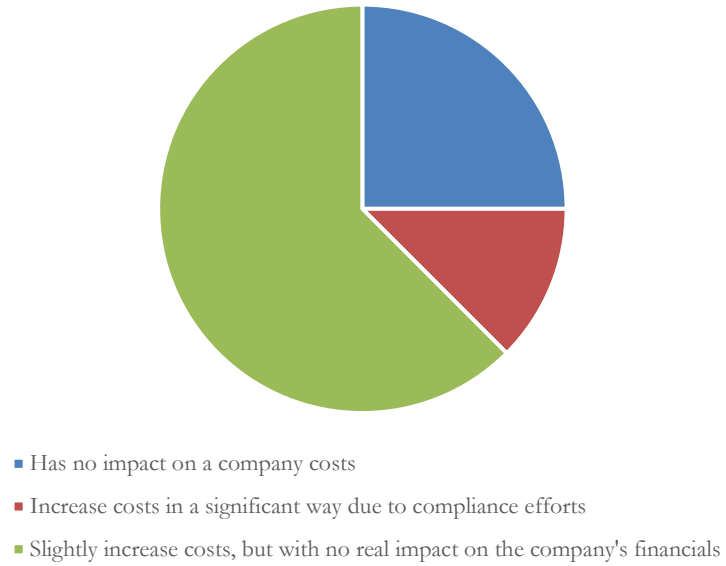


Figure 7. Distribution of opinions on GDPR's impact on costs

On the second hypothesis, the participants were asked if the GDPR should be considered when developing the idea for a new product or service. Seven of the respondents declared that the regulation should always be considered, while 3 of them claimed that there should be prioritization in the development of the product or service prior to the analysis of compliance. The respondents that answered that the GDPR should always be considered had a higher tendency to agree with the statement that claimed that the GDPR makes innovation more difficult due to the data collection and handling restrictions, as shown on Figure 8.

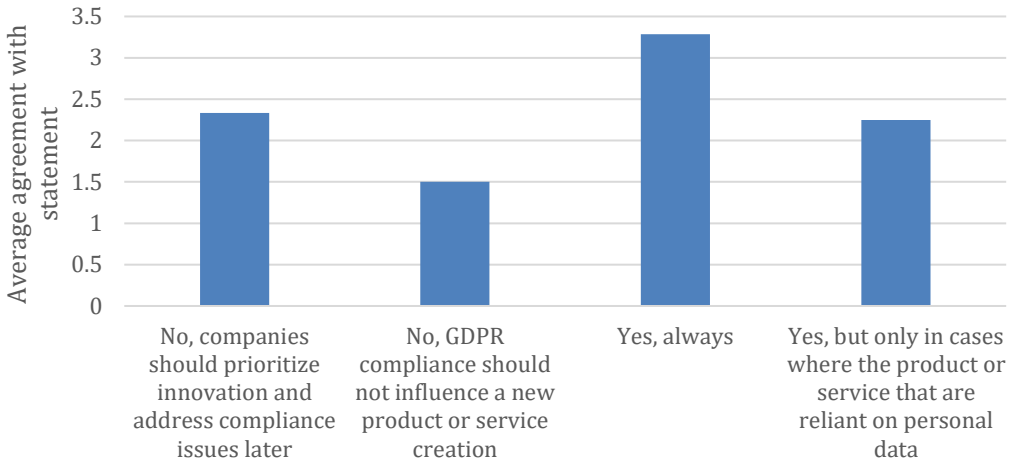


Figure 8. Average agreement with a statement (on a 0 to 5 scale) claiming the GPDR hinders innovation per vision on how the GDPR compliance influences product and service creation.

Regarding opinions on how the GDPR hinders growth, about a third of the respondents claimed that the GDPR impacts a company positively in the growth aspect, by fostering trust and ensuring responsible data practices. Half of the respondents indicated that there is no impact or neutral (doesn't incentivize nor hinder the growth of a company), while the rest indicated that the GPDR has a negative effect on the company's growth. Regarding agreeing with the statement "The GPDR makes it more difficult for Startups to grow its products and thrive", the scores were higher for participants that answered that the GDPR has a neutral impact on company growth, with a mean of 3.25. The lowest scores were attributed to the ones that indicated that the impact of the regulation is positive in this matter.

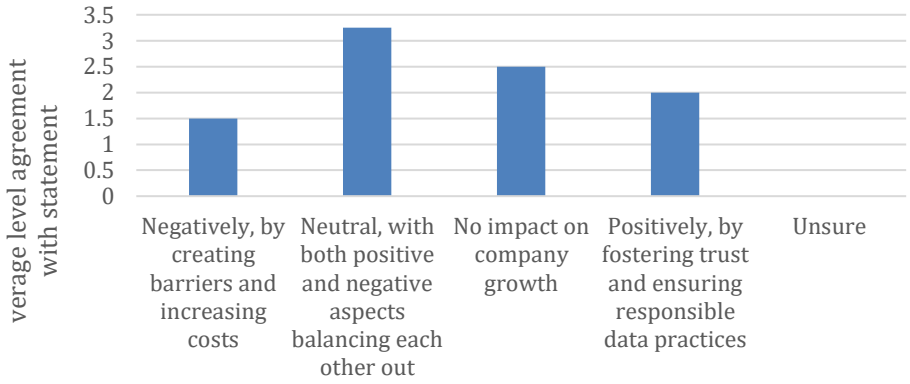


Figure 9. Average agreement with statement claiming the GPDR hinders growth per vision on how the GDPR affects company growth.

4.3. Company compliance characterization

From this section on, there's data for only 13 of the total 16 respondents, due to the lack of knowledge of the 3 about the state of GDPR compliance within their companies.

When asked if the company had a DPO assigned, 7 out of the 13 companies claimed to have a DPO assigned. Out of the 6 companies without a DPO, 3 claimed that there was no need for it according to the GDPR. One respondent claimed that it was never discussed in the company and that it wouldn't have resources available to make it a reality if needed.

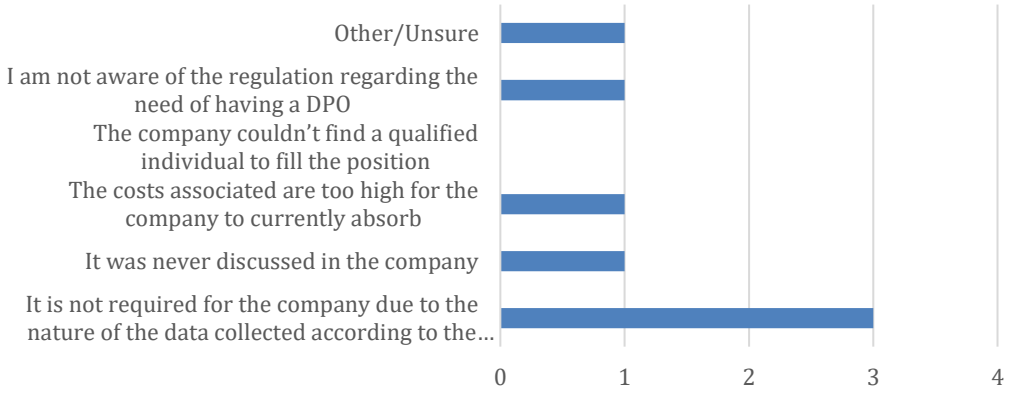


Figure 10. Distribution of reasoning for not having and assigned DPO in the company.

Regarding compliance efforts related to suppliers, 9 of the companies had established processes to ensure partners were compliant. When asked about the existing processes to obtain user consent, 85% claimed to have an established process for the matter. All the respondents claimed to fully fulfill the data subject's rights outlined in articles 15-22 of the GDPR (right to access, rectification, and erasure).

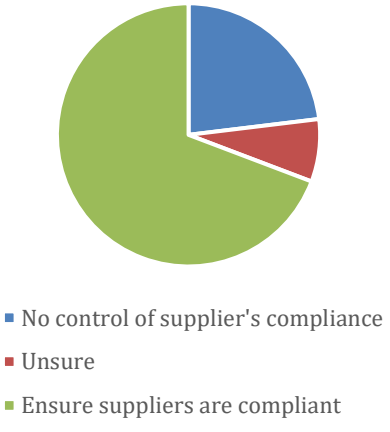


Figure 11. Control of suppliers' compliance.

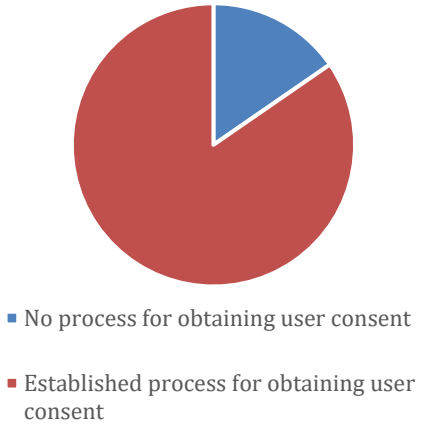


Figure 12. User consent obtention.

4.4. Hypothesis #1 – Cost

To evaluate the veracity of hypothesis #2 and understand the effects of the GDPR on startups, the research survey included questions designed to assess the experiences of these companies concerning regulatory compliance costs.

Participants were questioned specifically about whether compliance with GDPR had led to an increase in their company's operational costs. A notable finding from the survey was a mostly even split, with six respondents affirming an increase in costs due to GDPR compliance, while six others negated any such increase. One participant remained unsure, signifying a degree of ambiguity in discerning the financial implications of GDPR compliance.

Of the six participants who reported no escalation in costs, half asserted that their company had taken no special actions to achieve compliance with the GDPR. The other half offered a different perspective, stating that their company had been established with GDPR-compliant processes and data structures already in place. This illustrates that startups can employ different strategies to manage the costs associated with GDPR compliance, depending on their initial setup and operational model.

The respondents who reported an increase in costs due to GDPR compliance unanimously stated that the increase was minimal, accounting for between 0 and 5% of operational costs. These costs spanned legal, technical, administrative, and staff training expenses, offering a comprehensive view of the financial burden of GDPR compliance. The response distributions for reasons behind these increased costs are further detailed in Figure 13.

Crucially, all the respondents who reported increased costs highlighted a rise in legal and consultancy fees as a significant factor. Furthermore, five out of the six indicated that staff training and ongoing monitoring and auditing activities were areas where costs had increased due to GDPR compliance. This underlines the multifaceted nature of the GDPR's impact on startups, extending beyond pure financial costs to affect various operational areas.

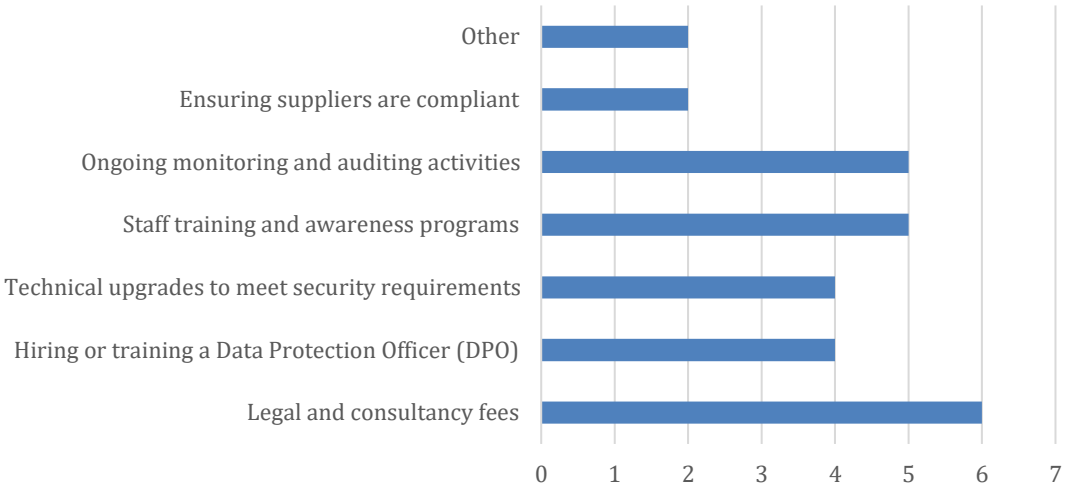


Figure 13. Increased costs generated by compliance with the GDPR.

4.5. Hypothesis #2 – Innovation

This hypothesis aimed to probe into the potential implications of existing privacy regulations on the innovation trajectory of startups. In order to validate or potentially discard the second hypothesis posited in this work, the survey incorporated queries revolving around the company's firsthand experience when brainstorming new products or services and the subsequent impact of the GDPR on the discussion, development, and eventual rollout of these new offerings.

The survey was particularly interested in investigating whether the GDPR and the associated compliance risks had led organizations to abandon or reconsider the conception of new products or services. To this end, the survey found that only two out of the total of thirteen participants confirmed that they had indeed abandoned or rethought new product or service ideas because of potential GDPR compliance risks. This is a noteworthy finding, as it indicates that while GDPR compliance is a significant consideration, it apparently does not necessarily throttle innovation within most of these companies.

When the participants were questioned on why the GDPR was not deemed a critical topic, the predominant response was that while the GDPR was certainly a topic of discussion and was identified as a potential risk, the businesses consciously decided not to discard any product or service ideas on the basis of GDPR compliance risks alone. This viewpoint is illustrated in Figure 14. Interestingly, a couple of interviews indicated that the GDPR was not a topic of discussion during the ideation stage of product development. These responses came from companies operating in two sectors — IT and R&D — in which the GDPR is

expected to have substantial implications. This demonstrates that the interpretation and application of GDPR compliance vary greatly across different sectors and individual companies.

As for the frequency with which the topic of GDPR compliance was raised during product or service ideation and development discussions, the respondents declared that it was a very recurrent subject. This underscores the pervasiveness of GDPR considerations in the contemporary business landscape, particularly within startups that are in the process of developing and introducing new products or services to the market.

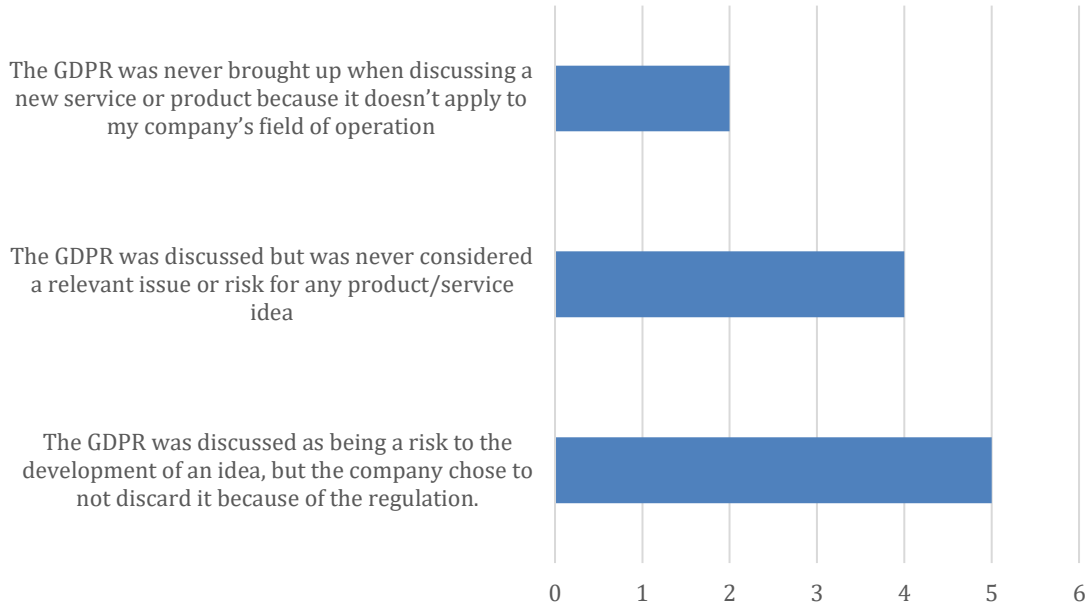


Figure 14. Reasons given for not discarding products/services due to GDPR compliance efforts.

4.6. Hypothesis #3 – Product Growth

The research survey aimed to gather insights from participants on the impact of regulatory compliance, specifically regarding the GDPR on product or service growth. In order to delve into this aspect, participants were queried about their experiences concerning any barriers they may have encountered in the expansion or growth of their products or services due to compliance issues related to the European Union's key privacy regulation. A significant majority of the respondents, 11 out of 13, conveyed that they had not faced any situations where GDPR compliance was perceived as a blocker to their product or service growth. For

four of these companies, not worrying about GDPR compliance was a business decision, choosing to focus on the growth of the product or service despite the challenge imposed by the regulation. These companies decided to continue to expand their product or service offerings, focusing on growth trajectories despite the complexities and challenges associated with GDPR compliance. This decision might be perceived as risky, yet it evidently showcases a proactive risk management strategy in navigating the GDPR compliance landscape.

In contrast, for another five of these companies, their products were already designed to be GDPR compliant from the outset. Therefore, their growth trajectory didn't involve additional compliance requirements or subjecting their operations to new clauses of the regulatory body. This represents a proactive approach, integrating regulatory compliance into the design and development process, effectively reducing future regulatory compliance burdens.

However, there were indeed a small proportion of participants who viewed GDPR compliance as a significant barrier to their company's growth. For these respondents, the primary challenges cited were the cross-border data transfer restrictions stipulated in Chapter 5 of the GDPR, and the security of processing mandates as defined in Article 32. These issues represent significant hurdles to overcome, signaling the need for companies to devise effective strategies to address these challenges while ensuring continued growth.

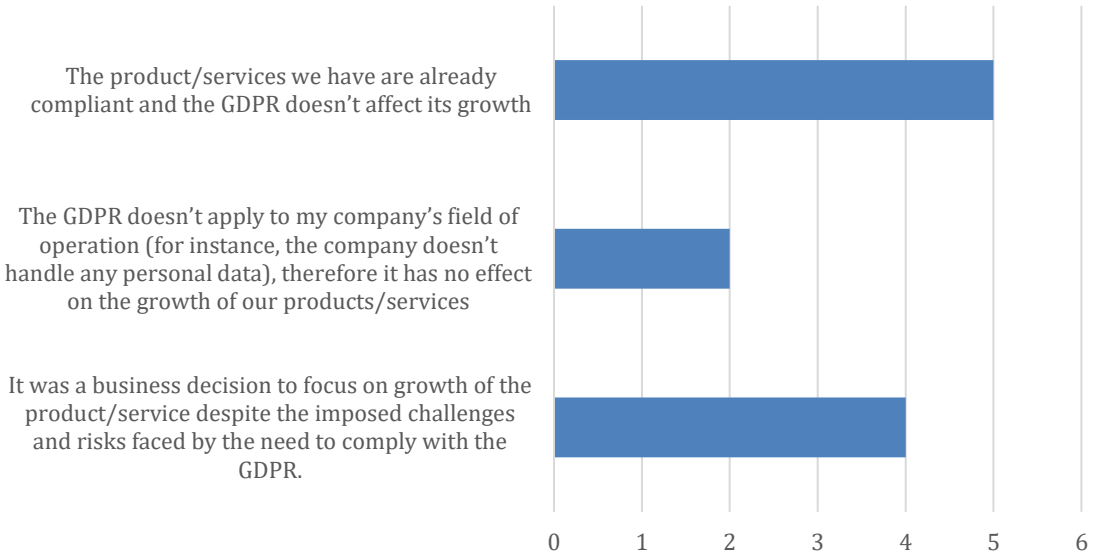


Figure 15. Reasoning perceived for product/service growth not being affected by the GDPR.

5. Discussion

This research aimed to understand the impact of the GDPR on startups, specifically examining its effects on operational costs, innovation, and growth, which were the three hypotheses raised to be validated in the study. As with any study, it is crucial to consider the limitations which may affect the interpretation and generalization of the results.

One of the most significant limitations of this study is the small sample size. With only 16 responses received, this investigation provides merely a preliminary insight into the impact of GDPR on startups. Due to this small number of respondents, the findings of this study are not conclusive and should be used primarily for exploratory purposes. A larger sample size would be needed to make substantial assertions and achieve statistical significance, thereby enhancing the reliability of the results.

Additionally, geographical limitations must be considered. All the companies included in this study were incubated in UPTEC. As GDPR applies throughout the European Union (including countries in other regions that ingest or process data from EU citizens), perceptions and impacts of the regulation by the companies could differ significantly across member states due to cultural, economic, and legal differences. Similarly, companies outside the European Union, who also must comply with GDPR when dealing with EU residents' data, may face additional challenges, specifically related to cross-border data transfers, which were not assessed in this study and might represent significant barriers regarding the hypotheses raised.

The third major limitation is the methodological approach adopted. The study relied solely on quantitative data collected through a questionnaire, with no qualitative interviews conducted to provide an in-depth understanding of the respondents' perceptions and experiences. The absence of qualitative data, which could add more depth and context to the responses, may limit the interpretation of the findings – especially due to the low sample size, since nuances regarding the way the questions were interpreted cannot be evened out as it is expected with a larger population.

Other potential limitations might include the risk of self-selection bias, which can occur when participants have the option to decide whether to participate in a study. In such cases, the results may not accurately reflect the entire population's views. Also, the study does not employ an objective measure of GDPR understanding, which could impact the self-reported knowledge and perceptions of GDPR, and consequently, the results. Again, this impact could potentially be lowered by interviewing a larger population.

Despite these limitations, the study still provides several valuable insights into the challenges startups face in the context of GDPR compliance. A notable finding is that respondents who identified themselves as founders or C-level employees reported higher levels of GDPR understanding. This underscores the importance of promoting GDPR knowledge across all levels of the organization, as a comprehensive understanding can contribute to better compliance and more informed decision-making. It is important to highlight that among the respondents there is a significant level of self-reported knowledge about the regulations, indicating that it might be an important characteristic for a startup founder and that it is a topic that is relevant to any startup company.

As for the financial implications of GDPR, the survey reveals a nuanced picture. While a majority of respondents indicated that compliance with the regulation caused a minor increase in costs, a small fraction reported perceiving a more significant impact. The varying responses suggest that startups have adopted different strategies to manage compliance costs, based on factors such as their business model, the nature of their data processing activities, and available resources. A significant number of respondents claimed to have built compliant products from the start, indicating that it is a relevant topic when ideating new products. This was confirmed by answers to the section that addresses how the GDPR relates to innovation – 9 of 11 companies discuss the GDPR as a relevant factor when ideating and building a new product or service.

The survey findings also shed light on how GDPR can affect the innovation processes in startups. While most respondents indicated that the regulation is part of the when developing new products or services, some pointed out that it should be a primary consideration and risk to be considered while others suggested that the focus should initially be on product or service development before considering compliance requirements. This shows the diverse approaches companies are taking to balance innovation with GDPR compliance and reflects the complex interplay between data protection and product development.

In terms of growth, most respondents perceive GDPR as either having a positive or neutral impact. Those who viewed GDPR as a positive factor attributed this to the trust-building benefits of GDPR compliance. Those who viewed it as neutral saw GDPR as an essential part of doing business that does not significantly affect their growth strategies. However, a small number of respondents perceived GDPR as a barrier to growth, showing that its effects on expansion efforts can vary widely depending on individual companies' perspectives and circumstances.

Lastly, the study provides an overview of the state of GDPR compliance among the responding startups. While most companies appear to have made efforts to comply with GDPR, there is wide variation in how certain requirements, such as the need for a designated DPO, are interpreted and implemented. This variation highlights the inherent complexity of GDPR and the challenges startups face in ensuring compliance.

Building upon the insights from the literature, the results of this study resonate with the findings of Li et al. (2022) who identified dependence on manual GDPR procedures and lack of privacy knowledge as major challenges for small businesses. The respondents in this study, particularly those identifying themselves as founders or C-level employees, expressed a significantly high level of understanding of GDPR, while upper-management employees indicate a lower self-reported knowledge of the regulation, which may suggest an over-reliance on a few key individuals for compliance. Nonetheless, it as a consensus that there is a great importance in training the employees of the company on the regulation and the compliance rules, and most of the respondents assigned this responsibility to either the company or the company and the EU, as the regulator.

The varying perception of the impact of GDPR on innovation found in our study echoes the results of Martin et al. (2019), who found that GDPR can both inspire and impede innovation within startup ecosystems. The differences in approaches to incorporating GDPR into product or service development reflect the complexity of balancing innovation with data protection obligations. The responses noted in this study were significantly distributed between companies that consider the GDPR when ideating new products and have discarded ideas due to difficulty of compliance and companies that have discussions regarding the regulations but chose, as a business decision, to not let compliance interfere with early-stage development of product or services. Ideally, in further studies, a qualitative approach should be taken in order to dive deeper into how the participants that consider or not the GDPR when ideating new product and service ideas.

The findings in this study around the cost implications of GDPR compliance don't fully resonate with Härting et al. (2020), who discussed high costs and process adaptation complexity among the challenges faced by SMEs. Our survey results suggest a mixed picture, with several companies indicating a minor or non-existing increase in costs and reporting no significant impact of the need to comply with the GDPR on the company costs, while other participants indicated a significant impact. This is an early indicative of the varying perceptions and strategies adopted by startups to manage compliance costs.

The findings around the readiness of startups in handling data protection issues align with Norval et al. (2021), who emphasized opportunities for tech startups to improve their GDPR compliance. The disparity in our respondents' implementation of certain GDPR requirements, such as the need for a designated DPO, underscores the need for further practical guidance on 'data protection by design', as suggested by Norval. Interestingly, all companies claimed to be able to fulfill all data subject's rights, such as the right to access, rectification, and erasure – even the ones that claim not having an established process for ensuring suppliers are GDPR compliant. This reinforces what is claimed by Norval, regarding the need for increased attention, support, and scrutiny to raise the standard of data protection in startups.

The research of Friedewald et al. (2022) on the operationalization of Data Protection Impact Assessments (DPIAs) provides a tangible tool that could benefit the startups in our study, especially those struggling with GDPR compliance within their supplier network, a challenge highlighted by Freitas et al. (2022). Our results indicate that while most startups are making efforts to comply with GDPR, there is wide variation in the interpretation and implementation of its requirements, supporting the need for such practical tools.

Looking at the impact of GDPR on AI, as discussed by Wallace & Castro (2018) and Bessen et al. (2020), our study did not specifically explore this area. However, considering the concerns raised about the potential stifling of innovation and escalated costs, it would be worthwhile to examine this impact in future research involving startups engaged in AI technologies.

The perceived impact of GDPR on growth aligns with the findings of Kircher and Foerderer (2021) regarding the potential constraints of GDPR on startup financing. While most of our respondents perceived GDPR as either having a positive or neutral impact, a small number saw it as a barrier to growth, indicating potential limitations to access to capital and resources.

The effect on third-party entities reported by Peuker et al. (2020) and the concentration of personal data ownership found by Johnson et al. (2020) could also have implications for the startups in our study, especially those that rely on third-party data or are in the early stages of growth. Our results do not directly address this issue, but future studies could delve into these aspects.

Finally, this study supports the findings of Chen et al. (2022) concerning the disproportionate effect of GDPR on smaller firms. Our results show a range of impacts, both positive and negative, that GDPR has on startups, suggesting a need for additional support and resources

for these companies. Given the geographical limitations of our study and those in the literature, future research should aim for a deeper study within a broader geographical scope to capture the varied impacts of GDPR across different regions and cultures.

6. Conclusion

The GDPR was instituted by the European Union to provide comprehensive protection for user data, enhance transparency, and ensure the privacy rights of individuals are respected by companies operating within its jurisdiction. While its implications are sweeping across industries of any size, this study specifically focuses on how it affects startups within the European Union.

The review of the literature highlighted the potential for the GDPR to impact startups in three main areas: costs, innovation, and growth. While GDPR was designed with the positive intention of protecting user data, its potential impact on these areas could potentially hinder startups' ability to thrive.

The first hypothesis investigated whether compliance with the GDPR creates significant extra costs for startups, potentially hindering their development. The GDPR's rigorous requirements can potentially necessitate hiring new employees, investing in training and new technologies, implementing data procedures, and carrying out Data Protection Impact Assessments (DPIAs). In addition, startups could face substantial fines in case of non-compliance, necessitating a strong legal team or acceptance of a higher risk of fines.

The second hypothesis explored whether the GDPR could impact innovation by creating obstacles for startups seeking to process large amounts of personal data in their products' development. Given that startups often operate under resource constraints and tight timelines, the GDPR could introduce an additional layer of complexity and uncertainty that could deter innovation and economic growth.

The third hypothesis examined whether the GDPR creates additional barriers to the expansion of a startup's product or service. The GDPR's clear requirements for consent, transparency, user rights, and the potential for severe penalties for non-compliance, could pose significant challenges for startups aiming to scale their businesses.

To test these hypotheses, a quantitative questionnaire was administered to Portuguese startups. The questionnaire focused on understanding the company's and the respondent's profile, their perspective on the GDPR and its impact, their level of compliance, and their views on each of the specific hypotheses. A limitation of the study was the small sample size, which doesn't allow for statistically significant results. Nevertheless, the data collected serves as an exploratory study that provides insights into the impact of the GDPR on technology startups.

Regarding the first hypothesis, which suggested that GDPR might significantly increase costs for startups, the responses demonstrate that GDPR compliance indeed contributes to increased costs, although with minimal impact on the overall operational expenses. However, there was a clear consensus that such expenses, predominantly related to legal, consultancy, and staff training, were necessary to ensure compliance.

With respect to the second hypothesis, the assumption that GDPR may hinder innovation, the responses were quite enlightening. Although the GDPR has an undoubted influence on the development of new products or services, this influence does not necessarily result in a decrease in innovation. Rather, GDPR is a regular topic of discussion during the ideation process, helping to guide the development of new products or services with compliance in mind. Therefore, while it is an important factor to consider, it does not necessarily stifle creativity or deter the evolution of new ideas.

Concerning the third hypothesis, on whether GDPR hampers startup growth, most respondents conveyed that GDPR did not hinder the expansion or growth of their products or services. Despite the complexities associated with GDPR compliance, most startups managed to navigate through the regulatory landscape without it being a barrier to their growth. For some, their products were designed to be GDPR compliant from the outset, showcasing a proactive approach to integrating compliance with the design and development process.

In summary, while the GDPR has indeed introduced new challenges and complexities, it does not necessarily stifle startups' innovation, growth, or impose unbearable costs. Rather, it necessitates a comprehensive understanding of the regulations, a focus on compliance, and the strategic incorporation of these requirements into business operations. Hence, startups must prioritize awareness and understanding of GDPR to navigate the regulatory landscape effectively. Ultimately, GDPR compliance can serve as a differentiator for startups, instilling trust among customers and fostering responsible data practices.

6.1. Limitations and Further Work

This study was limited to a small sample size of Startups incubated in a single accelerator in the north of Portugal (UPTEC). With the low number of respondents, this research is unable to present a statistically relevant conclusion to the research question. Building upon these limitations, several recommendations can be suggested for future studies to explore the impact of GDPR on startups in a more comprehensive and in-depth manner:

Expand the sample size: One of the main limitations of this study was the small sample size, which may not be representative of all startups. Future studies should aim to involve more participants to achieve statistical significance and enhance the reliability of the results and allow for the verification of stronger correlations in the data acquired. A larger sample size would provide a more comprehensive picture of how startups perceive and are influenced by GDPR.

Broaden the geographical scope: The current study was limited to startups incubated in UPTEC. Future research should consider conducting a comparative study across different regions or countries in the European Union. This can help identify if cultural, economic, or legal differences influence startups' perception and management of GDPR. Furthermore, it would be interesting to include companies outside the EU, who must also comply with GDPR when dealing with EU residents' data, to understand their unique challenges and experiences with GDPR compliance.

Incorporate qualitative data: Future studies should consider employing a mixed-methods approach that combines both quantitative and qualitative data. This could include conducting in-depth interviews or focus groups with startup founders and managers to gain deeper insights into their experiences and perceptions of GDPR compliance. Qualitative data can provide rich, contextual information that complements quantitative findings, helping to paint a fuller picture of the impact of GDPR on startups.

Focus on specific aspects of GDPR: Lastly, considering the breadth of GDPR, it might be valuable for future research to focus on specific aspects of the regulation, such as data subject rights, the role of a DPO, or cross-border data transfers, among others. Understanding how startups navigate these specific requirements could provide more targeted insights to guide best practices for GDPR compliance.

By addressing these limitations and incorporating these recommendations, future studies could contribute further to the understanding of GDPR's impact on startups, thereby aiding these organizations in navigating the GDPR landscape effectively and responsibly.

References

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*.

Brodin, M. (2019). "A framework for GDPR compliance for small-and medium-sized enterprises". *European Journal for Security Research*, 4, 243-264.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. EUR. (1995, October). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

Drucker, P. F. 1. (1999). "Innovation and entrepreneurship: practice and principles". *New ed. Oxford, Eng. ; New York, Elsevier Butterworth-Heinemann.*

Freitas, P. M. (2018). "The General Data Protection Regulation: an overview of the penalties' provisions from a Portuguese standpoint". *UNIO – EU Law Journal*, 4(2), 99–104. https://doi.org/10.21814/unio.4.2.10

Friedewald, M., Schiering, I., Martin, N., & Hallinan, D. (2022, February). "Data Protection Impact Assessments in Practice: Experiences from Case Studies". In *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers* (pp. 424-443). Cham: Springer International Publishing.

General Data Protection Regulation Official Legal Text. (2022, September 27). Retrieved November 13, 2022, from https://gdpr-info.eu/

Härting, R. C., Kaim, R., & Ruch, D. (2020). "Impacts of the Implementation of the General Data Protection Regulations (GDPR) in SME Business Models—An Empirical Study with a Quantitative Design". In *Agents and Multi-Agent Systems: Technologies and Applications 2020: 14th KES International Conference, KES-AMSTA 2020, June 2020 Proceedings* (pp. 295-303). Springer Singapore.

Härting, R. C., Kaim, R., & Ruch, D. (2020). "Impacts of the Implementation of the General Data Protection Regulations (GDPR) in SME Business Models—An Empirical Study with a Quantitative Design". *In Agents and Multi-Agent Systems: Technologies and Applications 2020: 14th KES International Conference, KES-AMSTA 2020, June 2020 Proceedings* (pp. 295-303). Springer Singapore.

Hashim J. (2015). "Information communication technology (ICT) adoption among SME owners in Malaysia". *Int J Bus Inf* 2(2):221–240

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2008). "Design science in information systems research". *Management Information Systems Quarterly*, 28(1), 6.

Kircher, T., & Foerderer, J. (2021, December). "Does EU-Consumer Privacy Harm Financing of US-App-Startups? Within-US Evidence of Cross-EU-Effects". *In Proceedings of the 42nd International Conference on Information Systems (ICIS)* (pp. 12-15).

Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). "The EU General Data Protection Regulation: A Commentary/Update of Selected Articles". *Update of Selected Articles (May 4, 2021).*

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). "Towards privacy compliance: A design science study in a small organization". *Information and Software Technology*, 146 doi:10.1016/j.infsof.2022.106868

Luysterborg, E. (2017). "The Deloitte General Data Protection Regulation Benchmarking Survey". Retrieved November 13, 2022, from https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/emea-gdpr-benchmarking-survey.pdf

Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). "How data protection regulation affects startup innovation". *Information Systems Frontiers*, 21(6), 1307-1324. doi:10.1007/s10796-019-09974-2

Norval, C., Janssen, H., Cobbe, J., & Singh, J. (2021). "Data protection and tech startups: The need for attention, support, and scrutiny". *Policy and Internet*, 13(2), 278-299. doi:10.1002/poi3.255

OECD (2002), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris, https://doi.org/10.1787/9789264196391-en.

Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2020). "European privacy law and global markets for data". *Center for Law & Economics Working Paper Series*, 1.

Schulze H., (2018). "GDPR compliance report". Retrieved 3 May 2023, from https://crowdresearchpartners.com/portfolio/gdpr-compliance-report/

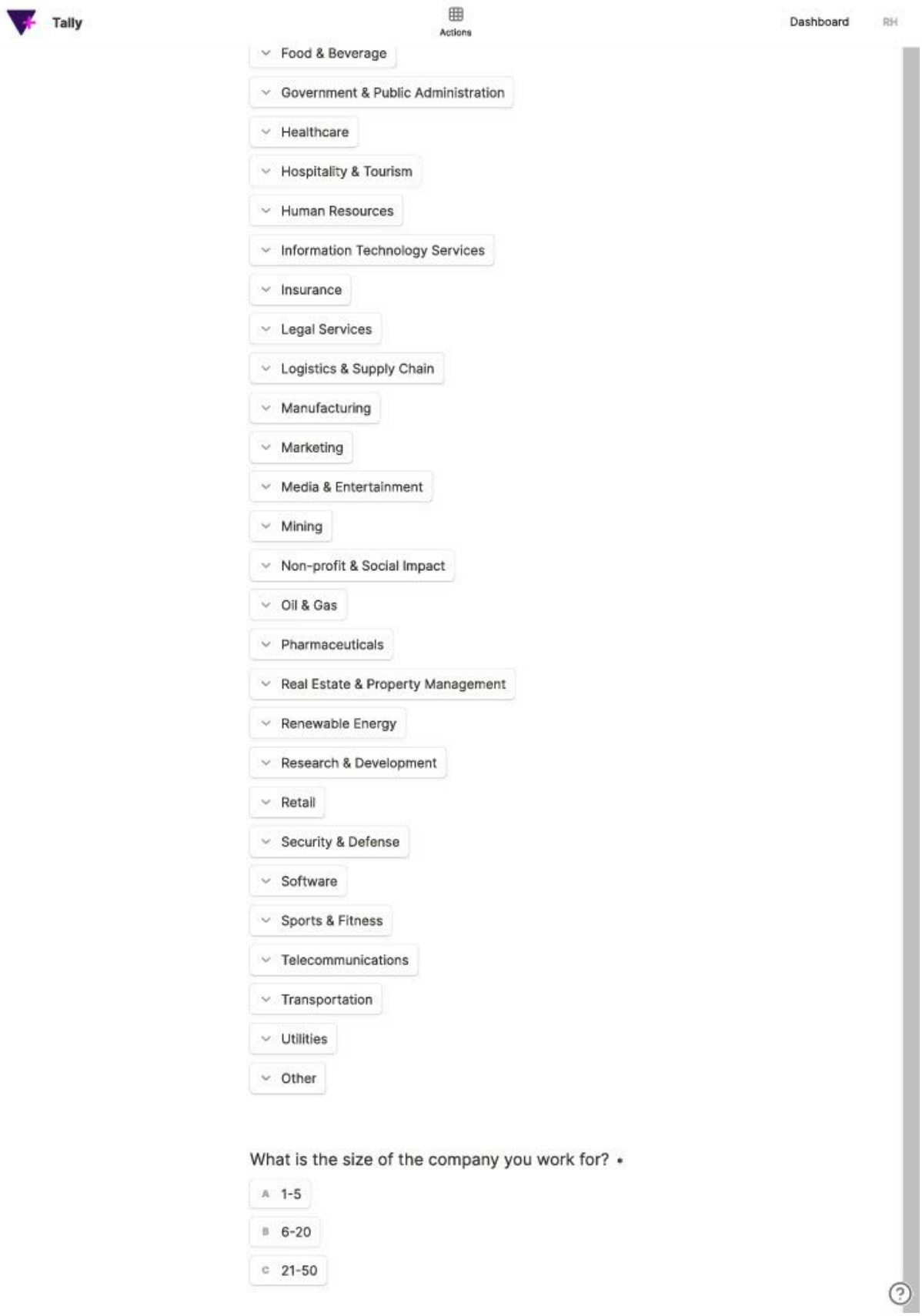
Supyuenyong, V., Islam, N., & Kulkarni, U. (2009). "Influence of SME characteristics on knowledge management processes: The case study of enterprise resource planning service providers". *Journal of Enterprise Information Management.*

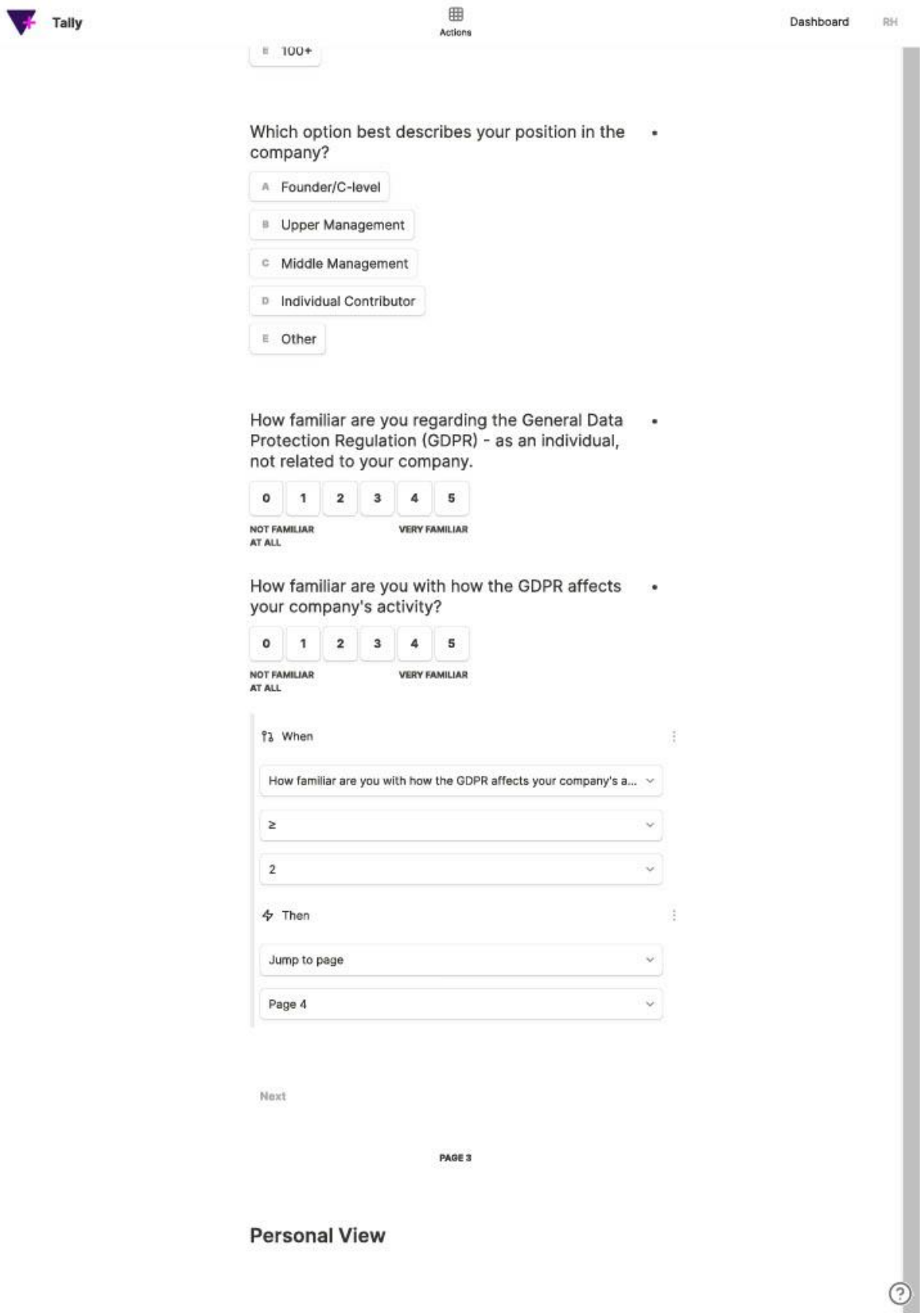
Tushman, M., & O'Reilly, C. (2004). "The ambidextrous organization". *Harvard Business Review*. https://hbr.org/2004/04/the-ambidextrous-organization

Voigt, P., & Von dem Bussche, A. (2017). "The EU general data protection regulation (GDPR)". *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, *10*(3152676), 10-5555.

Wallace, N., & Castro, D. (2018). "The impact of the EU's new data protection regulation on AI". *Center for Data Innovation*, 27.14

Appendix 1 – Full Questionnaire


Tally
Actions
Dashboard
RH
Food & Beverage
Government & Public Administration
Healthcare
Hospitality & Tourism
Human Resources
Information Technology Services
Insurance
Legal Services
Logistics & Supply Chain
Manufacturing
Marketing
Media & Entertainment
Mining
Non-profit & Social Impact
Oil & Gas
Pharmaceuticals
Real Estate & Property Management
Renewable Energy
Research & Development
Retail
Security & Defense
Software
Sports & Fitness
Telecommunications
Transportation
Utilities
Other
What is the size of the company you work for? •
A 1-5
B 6-20
C 21-50


Tally
Actions
Dashboard
RH
E 100+
Which option best describes your position in the company?
A Founder/C-level
B Upper Management
C Middle Management
D Individual Contributor
E Other
How familiar are you regarding the General Data Protection Regulation (GDPR) - as an individual, not related to your company.
0 1 2 3 4 5
NOT FAMILIAR AT ALL
VERY FAMILIAR
How familiar are you with how the GDPR affects your company's activity?
0 1 2 3 4 5
NOT FAMILIAR AT ALL
VERY FAMILIAR
When
How familiar are you with how the GDPR affects your company's a...
≥
2
Then
Jump to page
Page 4
Next
PAGE 3
Personal View

On a scale of 1 to 5, how important do you think it is for a general employee to be aware of the GDPR regulations and its impacts on the company?

0 1 2 3 4 5

NOT IMPORTANT AT ALL — EXTREMELY IMPORTANT

Who should be responsible for transmitting the knowledge to company's contributor? *

A The EU, as the Regulator
B The company
C Both the company and the regulatores
D The contributor should seek knowledge by themselves
E Other/Unsure

Regarding Company Costs, how do you feel the need to comply with data privacy regulations might affect your company? *

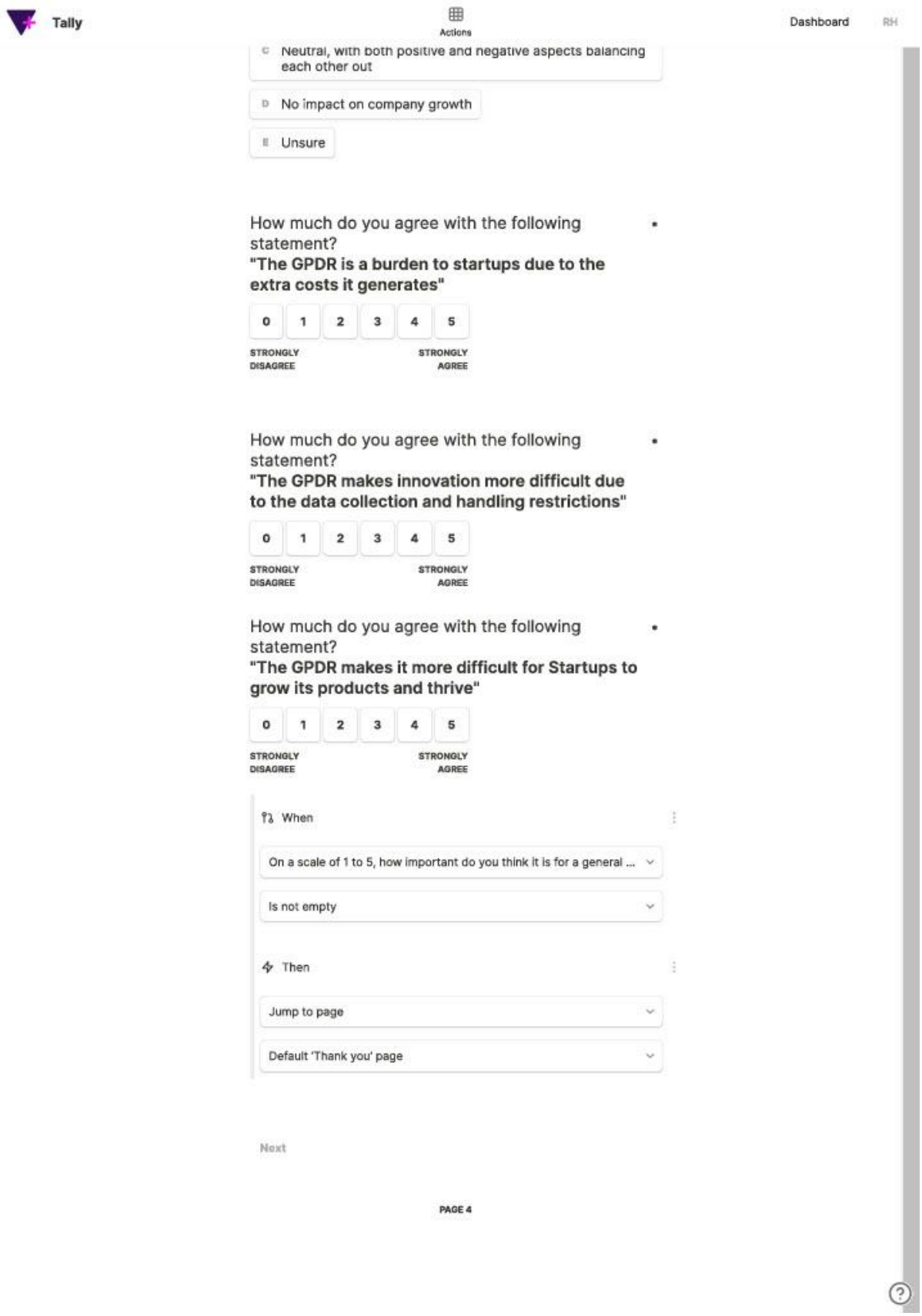
A Increase costs in a significant way due to compliance efforts
B Slightly increase costs, but with no real impact on the company's financials
C Has no impact on a company costs
D Decrease costs, reducing the risks of fines or legal actions by customers

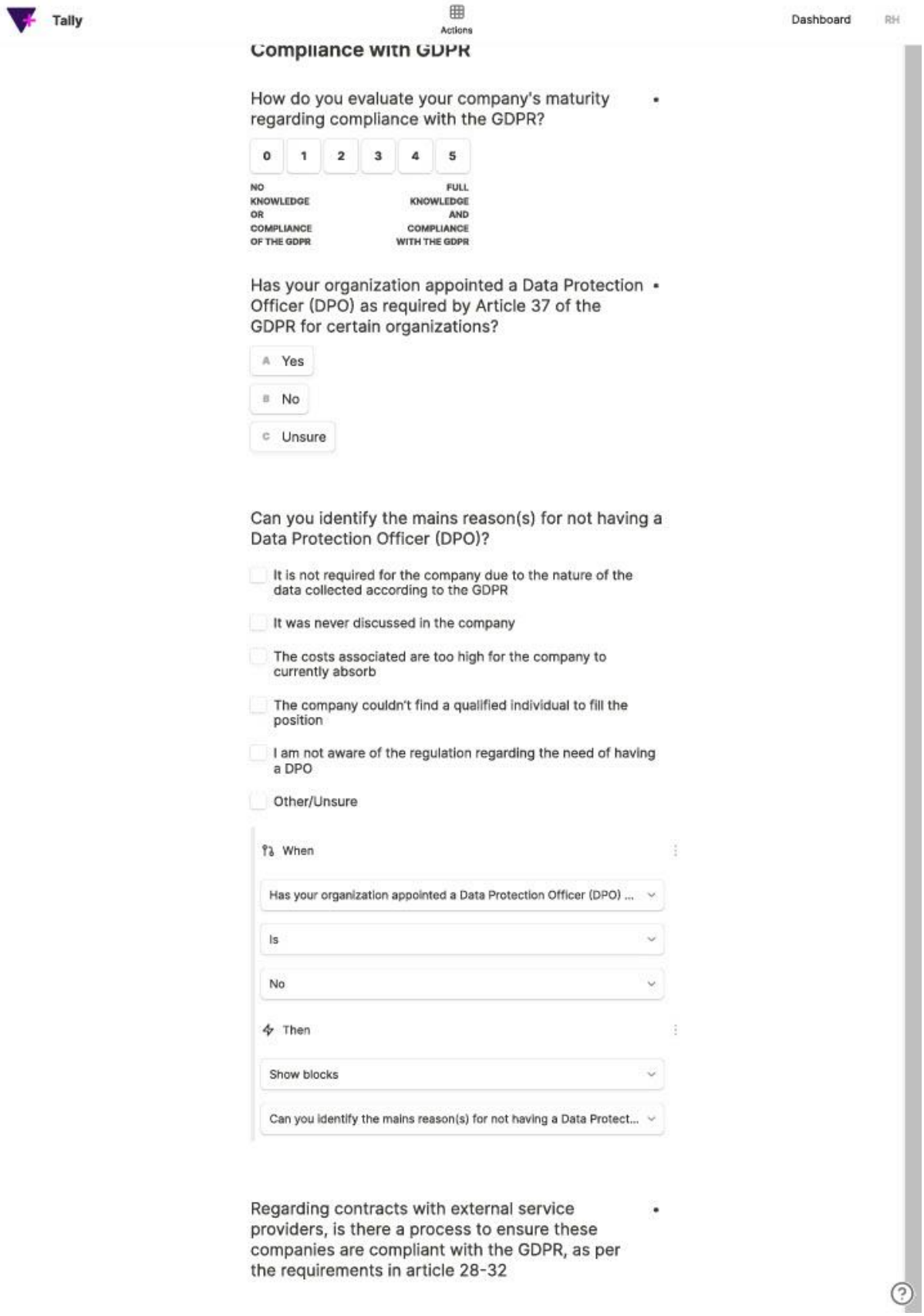
Should a company weigh the difficulty of complying with GDPR when creating new products or services? *

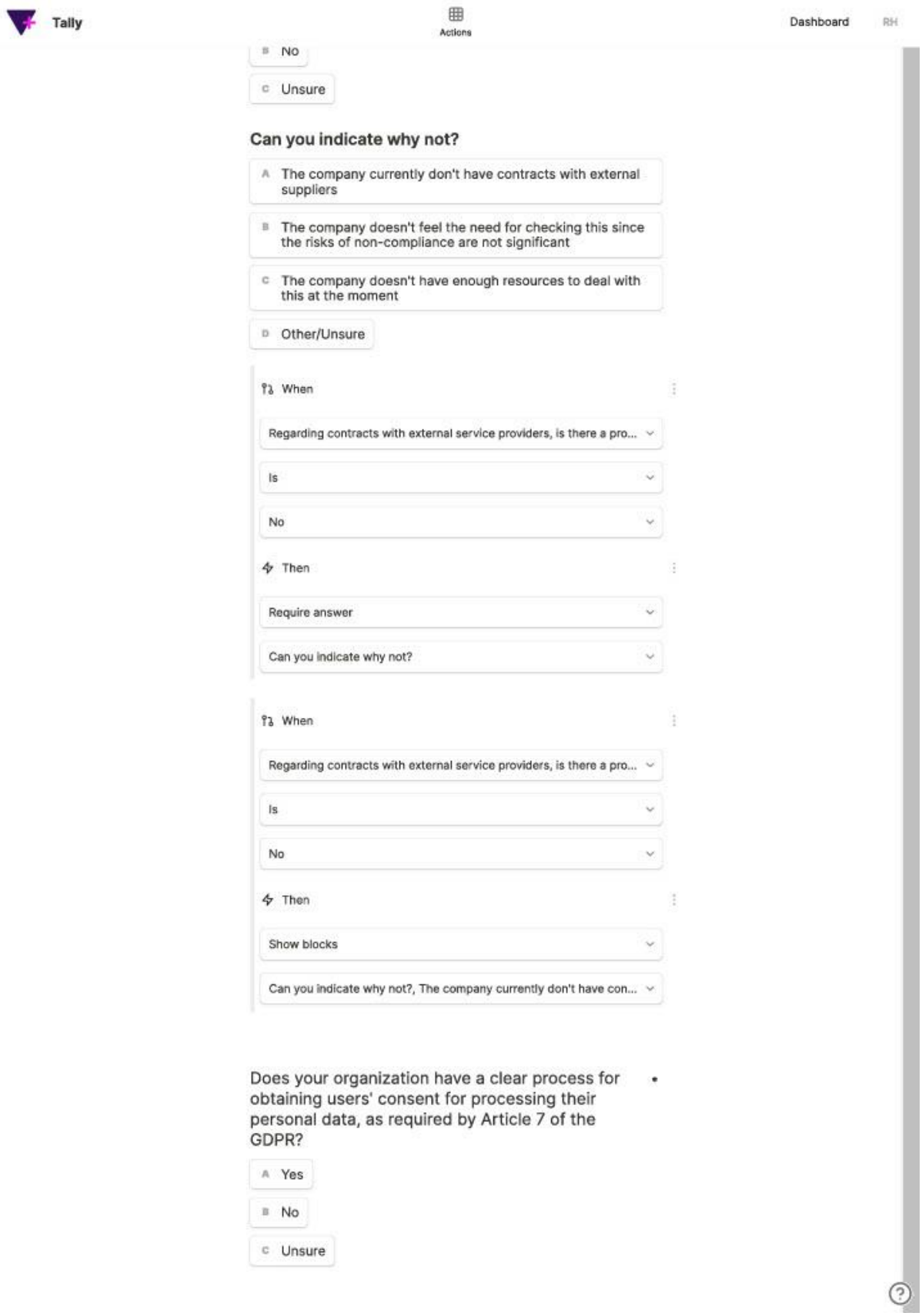
A Yes, always
B Yes, but only in cases where the product or service that are reliant on personal data
C No, companies should prioritize innovation and address compliance issues later
D No, GDPR compliance should not influence a new product or service creation
E Unsure

In your opinion, how might GDPR compliance affect a company's growth and expansion? *

A Positively, by fostering trust and ensuring responsible data practices


Tally
Actions
Dashboard
RH
C Neutral, with both positive and negative aspects balancing each other out
D No impact on company growth
E Unsure
How much do you agree with the following statement?
"The GPDR is a burden to startups due to the extra costs it generates"
0 1 2 3 4 5
STRONGLY DISAGREE
STRONGLY AGREE
How much do you agree with the following statement?
"The GPDR makes innovation more difficult due to the data collection and handling restrictions"
0 1 2 3 4 5
STRONGLY DISAGREE
STRONGLY AGREE
How much do you agree with the following statement?
"The GPDR makes it more difficult for Startups to grow its products and thrive"
0 1 2 3 4 5
STRONGLY DISAGREE
STRONGLY AGREE
When
On a scale of 1 to 5, how important do you think it is for a general ...
Is not empty
Then
Jump to page
Default 'Thank you' page
Next
PAGE 4


Tally
Actions
Dashboard
RH
Compliance with GDPR
How do you evaluate your company's maturity regarding compliance with the GDPR?
0
1
2
3
4
5
NO KNOWLEDGE OR COMPLIANCE OF THE GDPR
FULL KNOWLEDGE AND COMPLIANCE WITH THE GDPR
Has your organization appointed a Data Protection Officer (DPO) as required by Article 37 of the GDPR for certain organizations?
A Yes
B No
C Unsure
Can you identify the mains reason(s) for not having a Data Protection Officer (DPO)?
It is not required for the company due to the nature of the data collected according to the GDPR
It was never discussed in the company
The costs associated are too high for the company to currently absorb
The company couldn't find a qualified individual to fill the position
I am not aware of the regulation regarding the need of having a DPO
Other/Unsure
When
Has your organization appointed a Data Protection Officer (DPO) ...
Is
No
Then
Show blocks
Can you identify the mains reason(s) for not having a Data Protect...
Regarding contracts with external service providers, is there a process to ensure these companies are compliant with the GDPR, as per the requirements in article 28-32


Tally
Actions
Dashboard
RH
B No
C Unsure
Can you indicate why not?
A The company currently don't have contracts with external suppliers
B The company doesn't feel the need for checking this since the risks of non-compliance are not significant
C The company doesn't have enough resources to deal with this at the moment
D Other/Unsure
When
Regarding contracts with external service providers, is there a pro...
Is
No
Then
Require answer
Can you indicate why not?
When
Regarding contracts with external service providers, is there a pro...
Is
No
Then
Show blocks
Can you indicate why not?, The company currently don't have con...
Does your organization have a clear process for obtaining users' consent for processing their personal data, as required by Article 7 of the GDPR?
A Yes
B No
C Unsure

of the GDPR, such as **the right to access, rectification, and erasure**?

A Yes

B No

C Unsure

Next

PAGE 5

Section C: Cost-related impacts

Has your organization experienced increased costs due to GDPR compliance efforts? (e.g., legal, technical, administrative, staff training costs)

A Yes

B No

C Unsure

When

Has your organization experienced increased costs due to GDPR ...

Is

No

Then

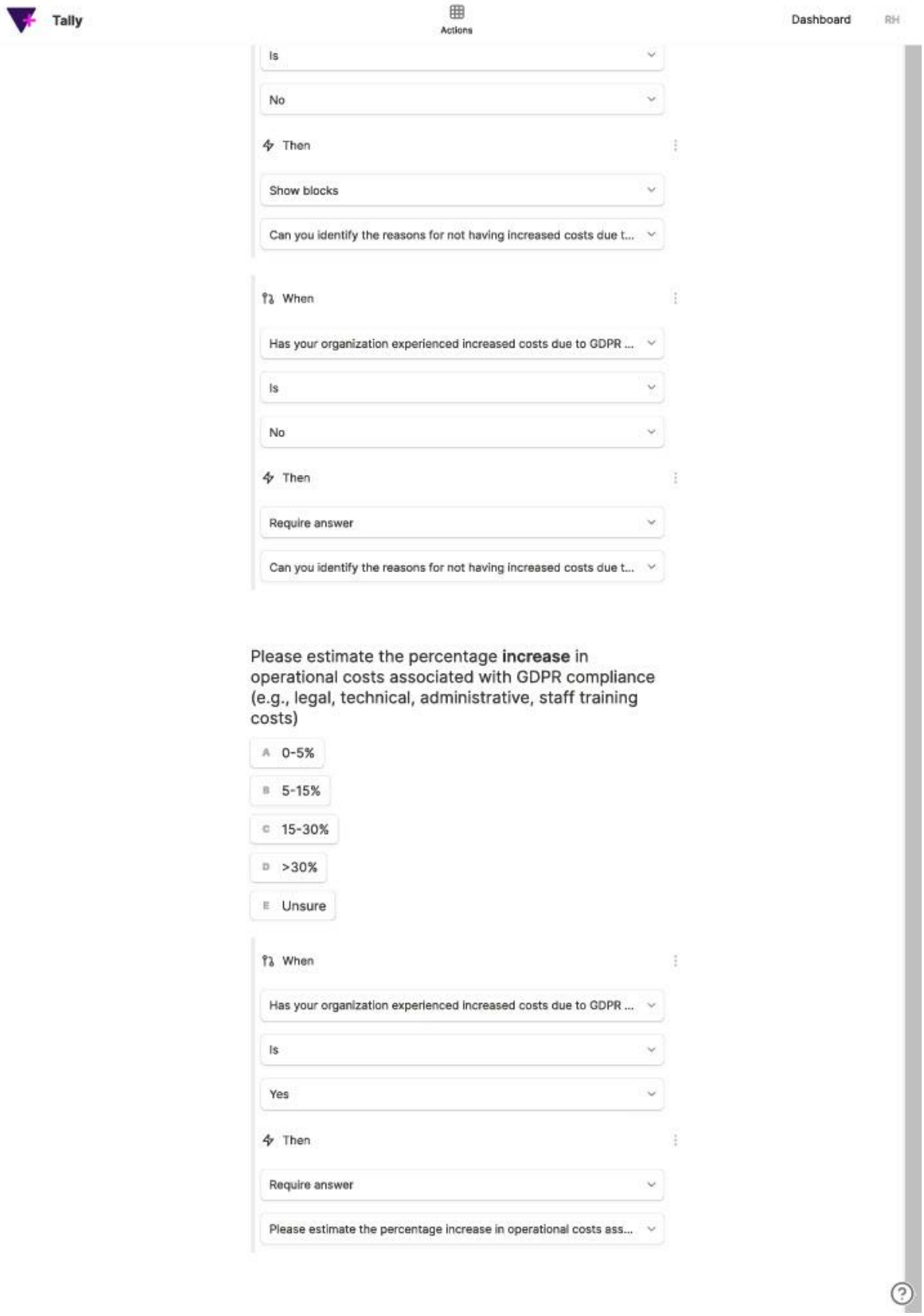
Hide blocks

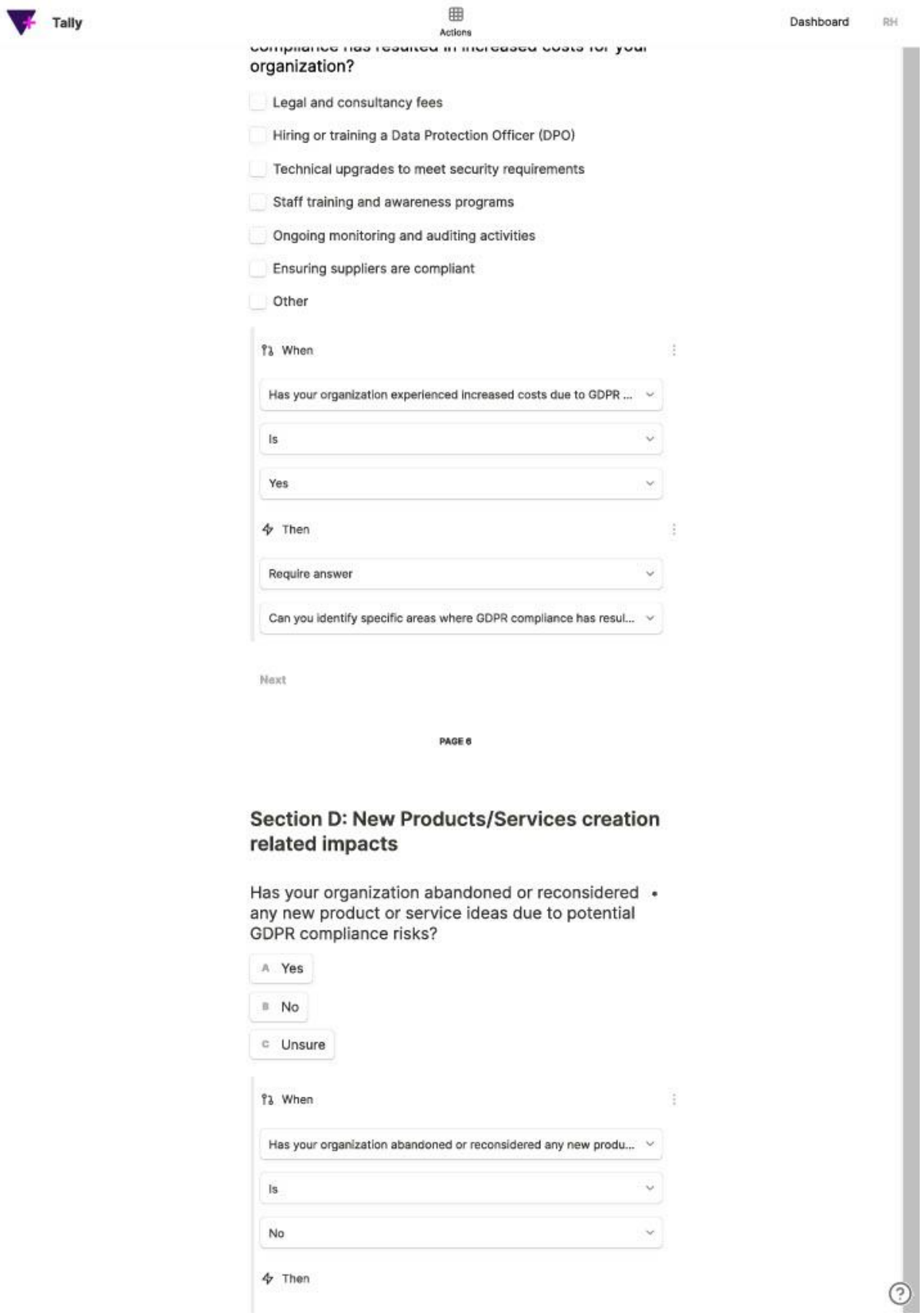
Can you identify specific areas where GDPR compliance has resul...

Can you identify the reasons for not having increased costs due to the GDPR?

- [ ] The company is not affected by the GDPR as far as I'm aware
- [ ] The company already had a solid data privacy structure despite the GDPR requirements
- [ ] The company hasn't taken any special action(s) to ensure it's compliant with the regulation due to a business decision
- [ ] Other

When


Tally
Actions
Dashboard
RH
Is
No
Then
Show blocks
Can you identify the reasons for not having increased costs due t...
When
Has your organization experienced increased costs due to GDPR ...
Is
No
Then
Require answer
Can you identify the reasons for not having increased costs due t...
Please estimate the percentage increase in operational costs associated with GDPR compliance (e.g., legal, technical, administrative, staff training costs)
A 0-5%
B 5-15%
C 15-30%
D >30%
E Unsure
When
Has your organization experienced increased costs due to GDPR ...
Is
Yes
Then
Require answer
Please estimate the percentage increase in operational costs ass...


Tally
Actions
Dashboard
RH
organization?
Legal and consultancy fees
Hiring or training a Data Protection Officer (DPO)
Technical upgrades to meet security requirements
Staff training and awareness programs
Ongoing monitoring and auditing activities
Ensuring suppliers are compliant
Other
When
Has your organization experienced increased costs due to GDPR ...
Is
Yes
Then
Require answer
Can you identify specific areas where GDPR compliance has resul...
Next
PAGE 6
Section D: New Products/Services creation related impacts
Has your organization abandoned or reconsidered any new product or service ideas due to potential GDPR compliance risks?
A Yes
B No
C Unsure
When
Has your organization abandoned or reconsidered any new produ...
Is
No
Then


Tally
Actions
Dashboard
RH
How often has GDPR compliance been discussed or influenced th...
Please indicate the alternative that better explains the previous answer
A The GDPR was never brought up when discussing a new service or product because it doesn't apply to my company's field of operation (for instance, the company doesn't handle any personal data)
B The GDPR was never brought up when discussing a new service or product, most likely because there's not enough knowledge about the regulation inside the company
C The GDPR was discussed but was never considered a relevant issue or risk for any product/service idea
D The GDPR was discussed as being a risk to the development of an idea, but the company chose to not discard it because of the regulation.
E Unsure
When
Has your organization abandoned or reconsidered any new produ...
Is
No
Then
Show blocks
Please indicate the alternative that better explains the previous a...
When
Has your organization abandoned or reconsidered any new produ...
Is
No
Then
Require answer
Please indicate the alternative that better explains the previous a...
Which GDPR requirements were the primary reasons for reconsidering the product ideas? (Please select all that apply)
Data minimization (Article 5(1)(c))

Consent requirements (Article 7)

- [ ] Data subject rights (Articles 15-22)
- [ ] Security of processing (Article 32)
- [ ] Data breach notification (Article 33)
- [ ] Other/Unsure

When

Has your organization abandoned or reconsidered any new produ...

Is

Yes

Then

Require answer

Which GDPR requirements were the primary reasons for reconsid...

How often has GDPR compliance been discussed or influenced the decision to abandon or reconsider new product ideas?

A Frequently

B Occasionally

C Rarely

D Never

When

Has your organization abandoned or reconsidered any new produ...

Is

Yes

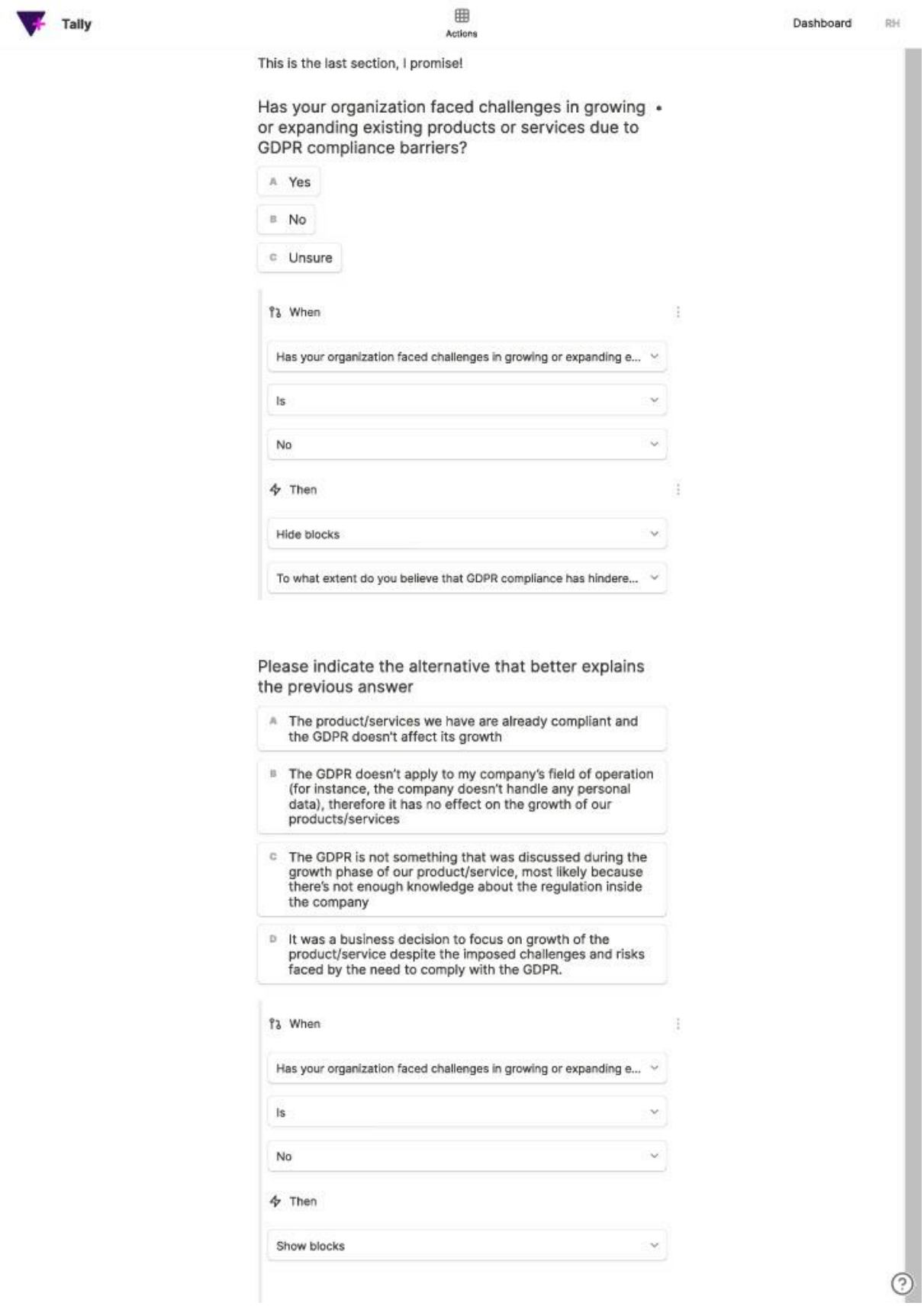
Then

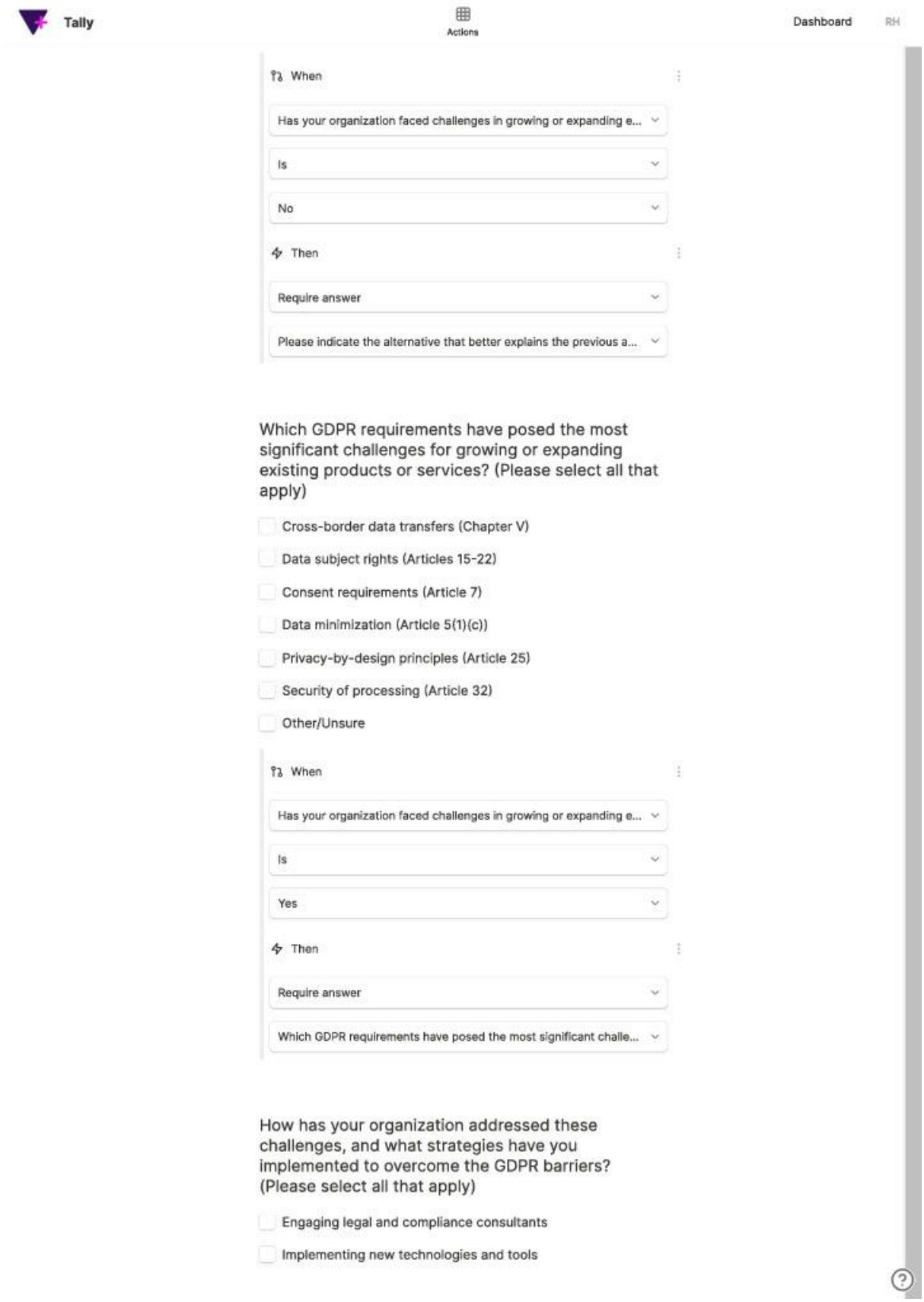
Require answer

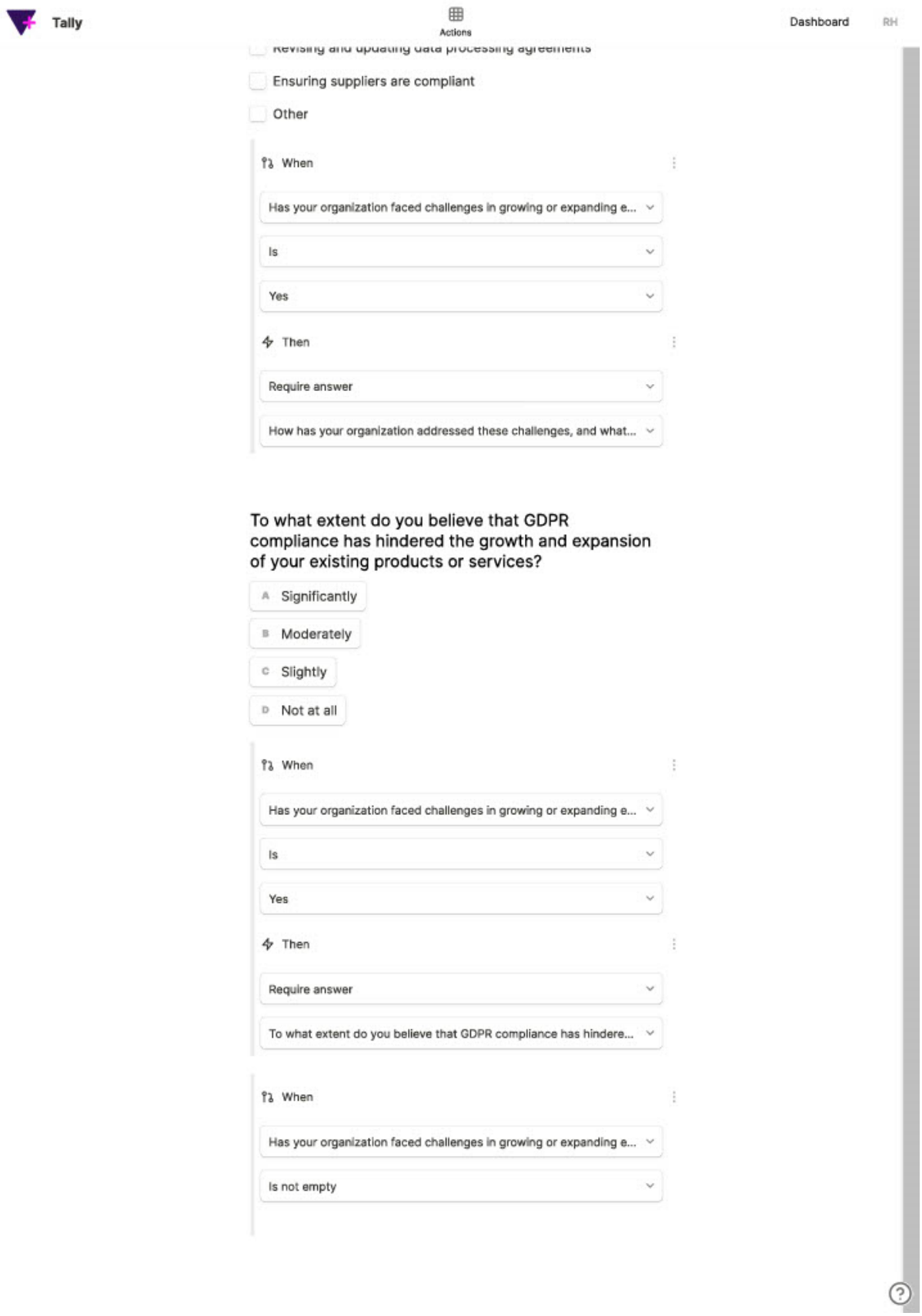
How often has GDPR compliance been discussed or influenced th...

Next

PAGE 7


Tally
Actions
Dashboard
RH
This is the last section, I promise!
Has your organization faced challenges in growing or expanding existing products or services due to GDPR compliance barriers?
A Yes
B No
C Unsure
When
Has your organization faced challenges in growing or expanding e...
Is
No
Then
Hide blocks
To what extent do you believe that GDPR compliance has hindere...
Please indicate the alternative that better explains the previous answer
A The product/services we have are already compliant and the GDPR doesn't affect its growth
B The GDPR doesn't apply to my company's field of operation (for instance, the company doesn't handle any personal data), therefore it has no effect on the growth of our products/services
C The GDPR is not something that was discussed during the growth phase of our product/service, most likely because there's not enough knowledge about the regulation inside the company
D It was a business decision to focus on growth of the product/service despite the imposed challenges and risks faced by the need to comply with the GDPR.
When
Has your organization faced challenges in growing or expanding e...
Is
No
Then
Show blocks


Tally
Actions
Dashboard
RH
When
Has your organization faced challenges in growing or expanding e...
Is
No
Then
Require answer
Please indicate the alternative that better explains the previous a...
Which GDPR requirements have posed the most significant challenges for growing or expanding existing products or services? (Please select all that apply)
Cross-border data transfers (Chapter V)
Data subject rights (Articles 15-22)
Consent requirements (Article 7)
Data minimization (Article 5(1)(c))
Privacy-by-design principles (Article 25)
Security of processing (Article 32)
Other/Unsure
When
Has your organization faced challenges in growing or expanding e...
Is
Yes
Then
Require answer
Which GDPR requirements have posed the most significant challe...
How has your organization addressed these challenges, and what strategies have you implemented to overcome the GDPR barriers? (Please select all that apply)
Engaging legal and compliance consultants
Implementing new technologies and tools


Tally
Actions
Dashboard
RH
Revising and updating data processing agreements
Ensuring suppliers are compliant
Other
When
Has your organization faced challenges in growing or expanding e...
Is
Yes
Then
Require answer
How has your organization addressed these challenges, and what...
To what extent do you believe that GDPR compliance has hindered the growth and expansion of your existing products or services?
A Significantly
B Moderately
C Slightly
D Not at all
When
Has your organization faced challenges in growing or expanding e...
Is
Yes
Then
Require answer
To what extent do you believe that GDPR compliance has hindere...
When
Has your organization faced challenges in growing or expanding e...
Is not empty

Appendix 2 – Questionnaire Responses

What is your company's main area of operation?	What is the size of the company you work for?	Which option best describes your position in the company?	How familiar are you regarding the General Data	How familiar are you with how the GDPR affects your company's
Engineering	06-20	Founder/C-level	0	0
Information Technology Services	06-20	Founder/C-level	5	5
Education	01-05	Founder/C-level	3	3
Software	21-50	Founder/C-level	5	5
Healthcare	01-05	Founder/C-level	4	4
Security & Defense	100+	Founder/C-level	5	4
Information Technology Services	06-20	Founder/C-level	4	5
Information Technology Services	06-20	Founder/C-level	5	5
Financial Services	06-20	Upper Management	0	0
Other	01-05	Founder/C-level	5	5
Research & Development	01-05	Upper Management	5	5
Retail	100+	Upper Management	5	5
Information Technology Services	21-50	Upper Management	1	1
E-commerce	06-20	Founder/C-level	4	4
Research & Development	100+	Upper Management	3	4
Education	06-20	Founder/C-level	5	3

On a scale of 1 to 5, how important do you think it is for a general employee to be aware of the GDPR regulations and its impacts on the company?	Who should be responsible for transmitting the knowledge to company's contributor?	Regarding Company Costs, how do you feel the need to comply with data privacy regulations might affect your company?
5	The EU, as the Regulator	Has no impact on a company costs
5	The company	Slightly increase costs, but with no real impact on the company's financials
5	The company	Slightly increase costs, but with no real impact on the company's financials
5	The company	Slightly increase costs, but with no real impact on the company's financials
5	Both the company and the regulatores	Slightly increase costs, but with no real impact on the company's financials
3	Both the company and the regulatores	Slightly increase costs, but with no real impact on the company's financials
4	Both the company and the regulatores	Increase costs in a significant way due to compliance efforts
5	The company	Has no impact on a company costs
2	Both the company and the regulatores	Has no impact on a company costs
5	Both the company and the regulatores	Slightly increase costs, but with no real impact on the company's financials
5	Both the company and the regulatores	Slightly increase costs, but with no real impact on the company's financials
5	Both the company and the regulatores	Slightly increase costs, but with no real impact on the company's financials
3	Both the company and the regulatores	Increase costs in a significant way due to compliance efforts
3	The company	Has no impact on a company costs
5	Both the company and the regulatores	Slightly increase costs, but with no real impact on the company's financials
2	Both the company and the regulatores	Slightly increase costs, but with no real impact on the company's financials

Should a company weigh the difficulty of complying with GDPR when creating new products or services?	In your opinion, how might GDPR compliance affect a company's growth and expansion?
but only in cases where the product or service that are reliant on personal data	Positively, by fostering trust and ensuring responsible data practices
always	Positively, by fostering trust and ensuring responsible data practices
always	Neutral, with both positive and negative aspects balancing each other out
but only in cases where the product or service that are reliant on personal data	Unsure
GDPR compliance should not influence a new product or service creation	Positively, by fostering trust and ensuring responsible data practices
always	Positively, by fostering trust and ensuring responsible data practices
always	Neutral, with both positive and negative aspects balancing each other out
but only in cases where the product or service that are reliant on personal data	No impact on company growth
companies should prioritize innovation and address compliance issues later	Negatively, by creating barriers and increasing costs
GDPR compliance should not influence a new product or service creation	No impact on company growth
but only in cases where the product or service that are reliant on personal data	Negatively, by creating barriers and increasing costs
always	Neutral, with both positive and negative aspects balancing each other out
companies should prioritize innovation and address compliance issues later	No impact on company growth
companies should prioritize innovation and address compliance issues later	No impact on company growth
always	Neutral, with both positive and negative aspects balancing each other out
always	Positively, by fostering trust and ensuring responsible data practices

How much do you agree with the following statement? "The GPDR is a burden to startups due to the extra costs it generates"	How much do you agree with the following statement?"The GPDR makes innovation more difficult due to the data collection and handling restrictions"	How much do you agree with the following statement?"The GPDR makes it more difficult for Startups to grow its products and thrive"	How do you evaluate your company's maturity regarding compliance with the GDPR?
0	0	0	
2	3	1	4
5	5	5	0
1	2	0	4
0	1	1	3
1	1	4	3
3	4	3	4
4	5	4	3
2	1	1	
4	2	3	3
5	2	2	0
1	3	2	5
4	3	2	
0	3	1	2
3	3	3	5
3	4	4	3

Has your organization appointed a Data Protection Officer (DPO) as required by Article 37 of the GDPR for certain organizations?	Can you identify the mains reason(s) for not having a Data Protection Officer (DPO)?	Can you identify the mains reason(s) for not having a Data Protection Officer (DPO)? (It is not required for the company due to the nature of the data collected according to the GDPR)	Can you identify the mains reason(s) for not having a Data Protection Officer (DPO)? (It was never discussed in the company)	Can you identify the mains reason(s) for not having a Data Protection Officer (DPO)? (The costs associated are too high for the company to currently absorb)	Can you identify the mains reason(s) for not having a Data Protection Officer (DPO)? (The company couldn't find a qualified individual to fill the position)
No	It is not required for the company	TRUE	FALSE	FALSE	FALSE
No	The costs associated are too high	FALSE	TRUE	TRUE	FALSE
Yes					
Yes					
Yes					
Yes					
No	It is not required for the company	TRUE	FALSE	FALSE	FALSE
No	Other/Unsure	FALSE	FALSE	FALSE	FALSE
No	It is not required for the company	TRUE	FALSE	FALSE	FALSE
Yes					
No	I am not aware of the regulation	FALSE	FALSE	FALSE	FALSE
Yes					
Yes					

Can you identify the mains reason(s) for not having a Data Protection Officer (DPO)? (I am not aware of the regulation regarding the need of having a DPO)	Can you identify the mains reason(s) for not having a Data Protection Officer (DPO)? (Other/Unsure)	Regarding contracts with external service providers, is there a process to ensure these companies are compliant with the GDPR, as per the requirements in article 28-32	Can you indicate why not?	Does your organization have a clear process for obtaining users' consent for processing their personal data, as required by Article 7 of the GDPR?	In general terms, is your organization able to fulfill the data subjects' rights outlined in Articles 15-22 of the GDPR, such as the right to access, rectification, and erasure?
FALSE	FALSE	Yes		No	Yes
FALSE	FALSE	Unsure		No	Yes
		Yes		Yes	Yes
		No	The company doesn't ha	Yes	Yes
		No	The company doesn't ha	Yes	Yes
		Yes		Yes	Yes
FALSE	FALSE	No	The company doesn't fe	Yes	Yes
FALSE	TRUE	Yes		Yes	Yes
FALSE	FALSE	Yes		Yes	Yes
		Yes		Yes	Yes
TRUE	FALSE	Yes		Yes	Yes
		Yes		Yes	Yes
		Yes		Yes	Yes

Has your organization experienced increased costs due to GDPR compliance efforts? (e.g., legal, technical, administrative, staff training costs)	Can you identify the reasons for not having increased costs due to the GDPR?	Can you identify the reasons for not having increased costs due to the GDPR? (The company is not affected by the GDPR as far as I'm aware)	Can you identify the reasons for not having increased costs due to the GDPR? (The company already had a solid data privacy structure despite the GDPR requirements)	Can you identify the reasons for not having increased costs due to the GDPR? (The company hasn't taken any special action(s) to ensure it's compliant with the regulation due to a business decision)	Can you identify the reasons for not having increased costs due to the GDPR? (Other)	Please estimate the percentage increase in operational costs associated with GDPR compliance (e.g., legal, technical, administrative, staff training costs)
No	Other	FALSE	FALSE	FALSE	TRUE	
No	The company hasn't taken a	FALSE	FALSE	TRUE	FALSE	
No	The company already had a	FALSE	TRUE	FALSE	FALSE	
Unsure						Unsure
No	The company hasn't taken a	FALSE	FALSE	TRUE	FALSE	
Yes						0-5%
No	The company hasn't taken a	FALSE	FALSE	TRUE	FALSE	
No	The company already had a	FALSE	TRUE	FALSE	FALSE	
Yes						0-5%
Yes						0-5%
Yes						0-5%
Yes						0-5%
Yes						Unsure

you identify specific areas where GDPR compliance has resulted in increased costs for your organization?
al and consultancy fees
Legal and consultancy fees, Hiring or training a Data Protection Officer (DPO), Technical upgrades to meet security requirements, Staff training and awareness programs, Ongoing monitoring and auditing activities, Ensuring suppliers are compliant
oing monitoring and auditing activities, Staff training and awareness programs, Other
Staff training and awareness programs, Technical upgrades to meet security requirements, Hiring or training a Data Protection Officer (DPO), Legal and consultancy fees, Ongoing monitoring and auditing activities, Ensuring suppliers are compliant
al and consultancy fees
Legal and consultancy fees, Hiring or training a Data Protection Officer (DPO), Technical upgrades to meet security requirements, Staff training and awareness programs, Ongoing monitoring and auditing activities
Legal and consultancy fees, Hiring or training a Data Protection Officer (DPO), Technical upgrades to meet security requirements, Ongoing monitoring and auditing activities, Staff training and awareness programs, Other

Has your organization abandoned or reconsidered any new product or service ideas due to potential GDPR compliance risks?	Please indicate the alternative that better explains the previous answer (1)
No	The GDPR was discussed but was never considered a relevant issue or risk for any product/service idea
No	The GDPR was discussed but was never considered a relevant issue or risk for any product/service idea
No	The GDPR was discussed as being a risk to the development of an idea, but the company chose to not discard it because of the regulation.
No	The GDPR was discussed as being a risk to the development of an idea, but the company chose to not discard it because of the regulation.
No	The GDPR was discussed as being a risk to the development of an idea, but the company chose to not discard it because of the regulation.
No	The GDPR was discussed but was never considered a relevant issue or risk for any product/service idea
No	The GDPR was never brought up when discussing a new service or product because it doesn't apply to my company's field of operation (for instance, the company doesn't handle any personal data)
No	The GDPR was discussed as being a risk to the development of an idea, but the company chose to not discard it because of the regulation.
No	The GDPR was never brought up when discussing a new service or product because it doesn't apply to my company's field of operation (for instance, the company doesn't handle any personal data)
Unsure	
No	The GDPR was discussed but was never considered a relevant issue or risk for any product/service idea
No	The GDPR was discussed as being a risk to the development of an idea, but the company chose to not discard it because of the regulation.
Yes	

How often has GDPR compliance been discussed or influenced the decision to abandon or reconsider new product ideas?	Has your organization faced challenges in growing or expanding existing products or services due to GDPR compliance barriers?	Please indicate the alternative that better explains the previous answer (2)	Which GDPR requirements have posed the most significant challenges for growing or expanding existing products or services? (Please select all that apply)
	No	The product/services we have are already compliant and the GDPR doesn't affect its growth	
	No	It was a business decision to focus on growth of the product/service despite the imposed challenges and risks faced by the need to comply with the GDPR.	
	No	It was a business decision to focus on growth of the product/service despite the imposed challenges and risks faced by the need to comply with the GDPR.	
	No	It was a business decision to focus on growth of the product/service despite the imposed challenges and risks faced by the need to comply with the GDPR.	
	No	The product/services we have are already compliant and the GDPR doesn't affect its growth	
	No	The product/services we have are already compliant and the GDPR doesn't affect its growth	
	No	The GDPR doesn't apply to my company's field of operation (for instance, the company doesn't handle any personal data), therefore it has no effect on the growth of our products/services	
	No	The product/services we have are already compliant and the GDPR doesn't affect its growth	
	No	The GDPR doesn't apply to my company's field of operation (for instance, the company doesn't handle any personal data), therefore it has no effect on the growth of our products/services	
Frequently	Yes		Cross-border data transfers (Chapter V), Consent requirements (Article 7), Security of processing (Article 32)
	No	It was a business decision to focus on growth of the product/service despite the imposed challenges and risks faced by the need to comply with the GDPR.	
	No	The product/services we have are already compliant and the GDPR doesn't affect its growth	
Frequently	Yes		Security of processing (Article 32), Cross-border data transfers (Chapter V), Privacy-by-design principles (Article 25)

How has your organization addressed these challenges, and what strategies have you implemented to overcome the GDPR barriers? (Please select all that apply)	To what extent do you believe that GDPR compliance has hindered the growth and expansion of your existing products or services?
Revising and updating data processing agreements, Ensuring suppliers are compliant, Engaging legal and compliance consultants, Implementing new technologies and tools	Slightly
Engaging legal and compliance consultants, Implementing new technologies and tools, Providing additional staff training and awareness programs, Revising and updating data processing agreements, Ensuring suppliers are compliant	Moderately