Thesis Dissertation

USER-FRIENDLY GENERATOR FOR PRIVACY POLICIES

Elia Nicolaou

UNIVERSITY OF CYPRUS

COMPUTER SCIENCE DEPARTMENT

May 2022

UNIVERSITY OF CYPRUS
COMPUTER SCIENCE DEPARTMENT

User-Friendly Generator for Privacy Policies

Elia Nicolaou

Supervisor
Dr. Anna Philippou

Thesis submitted in partial fulfilment of the requirements for the award of degree of Bachelor in Computer Science at University of Cyprus

May 2022

Acknowledgments

The moment I am writing this, I am one step closer to completing my thesis and completing a long road to acquire my degree in Computer Science at the University of Cyprus. Four years have gone, with many hardships, many enjoyable moments, and the acquisition of information that will lead me to my next path.

First and foremost, I'd want to express my gratitude to Anna Philipou, my dissertation supervisor, who remained by my side throughout the process, offering me with any direction and help I need. Moreover, I'd also like to convey my gratefulness to all of the professors who provided me with invaluable knowledge throughout those years.

Furthermore, I would like to thank my Scouting family, my leaders, my friends and especially my little cubs, who provided me with happiness, love and support.

In addition, I want to express my gratitude to my family, who have always stood by me, especially my parents and siblings, who have given me everything and helped me become the person I am today.

Finally, I must express my gratitude to my friends, my second family, who have always been supportive throughout the journey of my undergraduate degree.

Abstract

Unfortunately, nowadays, the use of websites is not always done in a way that protects individuals' privacy, as many companies record and archive users' searches, the pages they visit, the time they spend on each page, the site from which they link, and any other information that serves to create a detailed "preferences profile" for each user.

The tendency of online users to place their trust in the websites they visit without knowing how their data is processed poses a significant privacy concern. Driven by their desire to utilize different websites, people disclose sensitive information such as their financial situation, address, and e-mail, believing that the motives of websites are always positive. However, there is a great possibility that a page may deceive them and misuse this information.

Governments and nations have adopted numerous privacy restrictions in recent years, such as the GDPR. Enforcing privacy policies is one method specified in the regulations. The paradox is that, although being employed to enlighten the public, policies are not taken into account by anybody. Influenced by our tendency to disregard the privacy policies provided by each website, which can protect us from unknowingly giving our data when we visit various web pages, utilizing the fundamentals we acquired at university, we decided to use the thesis to help people understand the importance of their privacy by encouraging them to read privacy policies.

To accomplish this, we conducted extensive research on the ideas of user experience, privacy policies and privacy concerns. Then, we developed a user-friendly template of privacy policies and taking this template into consideration, we created a website that generates privacy policies for businesses, organizations and individuals that deliver content in a user-friendly and accessible manner to individuals.

To enhance the thesis more, we constructed a text-analysis for privacy policies. We built a new data-set based on the numerous findings and we used this data-set to do some logistic regression to build a model that will assess how comprehensible a policy is.

Contents

List of Figures

Chapter 1

Introduction

1.1 Today's world with Big Brother watching us

George Orwell, the English novelist, in 1949 published his novel Nineteen Eighty-Four, portraying Big Brother, a fictional character and symbol who is ostensibly the leader of Oceania, a totalitarian state, where the ruling party wields total power. Although Big Brother does not appear directly in the story, his presence permeates the gloomy society of Oceania where there are ubiquitous posters with the slogan "Big Brother is watching you" and hidden cameras in every room, creating fear for every citizen. Orwell created a fictional character who represents the emotions and situation of the then generation, with people under the power of politicians, the powerful, without having the opportunity to express their right to freedom and privacy.

Our generation is currently faced with similar issues, with problems of sensitive information leaks, fake news, and the violation of free expression and privacy rights. We have reached a point where Orwell's Oceania is no longer fictional but is paraphrased within the real world, where Big Brother has found a tangible expression in technology.

1.2 Motivation

People must first grasp the value of their privacy in order to avoid some of the problems that develop in today's technological culture. Data leakage on the internet, data interception, and data processing for personal advantage are all issues.

Based on the restrictions given in our cyberspace, many of the websites we use today warn us about how our data is handled and processed. There are several of those regulations enforced in today's world. Some of those regulations are CalOPPA [26], CCPA [3] and GDPR [38]. The most widely known regulation is General Data Protection Regulation, which says that a privacy policy is expected to include subjects such as what data

is gathered from the user, how the user's data is used, what rights the user has, and what third-party organizations utilize the data. The purpose of privacy rules is to inform users how their data is being used and protect them while using various websites and sharing data but at the same time helping the websites from lawsuits made by users.

However, we have a tendency to disregard this warning information. The explanation to the question why, however, can be separated into two categories: one is because users do not perceive the significance of protecting their privacy, and the other is that websites do not attempt to convey these regulations in an accessible manner.

In the thesis, we are attempting to address the second issue noted above: most websites' inability to provide information about a privacy policy in a user-friendly manner in order to assist users comprehend and spend some time reading the policy. We are attempting to make the policy more appealing to users while still ensuring that it complies with GDPR regulations, that the user knows how his or her data is being used, how the data is being processed and how the organisation/service stores the data.

In nutshell, we created a website called UIpolicy, that implements a user-friendly generator for developing user-friendly policies. There are several generators available on the market that can generate privacy policies. However, our contribution is to develop not only a GDPR-compliant privacy policy, but also one that is user-friendly and can be easily be comprehend by the average user. Furthermore, we did some research through questionnaires about privacy policies that can be used for future works.

1.3 Methodology

Ensuring that a privacy policy is understandable and user pleasant is a challenging task since most individuals have negative experiences with privacy policies, and most people just click "accept" without reading them. In order to persuade the user to read a privacy policy, the first step must be to understand why people do not want to read it. We discovered through a questionnaire presented in Section 3.2 that the quantity of words and layout of the policy is the number one reason. Policies must be broken down into manageable portions in order to be understandable, and the language must be delivered in a straightforward tone and viewpoint rather than using legal jargon.

A significant amount of research was required for the project's implementation. It was critical to examine the definition of privacy, policies, and legislation. Furthermore, because we aimed to design a user-friendly policy generator, it was critical to first understand the user and the user experience when reading policies. We prepared a questionnaire to evaluate how people react to current policies and what their experience with them.

Then, we leveraged our knowledge of usability and user-experience to build a template for how a policy may be written in a more user-friendly way. To determine if the template

actually works, we built another questionnaire that compared a standard privacy policy to our own template.

After receiving the responses, we began developing a website that we called UIpolicy, a generator that creates a privacy policy based on the template we created. The generator collects an organization's or an individual's info on how they handle data and then breaks the subjects down into smaller components, adding symbols and presenting them to the user in an easy-to-understand format. We utilized the Vuetify framework from Vue [40], CSS [4], and HTML [17] to create the generator. For the backend we used Node.js [24],and we hosted the authentication and database on Google's Firebase [14].

Furthermore, we conducted an analysis on various privacy policies. Based on this study, we produced a new data-set that we utilized it to build a logistic regression model to determine whether or not a privacy policy is comprehend by the average user. We used Python [32] for the analysis of the policies.

For the evaluation, we built another questionnaire to assess the users' experience with the generator and how user-friendly the output is. Overall, we attempted to include into the project all of the essential information we gathered from our background study and university classes.

In the current situation, the generator constructs the policy based on the template. However, it can be developed to allow the user to alter sections of the policy, such as changing colors and icons. Furthermore, its might be check through a GDPR compliant language, and it may be built to fulfill policy standards other than the GDPR.

1.4 Outline of thesis

The next chapter will go through the principles that served as the framework for the creation of this project. These notions are privacy, privacy policy, legislation, and the evolution of privacy rules in recent years. In addition, we will look at some related works that helped us develop this thesis.

The actions required to construct a user-friendly privacy policy template will be examined and reviewed in Chapter 3. In addition, the findings of the questionnaire used for the development of the template, will be discussed. The purpose of the questionnaire was to evaluate the privacy policy template.

The implementation, frontend, backend, and background research of the website will be discussed in Chapter 4. In this chapter, we examine the functional needs of the final system as well as the non-functional requirements of the web application and restrictions that must be considered, such as security and information privacy. Moreover, we will provide examples of some interfaces.

In Chapter 5, we will walk through the processes for text analysis of various privacy

regulations, as well as the outcomes and how those results might be applied in future research. In addition, we will give the logistic regression method for determining how comprehensible a policy is.

The website evaluation, the thesis review and suggestions for future work will be provided at the last chapter.

Chapter 2

Background

2.1 Privacy

2.1.1 The definition of privacy

In today's world, privacy is one of the most difficult concepts to analyze as everyone can perceive it from different angles and in different ways. Therefore, asking different people what privacy means can give you a variety of answers.

If we go back in time, we can see that the issue of privacy has always been a source of concern. Privacy was a point of distinction between «οίκος» [Oikos] and «δήμος» [municipality] in ancient Greece. The Greeks used to remark, 'Τα εν οίκω μη εν δήμω', which means "Those in the house are not in the municipality." The home-Oikos deals with personal matters, the private life, whilst the municipality deals with public issues, the public realm of political affairs. In fact, what Greeks intended to highlight with their deterrence is that their personal life should not be discussed in public or made available to the public [31].

Privacy is one of the most critical issues in today's environment. We live in an era where disclosing personal information to different websites has become part of the routine. Our "Oikos" is being attacked from all sides, but the security of our data is critical and necessary. A lot of people tend to believe that privacy is not a concern for them, as they tend to feel safe and they do not feel that they have something to hide from others. However, privacy is not about the things you hide; it is more about who you give the right to access your data and how your data will be used. Privacy is about integrity and safety, ensuring that there will be no information leaks or embarrassing situations.

Therefore, we can understand that privacy might not have one definition but many. However, all the definitions deal with our unique data, our personal lives, and their protection. Privacy is something that should be anyone's concern, as it is a dangerous item for someone to use without our consent. Overall, a common definition of privacy is de-

scribed as the state of being let alone and able to keep certain, especially personal matters to oneself. [22]

2.1.2 A hotly debated issue that is getting bigger

Privacy combined with the advances in technology is a hot topic, particularly in the twenty-first century, which is seen as the era of big data and advanced information technology, as well as the rise of large technological corporations and the processing and storage of huge amounts of data online. However, privacy is directly connected with technological advancements, as some of the most serious issues in the computer industry currently appear to be major data breaches, targeted advertising, fake news, and the illicit use of data for political advantage.

Privacy is undeniably a fundamental human right and a necessary precondition for individual liberty and societal progress, and it is thus safeguarded by all democratic constitutions. As a result, people have the freedom to decide what information about their lives is made public, what information must be made public, and where they provide their consent. However, with the massive new dimensions that technology has achieved in recent years, our personal lives are in jeopardy now more than ever. Without a doubt, our privacy is unquestionably being violated.

Major data breaches and the illicit use of data for personal gain are two of the most serious and most common privacy issues we face today. Many such incidents have occurred in recent years, putting at risk individuals' confidentiality, availability, and integrity.

A data breach is a security occurrence in which malicious insiders or external attackers get unauthorized access to confidential data or sensitive information, as a result costly settlements, business closures, and hefty fines are incurred [6]. However, privacy violation is not only as a result of a data breach but also illicit use of data and other. It is critical to address the issues as quickly as possible, but first, we must be willing to acknowledge and recognize them. Our privacy invasion must start to be a concern for all of us.

Therefore, privacy protection is now critical. It is imperative to prevent sensitive information from coming into the hands of unauthorized companies, hackers, government agencies, and other groups. All of the difficulties that have arisen in the rapidly emerging technology world require protection. Legislation, throughout the world, is one of the most safest ways that offers and guarantee this protection.

2.2 Privacy Legislation

2.2.1 Legislation at European Union

Privacy was one of the burning issues of post-war Europe. The war was characterized by the leak of information, leading to the emergence of importing new regulations concerning human rights, involving respecting the private life. Therefore, The Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights (ECHR) [10], was signed in Rome (Italy) on 4 November 1950 by 12 member states of the Council of Europe and entered into force on 3 September 1953.

In the convention, the following is presented:

- The Obligation to respect Human Rights [Article 1]
- The right to respect private and family life [Article 8]

It can be seen as a start to the future regulations concerning privacy information in Europe and the latest evolved legislation of GDPR.

On 24 October 1995, 45 years later from the adoption of the European Convention on Human Rights, The European Data Protection Directive (Directive 95/46/EC) [8] on the protection of individuals about the processing of personal data and the free movement of such data was adopted. The ideas set out with inside the Data Protection Directive were aimed toward the safety of essential rights and freedoms with inside the processing of private data. The purpose was to ensure that everyone respects the rights and fundamental freedoms of each individual, especially the right to privacy, concerning the automatic processing of personal data. The European Data Protection Directive however, has been replaced by Europe's latest regulation of GDPR.

The protocol [9] has the following articles relating to the privacy of personal data :

1. Member States shall provide that personal data must be:

   (a) processed fairly and lawfully

   (b) collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical, or scientific purposes shall not be considered incompatible provided that the Member States provide appropriate safeguards.

(c) adequate, relevant, and not excessive concerning the purposes for which they are collected and/or further processed.

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

(e) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical, or scientific use

2. Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1

3. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. [Article 8]

2.2.2 GDPR

Rapid technological advancement has necessitated more stringent controls over user personal data management. In a world where millions of people come and go, it is critical for any serious government to enact privacy laws.

The European Union pioneered, and as a consequence of the 1995 directive, produced the world's strictest privacy and security law, known as the General Data Protection Regulation (GDPR) [38].

The General Data Protection Regulation was proposed on January 25, 2012, and it entered into force in 2016 after being approved by the European Parliament; as of May 25, 2018, all companies are required to be compliant. Despite the fact that it was designed and passed by the European Union (EU), it puts duties on enterprises anywhere that target or collect data about people in the EU. The GDPR imposes heavy fines on those that break its privacy and security regulations, with penalties ranging from tens of millions of euros to huge amounts of money.

At a time when more and more people are entrusting their personal data to cloud services and breaches are occurring on a daily basis, the regulation has proven to be a necessary tool. Regulation's primary purpose is to offer individuals control over their personal data while also making the regulatory environment easier for international business by consolidating legislation throughout the European Union.

The regulation is composed of 99 articles and 173 recitals that are all detailed in depth. Understanding GDPR articles may be a hard undertaking at times. This is a brief of GDPR containing the ten key requirements [13].

1. Lawful, fair and transparent processing
2. Limitation of purpose, data and storage
3. Data subject rights
4. Consent
5. Personal data breaches
6. Privacy by Design
7. Data Protection Impact Assessment
8. Data transfers
9. Data Protection Officer
10. Awareness and training

Some important articles of GDPR are:

1. Art. 5 GDPR [Principles relating to processing of personal data] which states that personal data must be managed legitimately, fairly, and transparently in reference to the data subject.

2. Art. 6 GDPR [Lawfulness of processing] specifies the circumstances under which it is permissible to handle personal data.

3. Art.7 GDPR [Conditions for consent] which specifies in what conditions consent must be given from the user.

2.2.3 How GDPR has changed the technology world

The GDPR's implementation generated certain challenges for businesses and organizations since they were now required to make the appropriate modifications to their policies and practices in order to be GDPR compliant. It is obvious that no one piece of legislation has ever had the worldwide influence that the EU Global Data Protection Regulation does[15].

GDPR regulation was a trailblazer that other countries followed. In 2020, the California Consumer Privacy Act (CCPA) went into effect. In the United States, all fifty states have laws governing data storage, disposal, and breach notification.

Regulations throughout the globe have enhanced awareness of privacy problems, and individuals have begun to have higher expectations while using the Internet. Furthermore, data privacy is now recognized and priority for everyone, and rules have become the customer experience's new best friend.

The fact that it is no longer an option but a necessary process to implement the regulations is a significant factor in how much the world has changed. If they are not implemented, a significant amount of penalty may be imposed, fines of up to €20 million, or 4 percent of worldwide turnover for the preceding financial year, whichever is higher. Taking an example, Cyprus issued GDPR fines resulting in approximately €1 million worth of penalties in 2021 [7]. Figure 2.1 provides information about the Highest individual fines (Top 10) [12]

	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746,000,000	Non-compliance with general data processing principles	16 Jul 2021
2	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225,000,000	Insufficient fulfilment of information obligations	02 Sep 2021
3	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90,000,000	Insufficient legal basis for data processing	31 Dec 2021
4	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000	Insufficient legal basis for data processing	31 Dec 2021
5	Google Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000	Insufficient legal basis for data processing	31 Dec 2021
6	Google LLC	Media, Telecoms and Broadcasting	FRANCE	50,000,000	Insufficient legal basis for data processing	21 Jan 2019
7	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35,258,708	Insufficient legal basis for data processing	01 Oct 2020
8	TIM (telecommunications operator)	Media, Telecoms and Broadcasting	ITALY	27,800,000	Insufficient legal basis for data processing	15 Jan 2020
9	Enel Energia S.p.A	Transportation and Energy	ITALY	26,500,000	Insufficient legal basis for data processing	16 Dec 2021
10	British Airways	Transportation and Energy	UNITED KINGDOM	22,046,000	Insufficient technical and organisational measures to ensure information security	16 Oct 2020

Figure 2.1: List of the highest individual fines [12]

2.2.4 GDPR, privacy, and design

The General Data Protection Regulation (GDPR) changed the way companies and governments think about privacy. One of these methods is the decision to incorporate the notion of "Privacy by Design" into law via Article 25. "Privacy by Design" [29] simply implies "data protection through technological design." This is based on the idea that data protection in data processing operations is best adhered to when it is already built into the technology when it is produced.

The notion of Privacy by Design is based on seven foundational concepts: [33]

1. Proactive not Reactive/Preventative not Remedial: Proactive rather than reactive measures characterize the Privacy by Design approach. It foresees and stops privacy-invading situations before they occur. The approach does not wait for privacy hazards to manifest, nor does it provide remedies for addressing privacy violations after they have occurred; instead, it seeks to prevent them from arising.

2. Privacy as the Default Setting: Privacy by Design aims to provide the highest level of privacy possible by guaranteeing that personal data is automatically secured in any activity. Even if a person does nothing, their privacy is still protected. Individuals are not obliged to take any action to safeguard their privacy; it is integrated into the system by default.

3. Privacy Embedded into Design: Privacy by Design is included in the design and architecture of information technology systems and business activities. It is not tacked on afterward as an afterthought. As a result, privacy becomes an integral component of the primary functionality provided.

4. Full Functionality: Privacy by Design eliminates the appearance of false equivalencies, such as privacy vs security, by proving that both could be accomplished.

5. End-to-End Security: Privacy by Design continues safely across the full lifespan of the data involved, having been incorporated into the system prior to the first bit of information being acquired – robust security measures are important to privacy, from start to finish. This guarantees that all data is safely maintained and then securely erased in a timely manner at the end of the procedure

6. Visibility and Transparency: Privacy by Design aims to reassure all stakeholders that, regardless of the business practice or technology involved, it is, in fact, working in accordance with the stated promises and objectives, subject to independent verification.

7. Respect for User Privacy: Privacy by Design demands architects and operators to prioritize the individual's interests by including measures such as strong privacy defaults, adequate notice, and empowering user-friendly alternatives. Adopting a user-centric approach.

Privacy and GDPR requirements, without a doubt, present a significant challenge for designers, as they introduce a level of complexity that cannot be ignored.

2.3 Privacy Policies

2.3.1 The definition of a privacy policy

A privacy policy is a document that describes how a website or organization will collect, keep, safeguard, and handle personal information submitted by its users. Moreover, it outlines how the organization/website will use the information as well as how it will satisfy its legal requirements and how people who have shared their data can seek redress if the organization/website fails to meet those commitments.

2.3.2 Privacy legislation and privacy policies

The establishment of privacy policies has come from the rising need for personal data protection and the implementation of various data security rules such as GDPR throughout the world. Most nations require businesses to have a privacy policy in place if they gather personal information from their users.

The European Union is recognized for having some of the world's strongest privacy rules. The General Data Protection Regulation (GDPR), the cornerstone of privacy law, gives specific information in paragraphs 12, 13, and 14 on privacy policies and the necessity of allowing the exercise of users' data rights.

A number of regulations from the different nations necessitate data privacy policies. If none of the rules apply to an organization, it may still be compelled to establish a privacy policy due to the analytical tools, email tools, or advertising platforms that the organization employs.

2.3.3 How a privacy policy is compliant with GDPR

A privacy policy must have several very particular features in order to be considered GDPR-compliant. The GDPR's guidance in Article 12 defines the obligations for privacy policies. Data processing communications must be presented in a clear and simple language in order to create a concise, transparent, and intelligent document. The policy must

be easily accessible and free. Chapter 13 of the GDPR explains data subjects' rights and what information the policy must contain when personal data is gathered, including:

The reason for which the data is being collected
The type of personal information that is collected

In order to be compliant, a privacy policy must state eight particular rights:

1. The right to be informed
2. The right of access
3. The right of rectification
4. The right to erasure (the right to be forgotten)
5. The right to restriction of processing
6. The right to data portability
7. The right to object
8. The right to not be subject to automated decision-making

2.3.4 Privacy policies problems

A good privacy policy must not only be legally compliant, but also comprehensible and transparent to users. However, it is no secret that many businesses, including well-known social media sites, lack adequate policies.

Most privacy policies contain legalese terminology that are incomprehensible to the average individual who is not a lawyer. However, if a concerted effort is made to avoid using legalese phrases, there is a risk of not being in compliance with the regulations, which raises a new issue. Furthermore, many regulations are hidden in a difficult-to-find places, making it impossible for users to find them. As a result, the privacy policy is not given in a clear manner as it should. Designing a correct and transparent policy must be a major undertaking, keeping in mind all of the present policy concerns in mind.

2.4 User-Experience

2.4.1 Definition of user experience

User experience implies that the interface will help users through various phases of job completion. It reduces the gap between humans and systems, allowing people to interact

with tasks rather than the system. It is based on three principles,

1. Easy to learn
2. Easy to use
3. Easy to understand

2.4.2 Definition of usability

According to ISO/DIS 9241-110:2020 [19], the term usability is the extent to which a system, product, or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.

The ISO/DIS 9241-110 [19] standard specifies ways to identify the data that must be considered when specifying or evaluating usability. The goal is to provide a consistent and agreed-upon framework of important usability factors.

Nielsen's usability definition has most likely had the most influence on usability thinking in general. Unlike the ISO definition, Nielsen divides usability into five factors, known as characteristics, that can be quantified and utilized to describe usability objectives.

1. Learnability,
2. Efficiency,
3. Memorability,
4. Few errors,
5. User satisfaction,

2.4.3 Visual affordance

The term visual affordance means extracting information related to affordance from an image or a video. Similar to other machine vision domains such as object and human activity recognition, it uses computer vision techniques to perceive the affordance characteristics in visual media.

2.5 Machine Learning

2.5.1 Logistics regression

Logistic regression is a technique borrowed by machine learning from the field of statistics. It is described as the method of modeling the probability of a discrete result given

an input variable. The most frequent logistic regression models have a binary outcome, which might be true or false, yes or no, and so forth.

For binary and linear classification problems, logistic regression is a simpler and more efficient method. It is a classification model that is very simple to implement and achieves excellent performance with linearly separable classes. It is a widely used classification algorithm in industry.

Logistic regression is best thought of as a linear regression but for classification problems. To model a binary output variable, logistic regression employs a logistic function. The major distinction between linear regression and logistic regression is that the range of logistic regression is limited to 0 and 1. Furthermore, logistic regression, unlike linear regression, does not require a linear connection between input and output variables.

The logistic function also called a sigmoid function. It is a mathematical function with the property of being able to take any real value and map it to a value between 0 and 1

The logistic function :

$$\frac{1}{1+e^{-x}}$$

where $x \in \mathbb{R}$. And in the logistic function equation, x is the input variable.

2.6 Related work

In this section, we will examine some previous work and research publications on the subject of privacy, privacy policies, and the GDPR regulation. These publications cover research aimed at making privacy policies more comprehensible and user-friendly by identifying problems by analysing them. Moreover, we give information about similar websites with the generator that we created and discussing the differences with our website and the impact of them in this work.

2.6.1 An empirical study on the ignorance of privacy policies

The article Ignoring the privacy policies and terms of service policies of social networking services is an empirical survey of Privacy Policies (PP) and Service Terms of Service (TOS) undertaken in 2016 by researchers Jonathan A. Obar and Anne Oeldorf-Hirch [25]. An experimental survey (N=543) examined the extent to which people disregarded PP and TOS while signing up for a hypothetical social networking service called NameDrop.

According to the findings of the study 74% of 543 persons ignored Privacy Policies. The number one issue for ignoring was that the policy was too long to read. According to qualitative data, participants regard policies as a nuisance, ignoring them in order to achieve the purposes of digital production without being hampered by the methods.

	Factors and item loadings		
Items	Information overload	Nothing to hide	Difficult to understand
Privacy policies are too long	**.819**	.093	.088
There are too many privacy policies to read	**.802**	.149	.086
There are too many Terms of Service agreements to read	**.732**	.093	.086
Terms of Service agreements are too long	**.720**	.048	.073
I don't have time to read privacy policies for every site that I visit	**.630**	.203	.178

Figure 2.2: Results from the Survey

The figure above depicts some of the research's representative findings. According to the results, the policies are disregarded because they are too long, which is related to the overloaded information that they contain.Furthermore, many participants believe that there are several policies that should be read on every website they visit, thus they disregard them.

Based on this data in a genuine study with a significant number of replies, the aforementioned research helped us understand the reasons why people ignore privacy policies. Furthermore, it motivated us to jot out the questions we wanted addressed in our own study.

2.6.2 Privacy policy generator websites

As we indicated in the introduction, there are numerous websites on the market that allow you to create privacy policies. Some of them are:

1. TermsFeed [2]
2. PrivacyPolicies [30]
3. Termify [34]

These websites, which differ somewhat from one another, attempt to develop policies that will be used by users. When the user selects the "create policy" option, a form appears in which the user can specify specific features. A policy text is generated based on the user input. The job of these generators is exactly what we intend to achieve, with the exception that these websites do not investigate the anthropocentric element, therefore their output is simply text. What we wanted to adapt to this work, is the text to be more user friendly so

that we can gain understanding and user attention for reading the policy. As a result, the questions in our generator differ from those on the web pages in certain ways, because the goal is to understand as much as possible in order to produce an understandable template at the end.

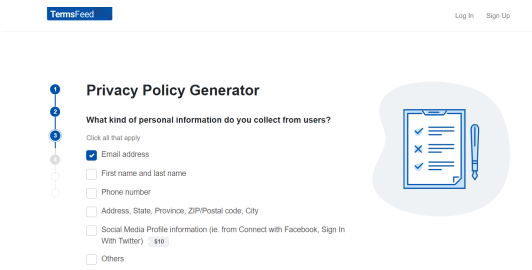
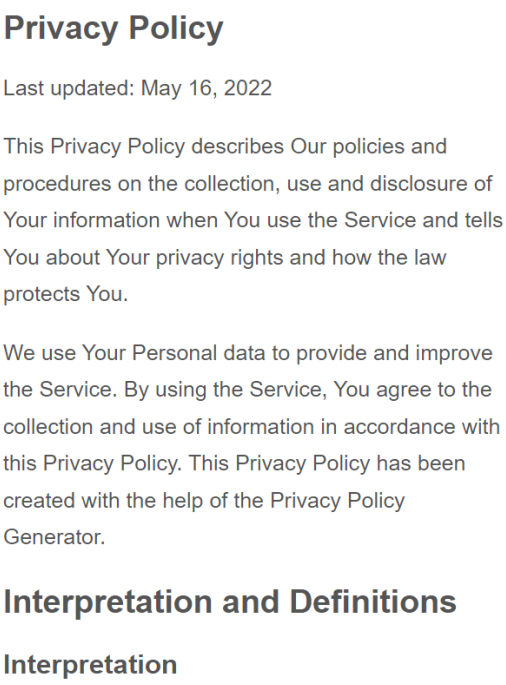


Figure 2.3: TermsFeed website example



Privacy Policy

Last updated: May 16, 2022

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service and tells You about Your privacy rights and how the law protects You.

We use Your Personal data to provide and improve the Service. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy. This Privacy Policy has been created with the help of the Privacy Policy Generator.

Interpretation and Definitions

Interpretation

Figure 2.4: TermsFeed result example

Figure 2.4 depicts the TermsFeed website's homepage, from which you may begin developing your privacy policy. The policy is developed in the manner indicated in Figure 2.5 after a few stages. As we can see, it is simply text.

Chapter 3

Creating a GDPR-compliant and user-friendly privacy policy template

3.1 The problem and the goal

As discussed in Chapter 1, privacy is an important issue in modern society. Those who use the Internet run the risk of having their privacy violated. We can deduce from the legislation enacted by governments that people have the right to be informed about the personal data gathered by websites and to choose whether or not to provide consent. This is something that is accessible via a website's privacy policy.

However, creating a privacy policy is not a simple task since you must consider two major factors:

1. To be in accordance with the regulations.
2. To be simple, effective
3. and user-friendly.

Most companies opt to spend more time focusing on the legal aspect of privacy policies while neglecting the anthropocentric aspect. This results in a scenario in which individuals acquiesce passively to regulations without even comprehending the substance.

For the purpose of the study, we created and disseminated a survey where we attempted to examine the needs and knowledge that exist regarding privacy policies and the current GDPR Regulations.

According to the study results, 40.8 percent of respondents stated that they will ignore the privacy policy, while 35.4 percent stated that they are extremely likely to ignore the privacy policy. Moreover, the most common reason for individuals ignoring the privacy policy is that it is time-consuming and contains legal jargon that they do not understand.

Second, they are unconcerned about it, and third, they cannot find it when using the website.

The objective is to produce a Privacy Policy Template that is consistent with GDPR regulations while also ensuring that the privacy policies are legible and that people take the time to understand how their personal data is being used, provide their consent, and feel safe when browsing the Internet. Simultaneously, website owners would feel that they have properly informed their visitors by establishing a user-friendly policy.

3.2 The survey

Purpose: The purpose of this questionnaire was to understand the current knowledge that exists around the concepts of privacy and how people interact and behave with privacy policies.

Sample: Participants (N = 130) consisted of an open call of different people who use the Internet. The sample was 38.5% female, 61.5% male (0% not identified) from ages 18 to 65. Furthermore, the majority of the sample were European (91.5%), 6.2% Asian, 1.5% North American, and 0.8% South American. In addition, as regards the education level the sample was 46.2% University Degree holders, 40.8% Postgraduates, 9.2% High School Diploma holders, and 3.8% Ph.D. holders. Moreover, 72.3% of the sample was familiar with Software Development. The given questionnaire was entirely voluntary, there was not given any credit and all the participants were required to give their consent and agree with requirements in order to complete the survey. In a scenario where the participant did not give his/her consent, the questionnaire was not available.

Procedure: The questionnaire was distributed by social media (Facebook, Twitter) and personal emails in February 2022. The survey was divided into four components. The first segment was about gathering personal information, while the second was about understanding people's perceptions and knowledge of privacy. Section three was about privacy policies; the goal of this section was to see how different people interact with current privacy regulations. The latter two sections discussed industry expertise and the concept of a GDPR-compliant anthropocentric privacy policy template and generator.

3.2.1 Results

In this section, we will present the research findings, as well as explanations and conclusions about the findings in connection to the thesis's continued development. The questions can be found at the Appendix part.

Section 2: Knowledge about Privacy and Legislation

	Possible Answers (%)		
Questions	Yes	No	Maybe
Do you understand what the term Privacy means?	*94.6*	*0.8*	*4.6*
Are you familiar with the current? regulations for protecting privacy (e.g. GDPR)?	*69.2*	*10.8*	*20*
Do you feel that privacy is important?	*99.2*	*0.8*	
Do you feel that the existing regulations are protecting your data?	*30*	*70*	
Have you ever read the privacy regulations?	*43.8*	*56.2*	
Do you know that the protection of data is a right of every individual?	*94.6*	*5.4*	

Figure 3.1: Knowledge about privacy

We can make the following inferences from the results of Figure 3.1: Despite the fact that 99.2 percent of respondents believe privacy is important, only 30 percent believe privacy regulations protect their data. This, however, contradicts the fact that just 43.8 have read a privacy policy.

	Possible Answers (%)				
Questions	*1*	2	3	4	5
How familiar you are with the regulations of GDPR?	*11.5*	*13.8*	*30*	*36.4*	*8.5*
How much do you feel that your privacy is being violated while using the Internet?	*0*	*7.7*	*28.5*	*33.1*	*30.8*

Figure 3.2: Knowledge about privacy in scale 1-5 (being the highest)

The following are the outcomes, as illustrated in Figure 3.2: Only a small fraction of 8.5 is entirely aware with the current regulations, while a large amount of 36.4 is very knowledgeable. Furthermore, the majority of participants believe that when they use the Internet, their privacy is being jeopardized..

Open Questions: In the question about what regulations are people are aware of, 120 people (92.3%) answered that they are aware about GDPR regulation, while a percentage of 10.8% said that they are also aware about CCPA and 7.7% COPPA.

Section 3: Privacy Policies

	Possible Answers (%)		
Questions	Yes	No	Skip
Do you know what a privacy policy is	*93.8*	*6.2*	
Have you ever disagreed with the privacy policy of a website?	*47.7*	*52.3*	
If the answer to the previous Question is yes, did you continue using the website without any problem?	*20*	*26.9*	*53.1*
Do you always give your consent about your personal data?	*29.2*	*70.9*	
Do you always know how your personal data are being used?	*7.7*	*92.3*	
Do you understand that a website is obligated to use your data if and only if you give your consent?	*96.9*	*3.1*	

Figure 3.3: Privacy Policies

According to results of Figure 3.3, 92.3 of the participants do not know how their data is used, despite understanding in 96.9 that a page can only use the data if you have given your approval. Furthermore, a substantial proportion of 47.2 stated that they had once again disagreed with a privacy policy, yet despite this 20% disagreeing, they continued to use the page normally. Participants also responded (70.9%) that they do not always grant their consent.

	Possible Answers (%)				
Questions	*1*	2	3	4	5
When visiting a website, how likely is it to ignore the privacy policy?	*1.5*	*4.6*	*17.7*	*35.4*	*40.8*

Figure 3.4: Privacy policies in scale 1-5 (5 being the most likely)

According to the results of Figure 4.3, a substantial number of 40.8 of the participants believe it is extremely probable (5) to disregard a privacy policy.

Open Questions:

Possible reasons for ignoring a privacy policy	*Answers (%)*
You do not care about it	*23.8*
You cannot find the privacy policy	*14.6*
You think is time-consuming	*76.2*
You are not aware of how important it is	*10.8*
Too much legal–type wording Text with a lot of details	

Figure 3.5: Privacy policies open question

According to the findings presented in Figure 3.5 regarding the reasons of ignoring a privacy policy, the primary reason for disregarding a policy is that it takes too much time, and the secondary reason is that they are not interested in reading it.

Possible reasons for declining a privacy policy	*Answers (%)*
You do not feel secure	*45.4*
You think that the website is violating your privacy	*52.3*
You think your data will be used for commercial purposes	*51.5*
You never decline the privacy policy	*15.4*

Figure 3.6: Privacy policies open question

Furthermore, according to the results shown in Figure 3.6, the primary reason for declining a policy is the fell that the website is violating their privacy and second that the data is going to be used for commercial purposes.

3.Section 4: Industrial Knowledge

	Possible Answers (%)		
Questions	Yes	No	Skip
Are you familiar with designing websites?	*55.4*	*44.6*	
Are you familiar with Software Development?	*72.3*	*27.7*	
Have you ever created a website?	*55.4*	*44.6*	
Have you ever considered inserting a privacy policy on your website?	*24.8*	*20.7*	*54.5*
Do you always know how your personal data is being used?	*7.7*	*92.3*	
Do you understand that a website is obligated to use your data if and only if you give your consent?	*96.9*	*3.1*	

Figure 3.7: Industrial Knowledge

In addition to collect information about the general understanding and knowledge of privacy policies, we wanted to see if anyone who knows how to create pages would find it

	Possible Answers (%)				
Questions	*1*	2	3	4	5
If you have inserted a privacy policy in your website, how easy was it for you to understand what it must contain?	*15.4*	*23.1*	*29.2*	*23.1*	*9.2*

Figure 3.8: Industrial knowledge on scale 1-5 (5 being very difficult)

simple to add a privacy policy to their page. As demonstrated in Figures 3.7 and 3.8, only 9.2 of the 72.3 participants who are familiar with Software Development and 55 who had re-created pages indicated in grade 5 that they knew or comprehended what to add to a page's privacy policy. This made us realize that there are many flaws in the realization of what is needed to be included in a policy.

It is clear from the results that, even though individuals understand that privacy is essential, and thus reading privacy rules is vital, they do not take the time to read privacy policies as they should. Passively accepting a privacy policy jeopardizes the integrity of people's privacy.

3.3 What is required for designing a user-friendly policy

When developing an object that will interact with people, we must keep in mind the necessity of user-centered design. Our purpose is to achieve objectives while adhering to strict guidelines. Our objectives are to gain a better knowledge of the design, who the object is intended for, and why. Furthermore, the constraints cover the type of material to be used as well as any safety concerns.

The golden rule is made up of two key components.

1. be familiar with the material and design
2. to comprehend people

The anthropocentric design must be considered for the second rule. The basic design tasks are governed by three anthropocentric design principles.

1. Desirability

2. Feasibility

3. Viability

Moreover, interface interaction is said to be a cognitive process. To be able to describe and predict human behavior, such as communication with a system or object, we must consider the cognitive processes that are triggered as well as the constraints in user perception. We must be aware of what users are anticipated to be able to do and what they are not expected to be able to achieve. This allows us to identify the texture and root causes of the difficulties that consumers encounter.

Privacy policies, as discussed above, confront the problem of being overly time consuming and long, and hence are ignored by users. People's interaction with policies it is very low as a result. The policy should be presented in such a way that it facilitates the cognitive process of understanding it. When a person attempts to identify a topic of the policy that interests him, for example, it should be prominently shown rather than concealed amid thousands of phrases.

All of the aforementioned aspects should be taken into account when building an effective user-friendly policy template.

3.4 Privacy policies design

Considering Privacy by Design principle 6, "Visibility and Transparency," we can see that users must be able to understand the privacy policies and how their data is being utilized in a straightforward way.

Article 12 of the General Data Protection Regulation (GDPR) [37] states that privacy notices – policies should be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. The information shall be provided in writing or by other means, including where appropriate, by electronic means.

Most websites, however, present privacy policies as legal documents. Usability methods described above aim to give the guidelines for creating policies that are not written by lawyers to lawyers. Unfortunately, today's privacy policies are not created with a user-centric design, and privacy and security researchers have concluded that privacy notices not only fail to help consumers make informed privacy decisions but are mostly ignored by them.

When asked why they disregard privacy rules in the survey that we created and described above, the majority of respondents said it is time-consuming, which is quite reasonable given that privacy policies are just a document with terms that most people do not comprehend.

The GDPR's criteria are strict, and the penalties for non-compliance are severe. There is a natural tension between making the policy attractive and accessible while remaining strong and legally sound. It is significantly more difficult to be brief than it is to be wordy when it comes to legal drafting. Privacy policies may provide the required information, but they are failing to maintain communication with the users. It is a significant difficulty and challenge to establish an incredibly strong privacy policy while preserving legal intricacy and actually making it readable.

3.5 Designing a User-Friendly policy template steps

To develop our own user-friendly privacy policy template we listed down some particular steps while thinking about the guidelines we mentioned before. In the future, these steps can be improved and fulfilled in greater depth.

1. First Step : The first phase in creating an effective user-friendly policy template is identifying the issues that contradict the usability and Web Content Accessibility Guidelines (WCAG) [1]. This has been made through the survey. From the survey, we had the opportunity to identify the problems that different users faced while interacting with privacy policies and how this affects their experience.

2. Second Step: In the first step, we highlighted the design challenges of a privacy policy; now it is time to think outside the box and build a design process that will provide a solution to the concerns described above. Usually, a successful privacy policy design must incorporate lawyers, content editors, and designers. To develop the best policy, we should have assembled the best team and begin with an end-user approach design. However, in our case, our purpose is to just provide the template for the policy and not the whole document, thus we utilized our knowledge, creating a team of myself and utilizing questionnaires to get the response of different users. All things considered, step two requires to find the best team to co-operate for creating and presenting the policy, but in this case it was about identifying the knowledge needed for the development of the policy.

3. Third Step: Step three should be given to the identification of needs. The initial purpose of this step is to identify the requirements that must be addressed in policy design. This is was the right time to revisit step one to check if the needs are compliant with the regulations mentioned.

4. Fourth Step: Based on the requirements set in step three, the fourth step is the time to put down ideas and create prototypes. In this step we created a variety of sample privacy policy templates. The goal of prototyping is to model the policy so that its

characteristics may be examined even if all of the requirements have not yet been chosen.The prototypes enable experimentation with various designs, as well as the rejection and correction of faults.

5. Fifth Step: After the prototypes have been produced, we had to select one of them that complies with all that we wanted the policy to have. This signifies that design decisions have been made at the previous steps.

6. Sixth Step: Step 6 is the evaluation and the acceptance of the users. User testing provides sufficient information about users' experiences and how they respond to policies. Because it is critical to create a user-friendly policy, the evaluation from the user itself is the most significant aspect. For this step, we gave the selected prototype to different users in order to evaluate them.

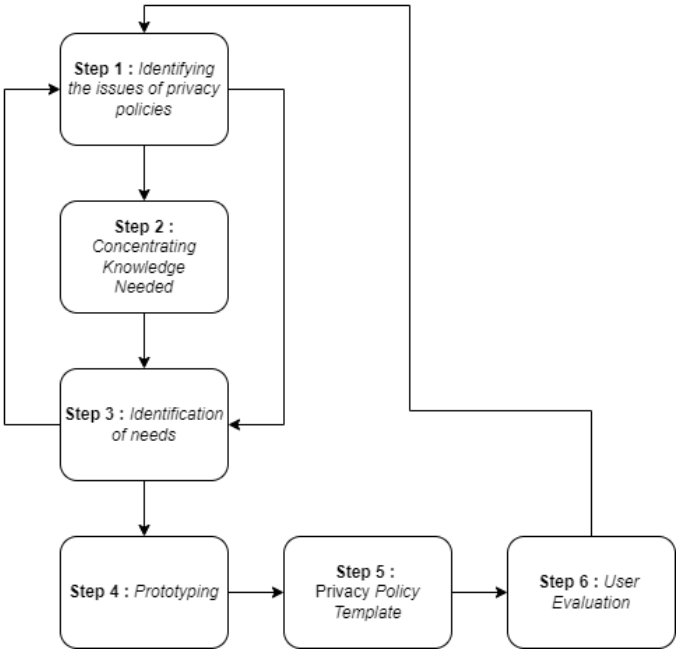


Figure 3.9: Designing Steps

3.5.1 Ensuring that the policy template is GDPR compliant

A GDPR privacy notice is a crucial tool for assisting consumers in making informed decisions about the data being gathered and handled.

According to the GDPR [38], every website must provide people with a privacy notice that is in a concise, transparent, intelligible, and easily accessible form. The GDPR also specifies the information that an entity must provide in a privacy notification. The criteria

differ slightly depending on whether, the website gathers data directly from a person or obtains it from a third party.

In our case, as the developing website collects information directly from a person, the following information must be included in its privacy notice: [28]

1. The identity and contact details.
2. The purpose for the website to process an individual's personal data and its legal basis.
3. The legitimate interests of the website (or third party, where applicable).
4. Any recipient or categories of recipients of an individual's data.
5. The details regarding any transfer of personal data to a third country and the safeguards taken.
6. The retention period or criteria used to determine the retention period of the data.
7. The existence of each data subject's.
8. The right to withdraw consent at any time (where relevant).
9. The right to lodge a complaint with a supervisory authority.
10. Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.

Per Article 14(3) [18], if you obtain personal data from a third party, you must communicate the above information to the data subject either: no later than one month after you have obtained the data, at the time you first communicate with the data subject, or before sharing the data with another organization.

The main questions that must be answered through a privacy policy and thus they must include in the user-friendly policy template are:

What data do we collect?
How do we collect your data?
How will we use your data?
How do we store your data?
What are your data protection rights?
What are cookies?

How do we use cookies?
What types of cookies do we use?
How to manage your cookies
Privacy policies of other websites
Changes to our privacy policy
How to contact us
How to contact the appropriate authorities

3.6 A user-friendly privacy policy template sample

The European Union has established a template for privacy policies to show how they should be organized and what they should include [42]. However, there are no instructions or information in this template about how the policy should be presented to users in a user-centric design.

My goal was to build a new template sample and representation that was both GDPR compliant and user centric. We used the terms described in Section 3.2 for building a user-friendly policy, the user-friendly design steps described in Section 3.3, and the GDPR regulations and template to do so.

There are two factors to note here, the user-centric design factor and the GDPR compliance.

In the template, the focus is on the user-centric design as our purpose is to create the policy to be in a more user-friendly form.

3.6.1 User-Centric factor

Three Challenges:

1. Present the overloaded information in a user-friendly environment
2. Provide memorability through visual affordance
3. Provide understandability

    (a) Present the Overloaded Information in a user-friendly environment

    One of the most common problems with privacy policies is that they are frequently too long, leading people to believe that it is time-consuming to spend their time there.

    Thinking about the aids of organizing information based on visual perception, we decided that the relative size of the material presented can be moved to a

single page containing information that is relatively appealing to the reader. A search or request can cover a wide range of details.

So, the goal is to gather the majority of the information on one page, to configure the page in little boxes responding to each one to policy questions, and to have a relevant link for extra information adjacent to each case, for example (What data we collect).

(b) Provide memorability through visual affordance

The virtual force of the information and the intimacy we feel towards it, according to the user-experience expertise field, alter our understanding of it. Thus, using familiar items with semantic content in design is a well-known strategy. When developing an interface, it is preferable to provide acknowledgment rather than a reminder, and virtual material is preferable because it is easier to understand.

To improve memorability , we decided to add some icons to the policy representation to add visual affordance; however, we were concerned that this would be prohibited by GDPR regulations. Surprisingly, GDPR UK stated in recital 60 of EU Recital: "that information may be provided in combination with standardized icons in order to give in an easily visible, intelligible, and clearly legible manner, a meaningful overview of the intended processing.

The right icons are the those that they are metaphors. In user interface design, an interface metaphor is a set of user interface visuals, actions and procedures that exploit specific knowledge that users already have of other domains. The purpose of the interface metaphor is to give the user instantaneous knowledge about how to interact with the user interface.

(c) Maximize Understandability

In order maximize understand-ability we decided to reduce the word count and the amount of legalese terms presented in the policy. We wanted the sentences to be represented in a more fluent way.

3.7 Template example

At this point, we will present the template we created to illustrate a user-friendly privacy policy. This template was chosen from among several options at step 5 of the steps we described above. All the steps followed steps are described in full below.

(a) First Step : The problems needed to identify and solve was the overloaded information of text presented at the user in one single page, the amount of legalese terms that used are presented and to make the policy more comprehensive to the average person. At this point, we recognized that in order to be completely correct, we needed to see in the user the capacity to read all of the terms and the official policy with the click of a single button.

(b) Second Step: The knowledge needed to provide solution to the above problems and challenges were discussed through the background study of this thesis. This includes the user-experience terms, the GDPR compliance factors and the designing steps.

(c) Third Step: The requirements that be addressed were the three challenges described above, present the overloaded information in a user-friendly way, provide memorability and learn ability and provide understandability.

(d) Fourth Step: In this step we created a variety of sample privacy policy templates. We tried different symbols and ideas on how the layout of the template we will be like.

(e) Fifth Step: We tried to combine all the things that we tried in the fourth step and select the right template. This was actually the most difficult part.

(f) Sixth Step: Step 6 is presented below at the evaluation of the template, and has be completed by a questionnaire by different users.

Figure 3.10: User-Friendly Policy Template

3.8 Evaluating the template

To examine how various individuals would respond if they saw this policy against a normal legalese privacy policy template, we built a questionnaire to assess how user-friendly the template that we designed is.

Sample: Participants (N=46) consinsted of an open call of different people who use the Internet. The questionnaire was created through google forms, and distributed through social media pages.

Procedure : In this questionnaire, we compared two proposed policies. The first template is the standard one found on most pages, whereas the second is one we made using user-friendliness and usability approaches.

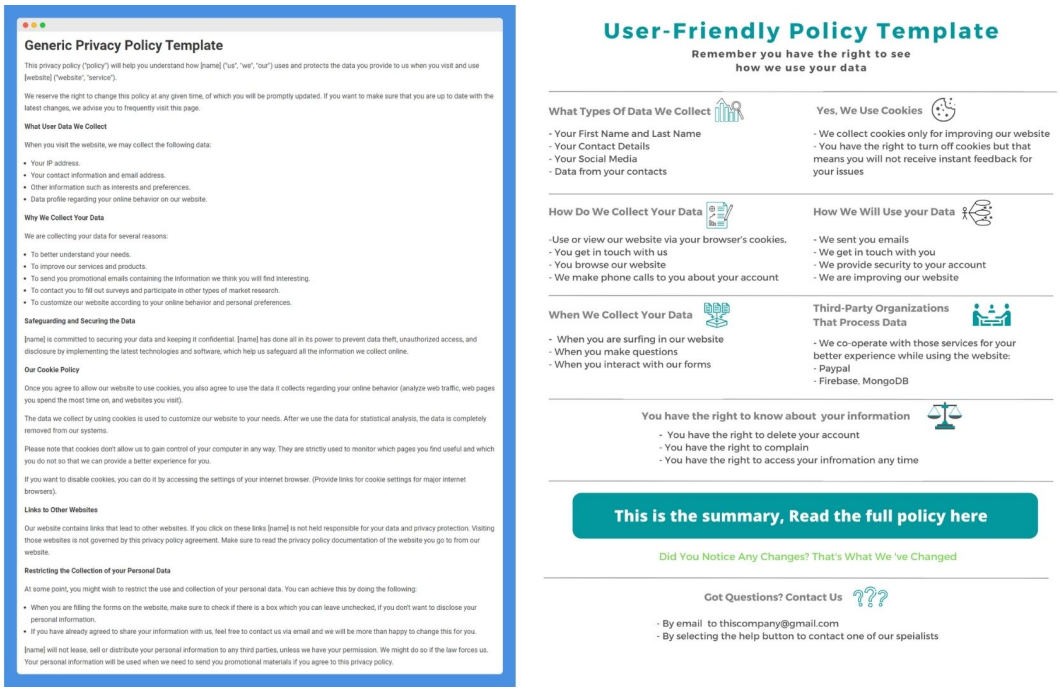


Figure 3.11: The two comparison policies

** The questionnaire can be found in the Appendix.

3.8.1 Results

Table 1 : Privacy Policy Template 1 (1-5) :

	Possible Answers (%)				
Questions	*1*	2	3	4	5
Would you spend some time reading this policy – 5 (being definitely)	*28.3*	*56.5*	*13*	*2.2*	*0*
How User-Friendly do you believe that is? – 5 (being a lot)	*26.1*	*43.5*	*23.9*	*6.5*	*0*

Figure 3.12: Template Evaluation 1

Table 2 : Privacy Policy Template 1 (Yes/No/Maybe)

	Possible Answers (%)		
Questions	Yes	No	Maybe
If you see this policy, would you care to read it?	*8.7*	*63*	*28.3*

Figure 3.13: Template Evaluation 2

According to the results shown in Figures 3.12 and 3.13 regarding policy template 1: As we can see from the results, just 2.2 percent would take a short time to read the policy, while 56.5 percent said they would read it in grade 2, indicating that it is highly unlikely. The respondents also assessed the policy's user-friendliness as 2 with a percentage of 43.5, suggesting that it is unreachable to the user.Furthermore, we can observe that the majority of respondents picked No when asked if they wanted to read the policy. This demonstrates that the policy is not easily accessible, and that the ordinary user would not read it.

Table 3 : Privacy Policy Template 2(1-5) :

	Possible Answers (%)				
Questions	*1*	2	3	4	5
Would you spend some time reading this policy – 5 (being definitely)	*0*	*4.3*	*15.2*	*43.5*	*37*
How User-Friendly do you believe that is? – 5 (being a lot)	*0*	*0*	*4.3*	*41.3*	*54.3*

Figure 3.14: Template Evaluation 3

Table 4: Privacy Policy Template 2 (Yes/No/Maybe)

	Possible Answers (%)		
Questions	*Yes*	No	Maybe
If you this policy, would you care to read it?	*73.9*	*0*	*26.1*

Figure 3.15: Template Evaluation 4

The outcomes of Policy 2, as shown in Figures 3.14 and 3.15, are vastly different from those of Policy 1. Initially, we had 0 in the selection "I would certainly read the policy" in the first policy, but now we observe a proportion of 37 picking it. Furthermore, we notice that 43.5 percent picked option 4, indicating that they would be extremely inclined to read the policy. When asked how much user-friendly policy is regarded the majority, they selected choice 5 with a percentage of 54.3, indicating that it is to a great extent.

Table 5: Comparison between both

	Possible Answers (%)		
Questions	*Policy 1*	Policy 2	Neither
What Privacy Policy Template do you believe is more User-Friendly?	*0*	*97.8*	*2.2*

Figure 3.16: Template Evaluation 5

According to the results of Figure 3.16, the answers indicate that choice 2 is preferred. We can corroborate this with the last question, in which respondents picked option 2 as the most user-friendly with an overwhelming majority of 97.8.

Conclusion: The questionnaire was designed to assess if we met the objectives in developing a template while preserving a user-friendly privacy policy. We may conclude that the template was effective based on the questionnaire responses that compared it to a common average template of current policies.

Chapter 4

User-Friendly Policy Generator

4.1 Explanation

Trying to come up with a solution to the major issue of unconventional acceptance of privacy policies, we decided to design a web application called PrivacyUI that would allow various companies to generate policies that are GDPR compliant, free, and presented to the user in a user-friendly manner. This generator varies from previous policy generators in that it produces a user-friendly policy and not just a plain text, as stated in the preceding chapters. The provided policy is based on the template mentioned at Chapter 3.

4.2 Analysis of requirements and specifications

4.2.1 Introduction

Life cycle model

From the beginning of development (concept definition) until completion (system in operation), most computer systems follow a life cycle model with a defined methodology for the process of content creation and software authoring. Breaking down the software development workflow into critical steps is what the software development life cycle is all about. It walks through the entire project from beginning to end and identifies the weakest points in your process as well as the most dangerous areas.

In the life cycle, there are six crucial phases [39] :

1. Requirement analysis
2. UI/UX Design
3. Software Development

4. Testing and Quality Assurance

5. Deployment

6. Maintenance

For the development process we used the **Agile software development life cycle**. Agile is a prominent software development methodology. The product is separated into small incremental builds and delivered in iterations with Agile development. To prepare working functionality with each build, all jobs are divided into tiny time frames. We picked this approach because we had prior expertise with it and because it is generally convenient to design a system when the team is small and development must be completed quickly. All of the needed features are included in the final product build.

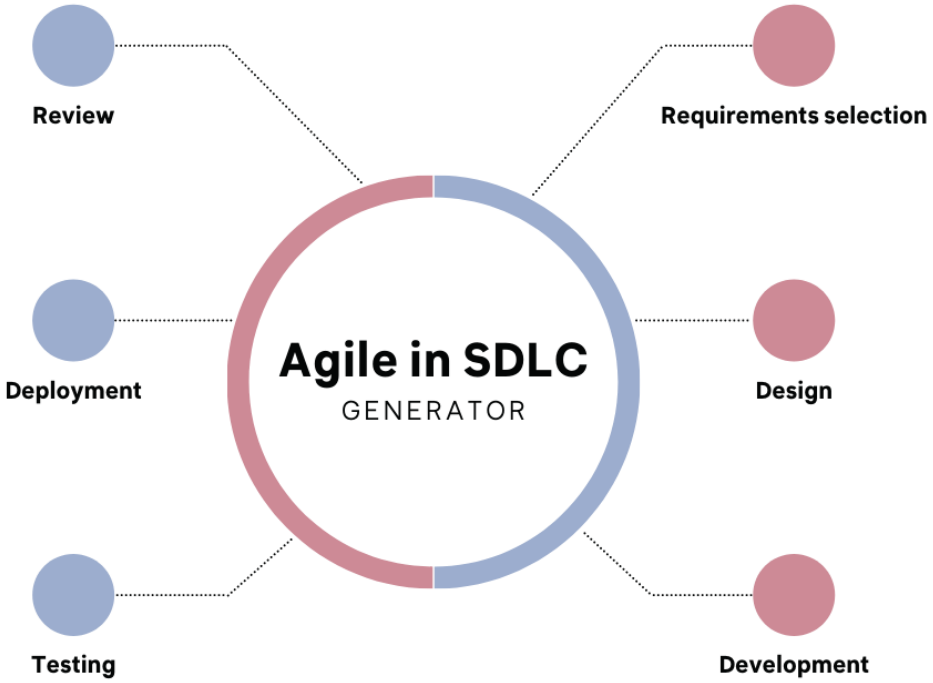


Figure 4.1: Agile Methodology Cycle

Identification of typical users

The system is primarily intended for people who own a business or organization and wish to develop a user-friendly privacy policy. Users can be classified based on their previous experience with a similar system as well as their use of the specific program.

1. Based on user experience : Users can be beginner, experienced, or even advanced.

   (a) Beginner Users: These users have limited experience. They are likely to run into issues the first time they interact with the system, as well as when employing features. However, the system was designed with the user in mind, and it was made as simple to use as feasible and including a tutorial. As a result, the difficulty will be moderate and may include specialized circumstances, but in general, they will be able to conduct operations successfully.

   (b) Experienced Users: These users may not be as familiar as advanced users, but they have most likely reused and interacted with similar systems. They can quickly explore the page, and their mental model assists them in understanding the continuity of their options.

   (c) Advanced Users: These users are entirely accustomed to reusing, familiarizing, and interacting with similar systems numerous times. They know exactly how to operate efficiently, they comprehend the functionalities, and they will have no trouble dealing with any difficulties.

2. Based on the frequency of use of the system : Users can be frequent or occasional.

   (a) Occasional Users: These users will not visit the page frequently, but they will engage with the specific system over time and may recall some information from past visits to improve their user experience. However, if the system is expanded, users will struggle to understand the additional functions.

   (b) Frequent Users: These are the users who will use our system on a daily basis, such as businesses who wish to alter and shape their policies. These individuals can pick up the system quickly, even if they have no prior knowledge. This is due to the familiarity gained through regular interaction.

Work Environment

Users will be able to select information about user data collected on their pages, create policies, and amend them. The page can be visited using any electronic device that has an internet connection.

Limitations and assumptions

We make a number of assumptions about the system. First and foremost, in terms of users, we believe that we have people of all genders and ages. In addition, we make the following assumption about the system: in order for the system to meet the needs of the user and be functional, it must have a server that communicates with a database. In our case the database is based on Firebase [14] and in the during phase can only store hundred users the same time, as it is the default for the free version. The latter is concerned with the limits and assumptions in the interaction of users with the system, with the purpose of making it easier for users to use sections of the system. As a result, we anticipate that it will be accessible from both mobile devices (such as smartphones) and desktop computers.

As a result, the system should be created in a mast format that is responsive in order to maintain the same quality of user experience for all users, whether they are mobile or not. Furthermore, we should make the system basic to facilitate learning, familiarization, and memorizing. In addition to simplicity, we strive for user-friendly elements such as grouping tasks, including a tutorial button, and using appropriate font-family, styles, and colors.

4.2.2 Needs identification

Questionnaire

We tried to think of questions that would assist us to better understand our target users and their needs when developing the questionnaire. We created the questionnaire on Google Forms and distributed it over social media. The survey can be found and explained in detail in Section 3.2

Need for the web-application

We was able to obtain the opinions of the participants for the development of the application by using the questionnaire. Based on the results showing at appendix, a template of a people-centered privacy policy would be very beneficial, according to 93.8 percent of respondents. Furthermore, 95.5 percent of the participants who are business owners believe that a generator of user-friendly policies will be beneficial.

4.2.3 Examples of typical tasks

The system will contain a number of tasks with which the user can interact. In essence, these standard processes describe and demonstrate the end user's capabilities when utilizing this system.

Some of them are:

1. **Creating an account on the system:**The user can create an account on the system in order to store the policies he/she has created and update them later.

2. **Exit the system:**At any point, the user will be able to log out of the system. The system, on the other hand, is responsible for maintaining its data and information if the user has an account so that information of interest to him/her is not lost.

3. **Providing a particular course (Tutorial):**When a user registers in the system, the system will provide him/her the choice to take certain steps to learn certain subjects. These steps are seen as critical in improving the efficiency and efficacy of the user's interaction with the system.

4. **Creating a policy:** The user can create his or her own policy in which he/she or she enters what is required for them from static options.

5. **Edit policy:** The user can make changes to a policy that he/she or she has already created.

6. **Delete policy:** The user can delete a privacy policy that has created.

7. **Create the user-friendly privacy policy:** The user can create the user-friendly policy based on created policies.

8. **Download privacy policy template:** The user has the opportunity to download the policy that he/she/she has created.

4.2.4 Use case diagram - needs identification

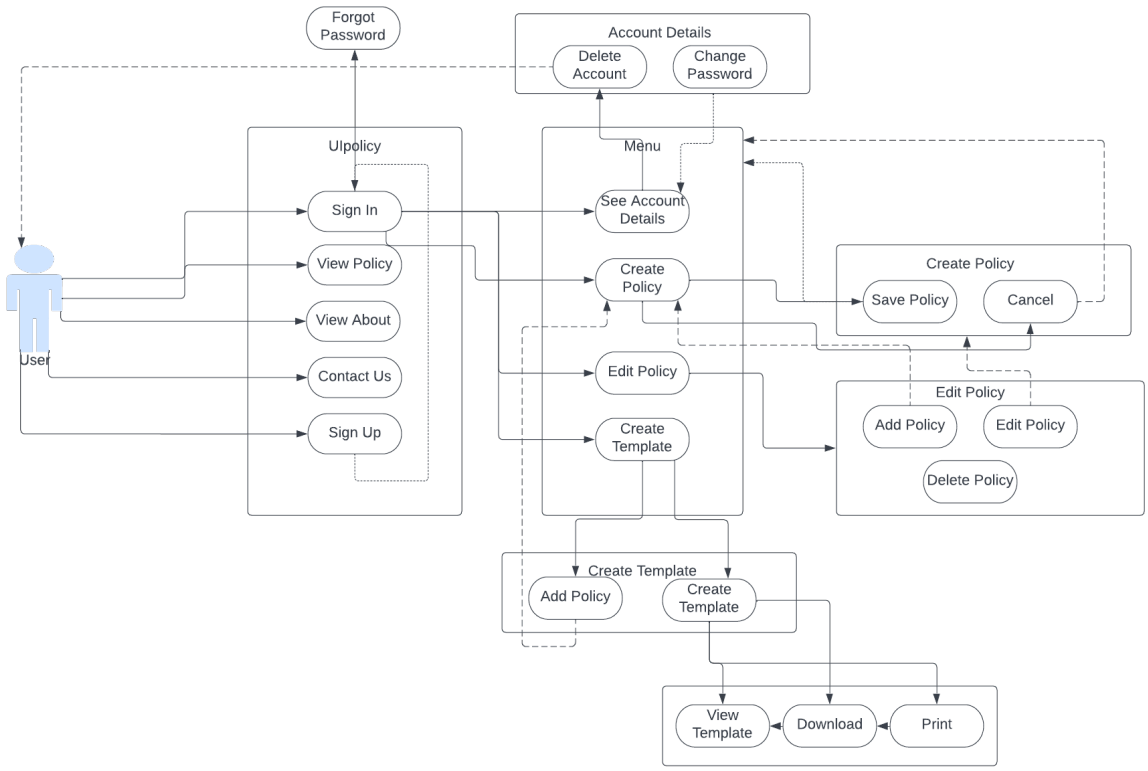


Figure 4.2: Analysis

We used a use-case diagram in order to illustrate the system's high-level functionality and scope. This diagram show how the system and the user interact with one another. Essentially, the diagram depicts the options available to the user when he/she visits each page. This assists in properly organizing the system so that We can be close to the user's mental model and make navigation simple and easy. The diagram defines what the system but not how the system runs inside.

4.2.5 Definition of requirements

When we use the term requirements, we are referring to the what the system must do, i.e. what the result and intermediate function will be, rather than the how," i.e. how this process will be carried out. Requirements are often classified into two types: functional and non-functional requirements. Functional requirements are system features or functions that developers must implement in order for users to complete their tasks. Non-functional requirements are requirements that define criteria that can be utilized to judge the functionality of a system like user-friendliness.

4.2.6 Functional requirements

Number	Functionality	Description
1	Sign Up to the System	The user has the right to register on the website with valid information and to accept the platform's rules.
2	Sing In to the System	The user can access the website by entering a valid email address and a password that matches.
3	Password Recovery	In the event that a person forgets their password, they can retrieve it.
4	Privacy Policy Reader	Any user can read the terms and conditions, the privacy policy on the page.
5	Account deletion	Each user has the option to delete their account.
6	Creating a Privacy Policy	Each user the has an account to the System can create a number of privacy policies
7	Edit a Privacy Policy	Each user the has an account to the System can select a previous policy and edit it
8	Delete a Privacy Policy	Each user the has an account to the System can select a previous policy and delete it
9	Download a Privacy Policy	Each user the has an account to the system can select a policy and download it.
10	See tutorial	Every user has the right to see a tutorial.
11	Logout	Users can log out from the system anytime.
12	Contact Us	Every User can contact the administrator of the page
13	Change Password	Every User has the right to change their account password
14	Change Parts	Every User has the right to change some parts of the policy

4.2.7 Non-Functional requirements

1. Privacy: The data of all users is saved in the Firebase. The password that grants access to the functions is encrypted in the database, so that even the administrator cannot decode it. Before signing up for the web application, the user must be aware of and agree to the data that must be provided.

2. Security: The online application must be protected from outsiders, and user data must be saved securely.

3. Usability: The system should be simple to learn. Techniques such as icons that represent their function and allow the user to predict what will happen next help users avoid mistakes and learn the system more readily.

4. Performance: The system response speed must be low while traversing the system and conducting tasks.Furthermore, the page must be able to handle a large number of concurrent users.

5. Reliability and Accessibility: The system must be dependable in the sense that they must be operational at all times.Furthermore, the website should be capable of ensuring the successful completion of a task.

4.2.8 Definition of usability goals

A system's usability is of the utmost significance. Usability is a crucial parameter of an interactive system's quality and a critical factor in the successful development of a user-focused system. Anthropocentric design, paired with usability goals, ensures that each user has a gratifying and efficient experience.

The usability of the system is confirmed through the five parameters of J. Nielsen

1. **Ease and speed of learning to use the system:** It is critical that users have an easy time using the system and do not require any assistance or advice. We want to give the user the option of quickly adapting to the system. As a result, we employ metaphors and make extensive use of Visual Affordance to ensure that the design model is as close to the user's mental model as feasible. Furthermore, we kept the design simple enough to ensure maximum user happiness.

2. **High-performance function execution:** Users will be able to fully utilize the system's capabilities, completing their desired goals through the system. We want users to be pleased with the system after they utilize it. A policy must be developed swiftly and efficiently.

3. **Ability of casual users to retain their ability to utilize the system over time:** My goal is to increase the system's usability with each subsequent user contact. So, the goal is to not require any assistance or repetition of the instruction after the initial touch with the system. The interface will remain simple, but the user experience will facilitate engagement.

4. **Small number of incorrect handling when using the system and easy way to recover from them:**We have put limits in place so that there is no likelihood of error that will put the user in an uncomfortable spot when using the system.

5. **Subjective satisfaction of users from their contact with the system:** We want the system to be enjoyable for the users, to provide them with complete satisfaction and great emotions. This is accomplished by system maintenance and constant optimization control, which will always provide consumers with complete enjoyment and contentment.

4.3 Explanation of design decisions

4.3.1 Interaction style

We used easy, simple and user-friendly interaction styles

1. **Forms method:** It was thought to be the best fit for the Sign in and Sign Up screens because it is a simple form that collects input from the user. Furthermore, because the fields he/she must fill out are clearly defined and assist him/her throughout the process, this procedure reduces the need for the user to learn. The user merely needs to identify and pick the data. This procedure is sped up because the user uses a familiar keyboard, which he/she is already accustomed with.

2. **Options Menu:** Use the choice menu presentation technique for displays like the generator screen. It was deemed the most appropriate method for correctly presenting the data provided to the user. This makes it incredibly simple for inexperienced users. Also, because we have predefined alternatives from which the user can choose, we don't need to check for inaccurate data input from the user in most circumstances.

4.3.2 Metaphors

There have been numerous metaphors employed. The goal is to get the system as close to the user's mental model as feasible and to improve the user experience. The user

associates the icons with daily things and consequently understands what each function does without assistance. They aid in the system's learning process.

4.4 Technologies and Architecture

1. Prototyping

We utilized prototyping to create the application. Prototyping is a simple technique to create your system's concept and specify requirements prior to the design process. Furthermore, prototyping assists you in selecting the right tools for your implementation. In this situation, we made use of proto.io [20] website.

2. Front-end

For the front-end of the web-application we utilized the Vuetify framework [40]. Vuetify is a Vue UI Library with beautifully handcrafted Material Components. It is a component framework for Vue. Its goal is to create clean, semantic, and reusable components that make constructing your application simple.

3. Back-end

For the back-end of the web-application we utilized Node.js [24]. Node.js is a back-end JavaScript runtime environment that is open-source, cross-platform, and runs on the V8 engine. It executes JavaScript code outside of a web browser. Some of the benefits of Node are its speed, efficiency, and scalability.

4. Database

We host the authentication and database on Google's Firebase [14]. Google Firebase is a Google-backed app development platform that allows developers to create iOS, Android, and Web apps. Firebase offers capabilities for tracking statistics, reporting and resolving app errors, as well as executing marketing and product experiments.

5. Architecture

The architecture we followed in implementing the system is the two-tier web application model using firebase. Firebase is both a storage and real-time database, implement a 2-tier web application where you communicate with the data services directly from the client-side, skipping the classical application server altogether. The system is founded on the presence of a graphical environment with which our page's users will engage by executing the functions.

4.5 Interfaces

4.5.1 Common system interfaces

Main Page

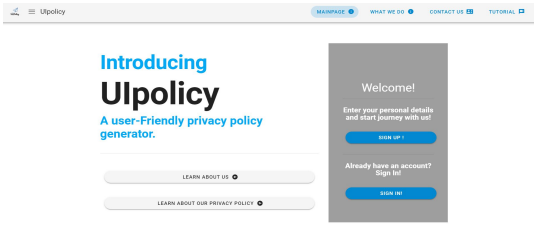


Figure 4.3: Main Page

Figure 4.3 illustrates the user's first point of interaction with the system. When a user clicks on the platform's hyperlink, he/she is directed to the main page. This interface allows the user to register on the platform, what it is the website about, view the website's privacy policy, and view a little tutorial on how the website works and how to communicate. If the user has an account, he/she can log in to it through this page by clicking the Sign In button.

Sign In Page

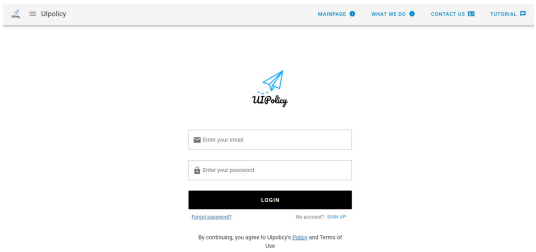


Figure 4.4: Sign In

This page, presented in Figure 4.4, is a sub-page of the "Main Page" page and is used to connect the user to the system. This allows the user to use the page's functionalities. The user's email address and password, as shown in figure 4.5, are required for completion.

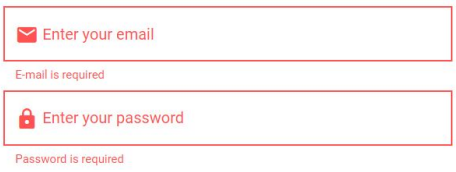


Figure 4.5: Sign In Requirements

If the user enters the information correctly and the database results are valid, the user will be sent to the options menu described below. Otherwise, an error notice will display indicating that the input data is wrong. If the user does not already have an account, clicking the "Register" hyperlink will allow him/her to establish one, while clicking the "I lost my password" hyperlink will take the user to the appropriate page in order to reset the password.

Forgot Password

This page, as shown in Figure 4.6, serves as a backup in case a user forgets his/her password. The user must enter his/her email address, which is associated with the registering account, and then click the Send button. Again, in order to send the request for the password the email is required and it must exists.

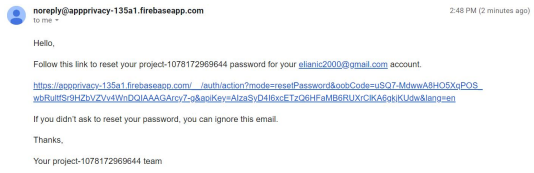


Figure 4.7: Reset Password Link

The reset of the password is implemented by Firebase as default and the process can be seen in the Figure 4.8. The user's new password will be automatically inserted into the database. As a result, the user must use the new password the next time. It should be noted that a link to reset has a time limit.

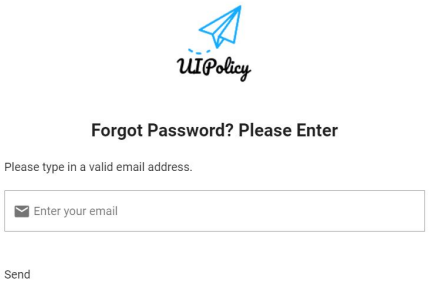


Figure 4.6: Forgot Password

When the user clicks the Send button, an email with a link to change his/her password is delivered to him/her. An email example can be seen in the Figure 4.7.

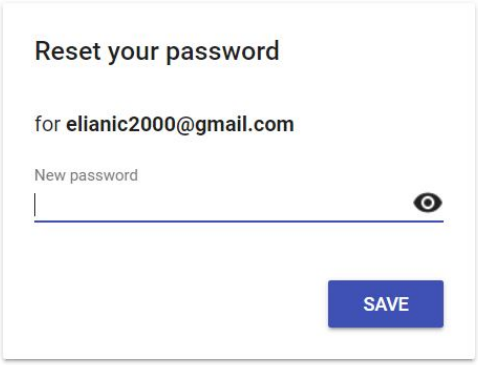


Figure 4.8: Password Reset

Sign Up Page

To access the system functions, you must first create an account. Users set up their own accounts. If the Sign Up button is clicked on the main page, this feature will appear In step one, as shown in Figure 4.9, the new user must provide his e-mail address and name. Acceptance of the platform's guidelines on the General Data Protection Regulation is also required (GDPR). After completing step one, the user clicks the "Next" button to go to the next step of registration.

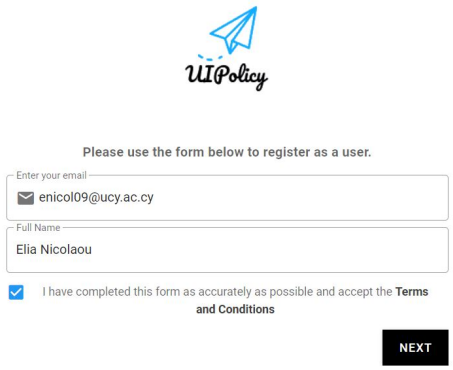


Figure 4.9: Sign Up Step One

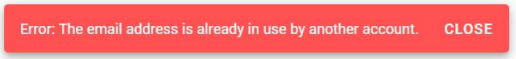


Figure 4.10: Existing User error

The user's email address is examined to see whether it already exists in the database. If it already exists, it prevents the user from proceeding and displays an error notice, as shown in Figure 4.10.

Figure 4.11, illustrates the second step of the registration. The user is prompted to enter his password twice at the second step of user registration. Otherwise, an error notice will be displayed if the password is less than 6 characters long. If everything is right, the user information is saved in the database and the Firebase Authentication hashes the password using an internally modified version of scrypt.

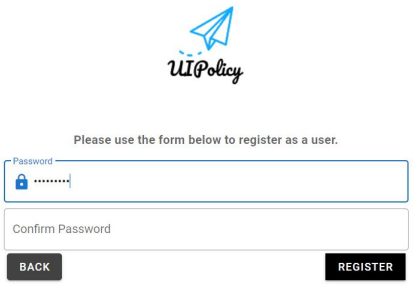


Figure 4.11: Sign Up Step Two

What we do page

The screen seen in the next illustration is entirely auxiliary to the system. This page encourages the user to understand what the system performs in order to decide whether or not to utilize it. Thus, the user may learn about the website by clicking the "What We Do" option from the toolbar.

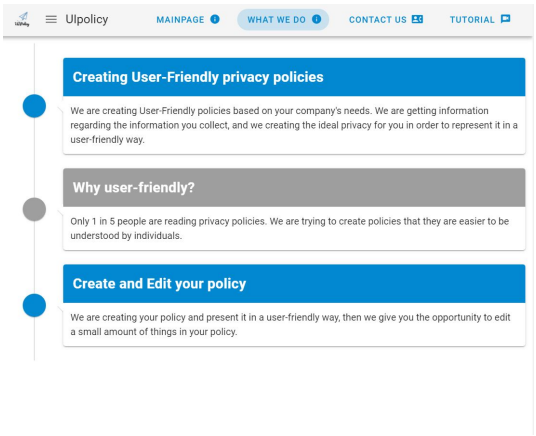


Figure 4.12: What We Do

Contact us page

The Contact Us interface, as illustrated in the Figure 4.13, is likewise the above screen, entirely auxiliary to the system. This screen instructs the user on how to contact us in the event of a system failure or other problem.

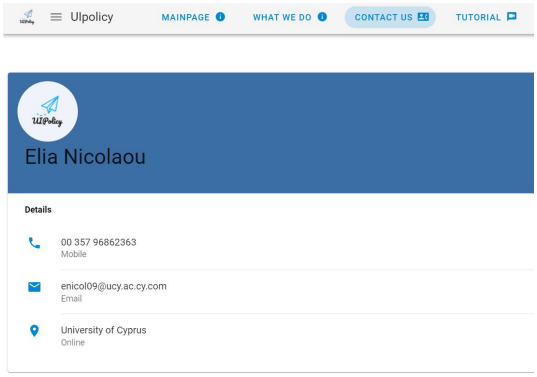


Figure 4.13: Contact Us

Tutorial page

To make the system's operation more comprehensible to the user, we implemented the tutorial option, which can be accessed at any time and from any location. The instructional option allows the user to view a video that explains the system. The tutorial page can been seen in the Figure 4.14.

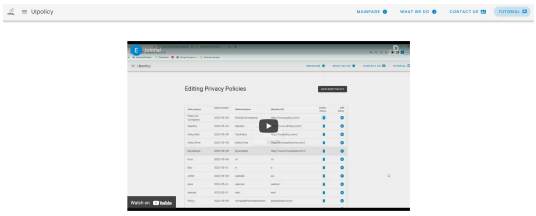


Figure 4.14: Tutorial Page

Privacy policy view

With this option, shown in Figure 4.15 the user may view system's privacy policy.

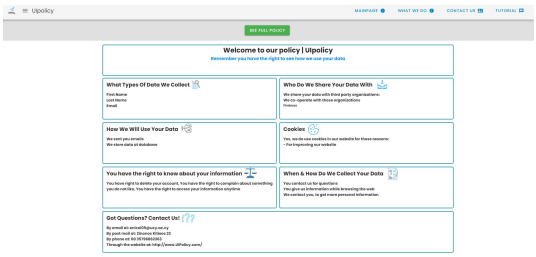


Figure 4.15: Privacy Policy

4.5.2 User interface

Menu

This interface appears once the user enters the system and all user data has been confirmed. This screen essentially displays the user's options for what he/she can accomplish while using the system. The user may create a new policy, amend an existing policy, understand what a policy must have and the system's most essential function to generate a policy in a user-friendly style.

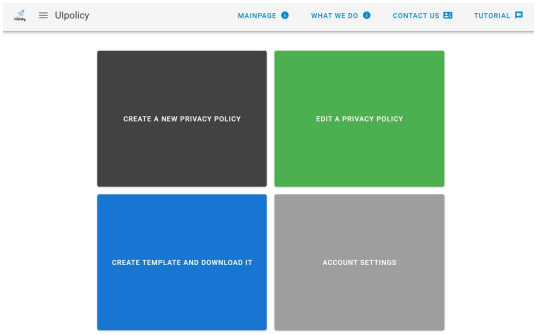


Figure 4.16: Menu

Create a new privacy policy

The function of creating a new privacy policy is one of the most critical functions of the system and is required for the rest functionalities of the system to work. The user selects "Create a new privacy policy" from the menu, which leads him/her to the screen seen in Figure 4.17. To create the policy, the user answers the questions that arise and picks the information that the user wants. The creation is separated into four phases, which display in order when the user completes each step and clicks the "continue" button. The steps can be seen at figures 4.17-4.20.

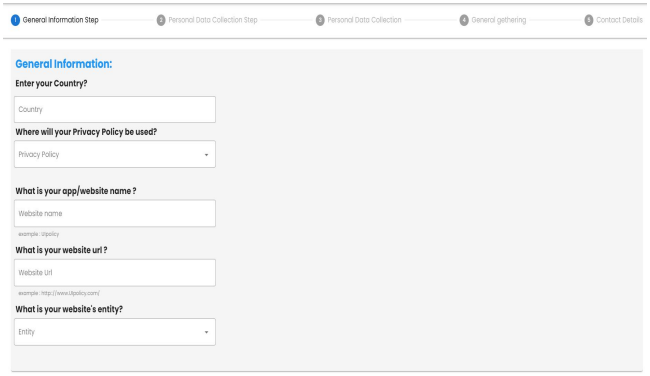


Figure 4.17: Generator step 1

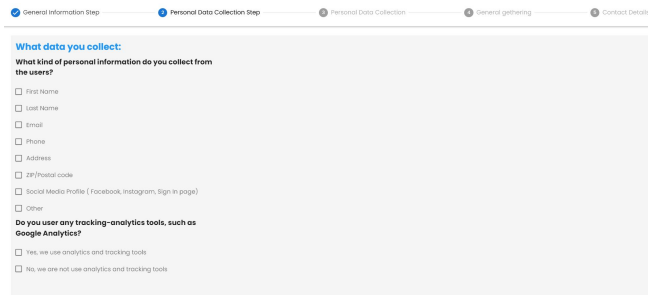


Figure 4.18: Generator step 2

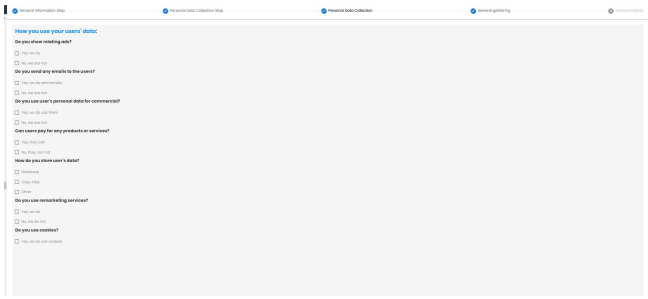


Figure 4.19: Generator step 3

If the user wishes to cancel the policy creation at any moment, he can do so by selecting the "Cancel" button, which returns to the menu. If it reaches the last stage, the Save option appears, allowing users to save the policy.

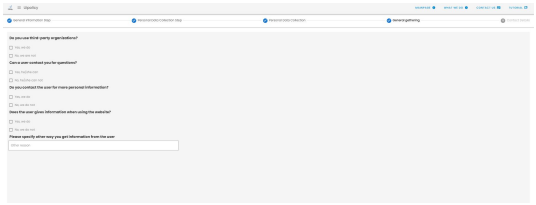


Figure 4.20: Generator step 4

Save a new privacy policy

After creating the privacy policy, the user can save it for future use. This is accomplished by selecting the save option in the generator's final stage. After selecting it, the save screen appears, where the user must enter a name for the policy as well as the date it was created. When the user clicks save, the policy is saved in the database, and when they click cancel, it returns to the previous step.

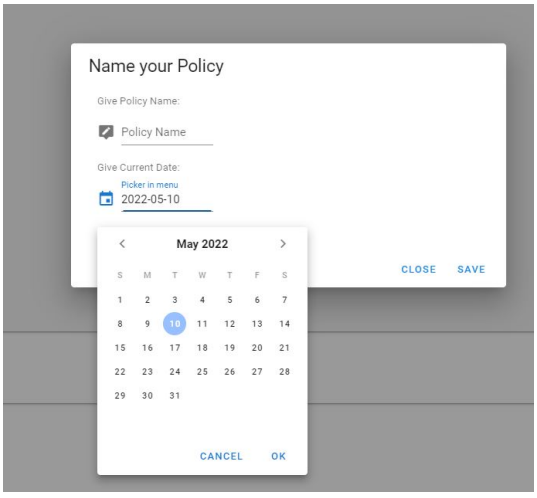


Figure 4.21: Save privacy policy

Edit privacy policy

The policy edit option is the second item on the menu page. The user may view the policies that has created, delete them, or edit them in the sense that he/she can update, add, or remove something. Furthermore, it is given the option to return to the generator screen and construct a new policy by hitting the add new policy button.

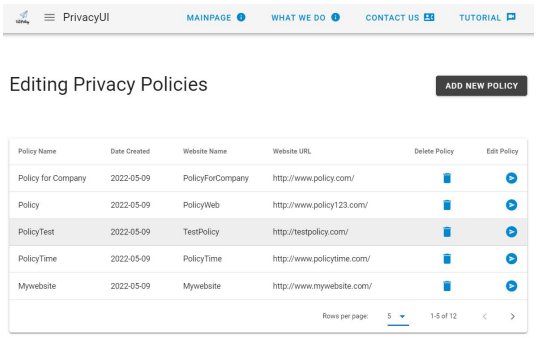


Figure 4.22: Edit privacy policy

Figure 4.23: Edit Policy

In order to update an already generated policy, the user must click the symbol shown in Figure 4.23, which takes the user back to the generator page.

However, this time the page is pre-filled with the user's prior selections as shown in figure 4.24. The old policy will be amended to include the additional possibilities.

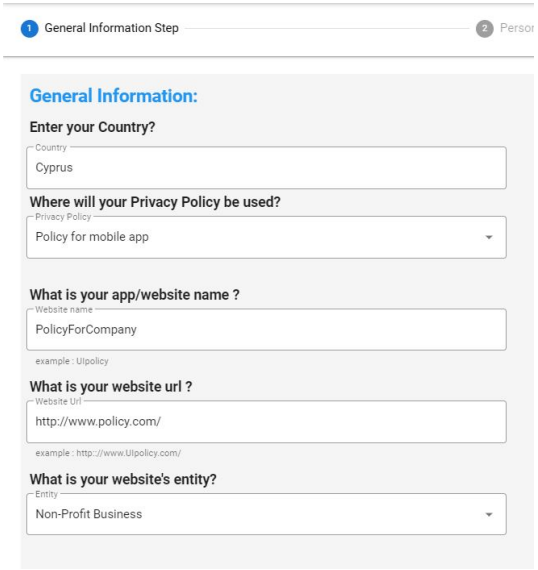


Figure 4.24: Pre-filled policy

Delete privacy policy

Every user can delete a policy that may not want. This is achievable if the user picks the "edit privacy policy" option from the menu and then selects the icon displayed in Figure 4.25, at the line of the policy he/she wishes to remove.

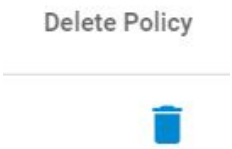


Figure 4.25: Delete policy

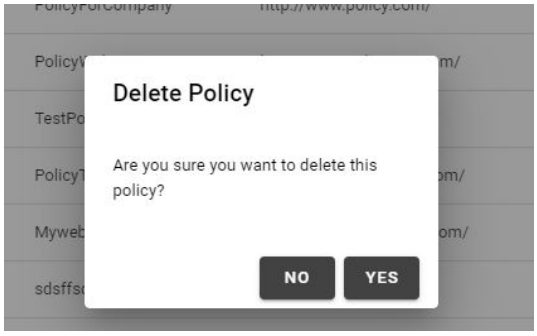


Figure 4.26: Delete policy dialog

When the user clicks the icon, a dialog appears asking the user whether he/she actually wants to remove the policy; if the user selects yes, the policy is erased from the database and no longer appears to the user.

Create privacy policy template

This screen describes the system's most significant and fundamental function.
The system's goal is to generate policies that are presented to the user in a more user-friendly manner using our own template described at chapter three. To do so, the user must select the third option from the menu, "Create template and download it", which will display the screen shown in Figure 4.27. The user may view the policies he has previously written, add a new policy by clicking the button, add new policy, and build the policy template by clicking the button underneath the create template column in each policy.

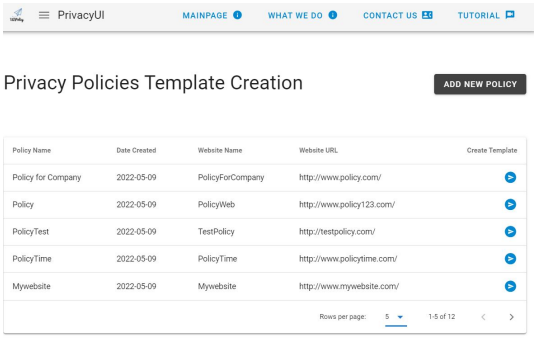


Figure 4.27: Create privacy policy template

Template Creation

The template is created based on the choices given by the user when creating the policy. The template is fixed and deals with the options that the user puts, that is, if the user set that receives three personal information at his/her website, then these three personal information will be presented below the point of the template that refers to it.

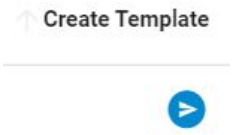


Figure 4.28: Create Template

Template Example

Figure 4.29 illustrates an example of an output policy. The structure is based on the template described on chapter 3. The user has the opportunity to interact with this template by changing the boxes position or changing their side. An example of drag is shown in figure 4.30.

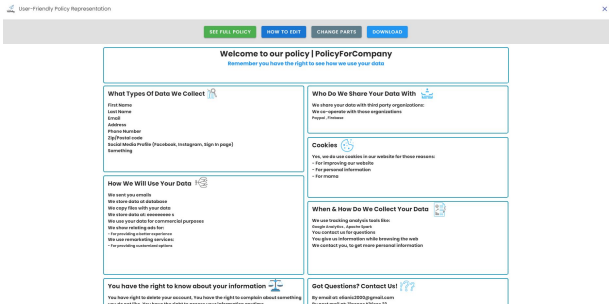


Figure 4.29: Template Example

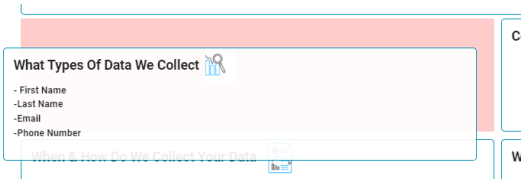


Figure 4.30: Changing position

Download policy as pdf

If the users wish to download the policy locally on their computer, they must pick the download policy button placed on the toolbar of the screen containing the policy, as it shown at figure 4.31. The save window appears when the user picks the button.

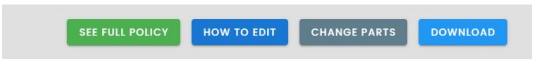


Figure 4.31: Toolbar buttons

Change Parts

Each user has the right to amend particular things in their privacy policy. To do so, the user must click the Change Parts button, as shown in Figure 4.31. The user will then be presented with a dialog in which the user must select the policy part that wish to edit. As shown in Figure 4.32, the user in this example elected to update the header, so the dialog displays the situations that the user can amend.

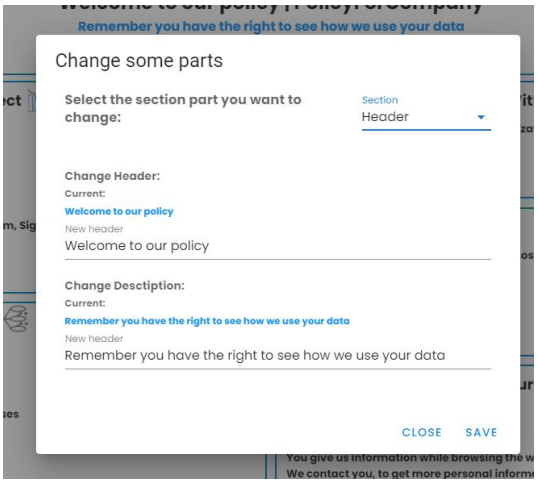


Figure 4.32: Change Parts

See full policy

The user can view the complete legalize privacy policy by clicking the option View full policy, as illustrated in figure 4.31. The full policy is shown in Figure 4.33.

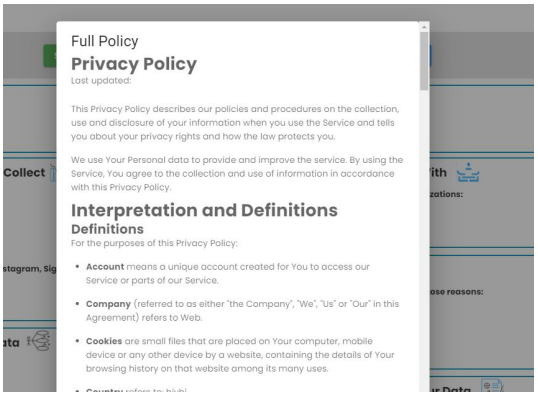


Figure 4.33: Full policy

How to edit

As soon as the user enters the screen, it is unclear what he/she can edit and what he/she can modify, so by clicking on the "How to edit" option, a popup displays, as shown in Figure 4.34, that describes what the user can do.

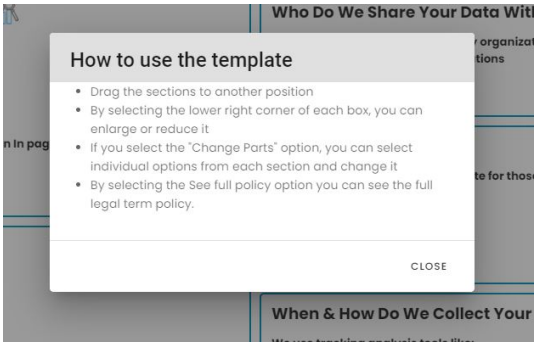


Figure 4.34: How to edit

See account details

Each user has the right to view their account information. The user also has the ability to change the password, log out, and delete the account. To do so, the user chooses the fourth option "Account Details" from the menu. When the user clicks on it, the screen depicted in Figure 4.35 appears.

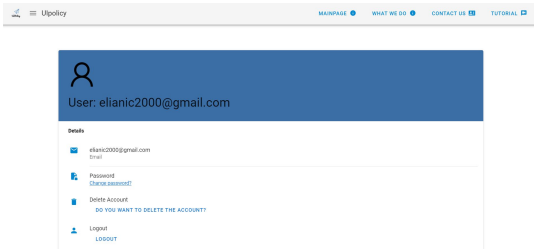


Figure 4.35: Account Details

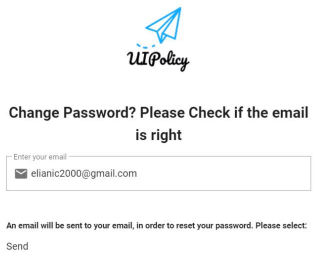


Figure 4.36: Change password

When a user wishes to change the account, he/she must select the change password option. When the option is selected, a screen similar to the "forgot password" screen appears, as shown in Figure 4.36. As with the forgotten password functionality, the user receives an email with a link to change the password.

If the user wishes to delete the account, the very same thing occurs. When the user selects "Do you want to remove the account?" a dialog box appears to confirm the user's choice. If the user chooses yes, the account is deleted and the main page is displayed. When a user sees their account, the final thing they can do is log out. This is accomplished by clicking the log out button, which returns the user to the main page.

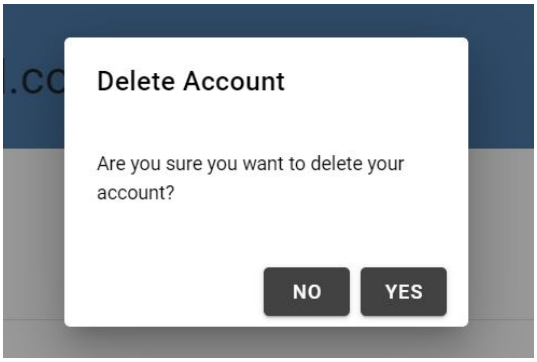


Figure 4.37: Delete account

4.6 Code part

It is a fact that creating a website from scratch takes a significant amount of effort, time and coding. UIpolicy is made up of 38 classes, components, and views in total. The entire project may be found on github at: https://github.com/enicol09/PrivacyThesis

Chapter 5

Privacy policy analysis

5.1 Introduction

At this point, we decided to include a text analysis of privacy policies in the thesis. We used the Python NLTK library and the Textstat library for the text analysis. We built a new data-set based on the numerous findings we drew from the investigation. Then we used this data-set to do some logistic regression, as this described in Chapter 2, to build a model that will assess how comprehensible a policy is in a binary form.

5.2 Text analysis

5.2.1 Important libraries used for the analysis

Textstat Library

Textstat is a simple toolkit for extracting statistics from text. It aids in the determination of readability, complexity, and grade level [35].

Pandas Library

Pandas is an open source data analysis and manipulation tool that is quick, powerful, flexible, and simple to use [27].

NLTK library

Natural Language Toolkit (NLTK) [23] is a Python package that can be used for Natural language processing (NLP) which is the study of how to make natural human language understandable to computer programs. A large portion of the data we may be analyzing is

unstructured and contains human-readable text. We must first preprocess the data before we can analyze it programmatically, and this is succeeded through the NLTK library. [23].

5.2.2 Dataset

For the analysis, we used the OPP-115 [5] data-set to get the text, but we also searched online for other website policies and copied and pasted them into [txt] files. We chose only the [txt] policies from the OPP-115 data-set. The overall dataset for the text analysis consists of 125 privacy policies. Given the hundreds of thousands of privacy rules from current websites, the dataset that we used is minimal and it just representative. However, it was sufficient to obtain some understandable and clear outcomes.

5.2.3 Steps for the text analysis

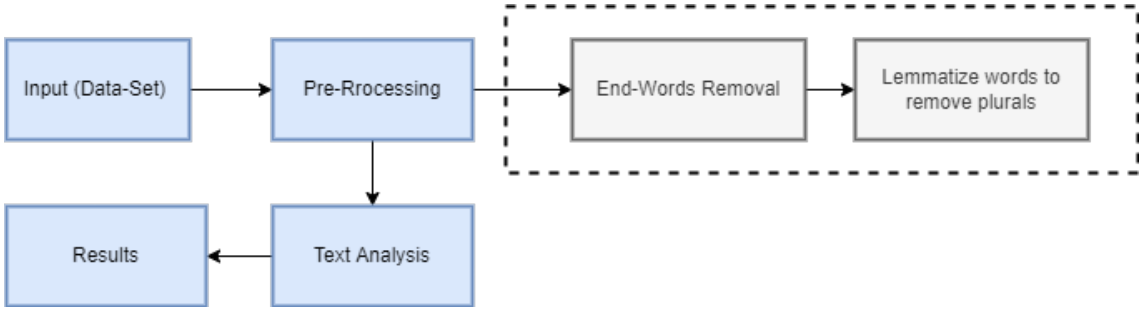


Figure 5.1: Steps for the text analysis

Pre-processing

1. Removing end-words
   A stop word is a widely used word (such as "the," "a," "an," or "in") that a search engine has been configured to disregard while indexing items for searching and retrieving them as a result of a search query. We do not actually desire those words since we cannot get the information we need.

2. Lemmatization of words
   The technique of collecting together the various inflected forms of a word so that they may be studied as a single item is known as lemmatization. Lemmatization is similar to stemming in that it adds context to words. As a result, it connects words with similar meanings to a single word.

Metrics used for the analysis

We created the analysis using the possibilities provided by the libraries described above, and we came up with the metrics listed below.

1. **Word count :** It counts the number of words of the policy after pre-processing.
2. **Line count :** It counts the number of text lines of the policy after the pre-processing.
3. **The Flesch reading ease score:** The score determines a text's readability. The readability score is determined by two variables: the average length of the sentences and the average number of syllables per word. This was found by a function from the TextStat library [11].
4. **Dale-Chall readability Score:** The Dale–Chall readability formula is a readability test that offers a numerical measure of the comprehension difficulty that readers have when reading a document. It employs a list of 3000 words that groups of students can reliably understand, with any word not on that list considered difficult. This was also calculated through a function from the TextStat library [36].
5. **Automated readability index:** The Automated Readability Index returns a value that approximates the grade level required to understand the material. This statistic is also calculated as a function in the text-stat library.
6. **Readability Consensus:** Based on eight readability algorithms, readability consensus assigned a score to the text based on the projected school grade level necessary to understand it.
7. **McAlpine EFLAW readability score:** It returns a score for the readability of an English text for a foreign learner or English, with emphasis on the quantity of mini-words and sentence length [21].
8. **Reading time:** It is the calculated time that need for the text to be read.
9. **Cleaned word count:** The cleaned words number, without the stop words.
10. **Unique word count:** The number of specialized words that they are presented only once.
11. **Cleaned unique word count:** The cleaned specialized words number, without the stop words.

5.2.4 Analysis results

We generated a correlation heatmap to show the correlations between the metrics in order to assess the correlation that each metric might have with each other for the 125 policies. A correlation heatmap is a heatmap that depicts a 2D correlation matrix between two discrete dimensions, with colored pixels representing data from a monochromatic scale. The values of the first dimension display as rows in the table, while those of the second dimension appear as columns [16]. The Figure 5.2 depicts the correlation heatmap. Specifically in this heatmap the darker color means negative correlation between two metrics and very light means positive correlation between the metrics.

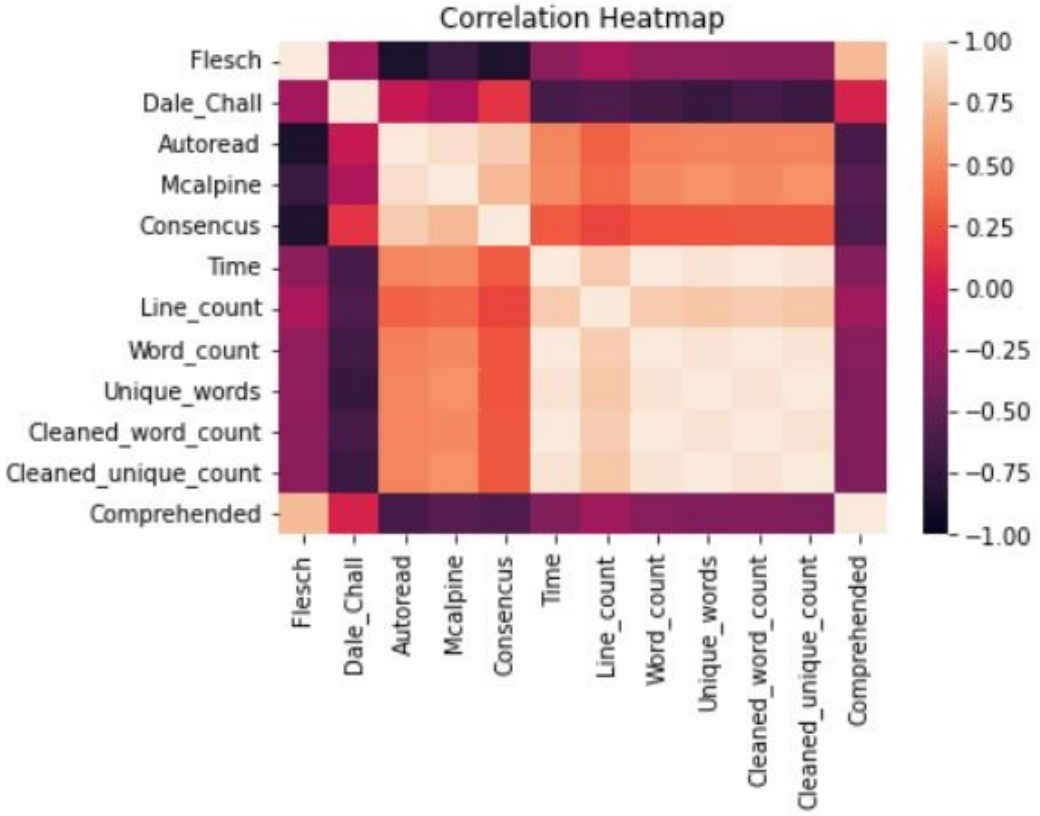


Figure 5.2: Correlation Heatmap

According to Figure 5.3, strong correlations are depicted between the following metrics:

1. "Time" and "Dale Chall"
2. "Line count" and "Dale Chall"
3. "Flesch" and "time"
4. "Dale Chall" and "word count"

We should point out that the association between the metric "comprehended" and the remainders, will not be included in the analysis here.

5.2.5 Graphs analysis

At this point, some interesting findings from the correlation heatmap, along with their explanations, will be presented. The reliability of those findings are given through the accuracy of the functions of textstat library. We assume that the findings are based on specific policies that do not meet the user-friendly model presented above. To compare with this concept, many policies must be created in a user-friendly format, and the analysis must be repeated.

Time and Dale Chall

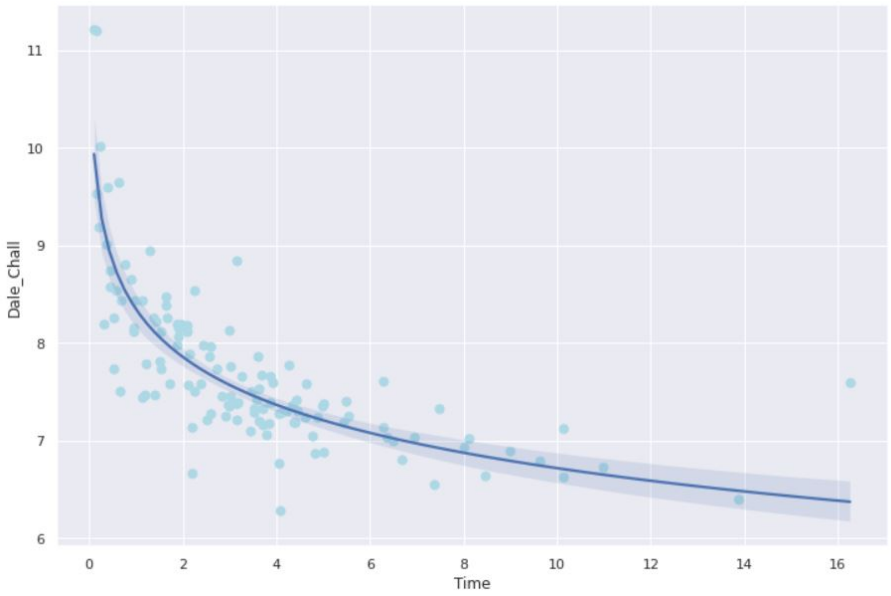


Figure 5.3: Time/ DaleChall

The comprehension rate based on the Dale Chall formula, which assesses the degree of difficulty people face when reading policies, is proportional to time, as shown in the graph presented in Figure 5.3. The higher the percentage, the more difficult it is to interpret the text. We find that the longer the time period, the more understandable the privacy policy is. However, in our case, this is not desirable, because one of the goals for a user-friendly policy is that it needs to be understood quickly.

Line count and Dale Chall

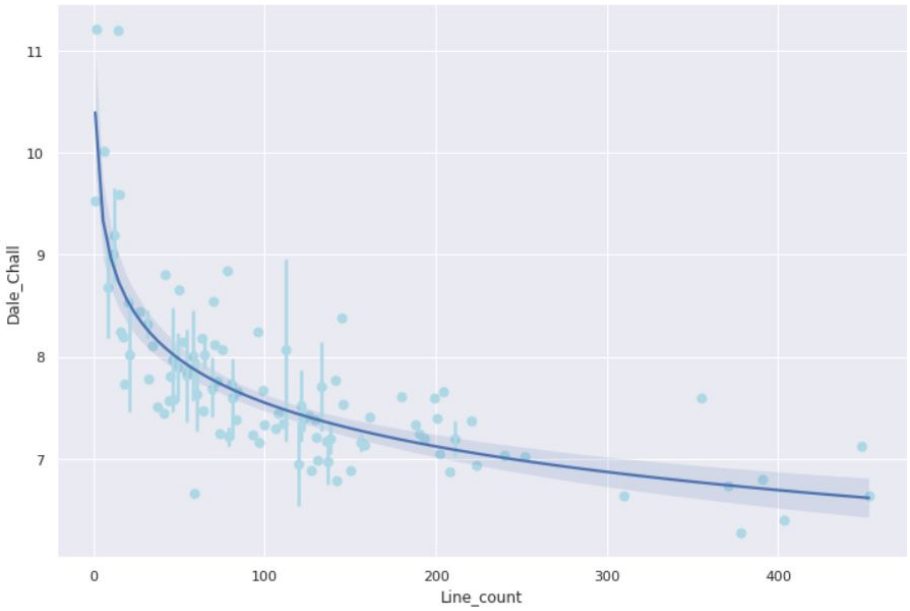


Figure 5.4: Line Count / DaleChall

Dale Chall's graph with the number of lines shows that as the number of lines increases, so decreases the difficulty of understanding. This is strange and calls into question the goal of simplifying a privacy policy, as the graph shows that more lines are needed to make the policy more understandable but the challenge is to avoid the overloaded information.

Flesch and time

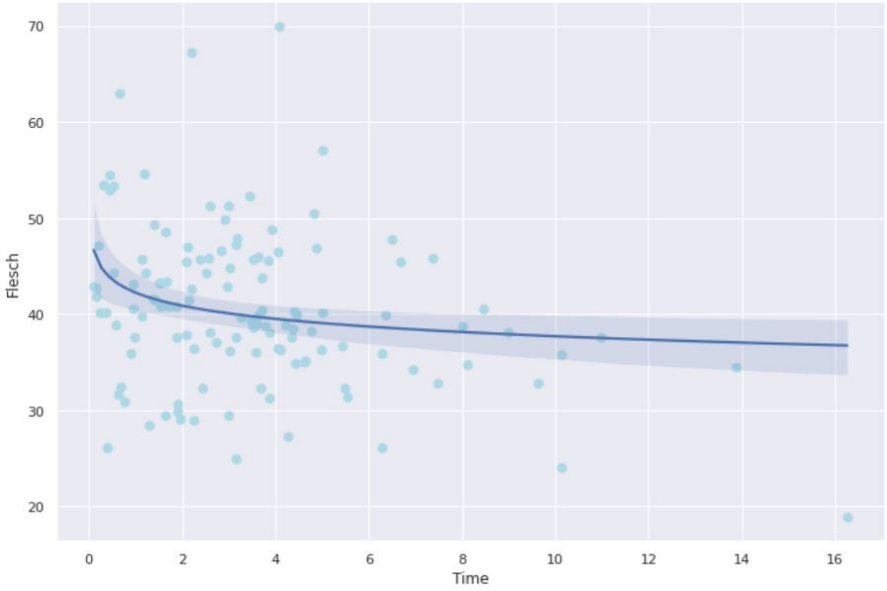


Figure 5.5: Time / Flesch

The flesch type provides a readability grade as well. A score of 100 indicates that the text is very readable, while a score of 0 indicates that it is extremely difficult to read. The graph shows that regardless of how much time that someone spends reading each policy, the score remains nearly constant around 35-40. This number suggests that the words are unreadable and better understood by college graduates, demonstrating the intricacy of language and policy proposals.

The preceding leads us to the following conclusions:

1. In their current form, privacy policies must take a long time to read in order to be comprehended. That is not what we desire. We want policies to be basic and easy to grasp.

2. Furthermore, policies with many lines are more comprehensible. However, this raises an issue because the challenge is to remove information from the policies to make them more user-friendly.

3. According to Flesch's statistic, privacy policies contain a percentage of difficult jargon. This demonstrates that policies do not get more understandable with time due to the difficult terms that they are contain.

5.3 Logistic regression for comprehensive privacy policies

Using the metrics discussed above, those that emerged from the 125 policy analysis, we produced a new dataset, and based on this dataset, we developed a logistic regression model to determine whether a policy is comprehensible or not. Logistic Regression is an algorithm that can be used to predict the likelihood of a specific class or event. When the data is linearly separable and the outcome is binary, it is used. Thus, in our case, the model determines whether a policy is comprehensible (1) or not (0). This is determined by the "comprehended" metric, which is a combination of several other metrics in the dataset. The goal is to build a prediction model that is both accurate and trustworthy in determining how different measures, as discussed above, impact the comprehend of privacy policies. The goal of the model is to be as accurate as feasible while minimizing any inaccurate predictions.

Dataset

The dataset comprises the metrics specified in the preceding section, as well as additional variable named comprehend, which receives values of 0 or 1. The zero value means that the policy is not comprehensible while the value 1 means that it is. To get this number, we used a mix of the aforementioned criteria and the knowledge gained during the thesis study.

	Policy	Flesch	Dale_Chall	Autoread	Mcalpine	Consencus	Time	Line_count	Word_count	Unique_words	Cleaned_word_count	Cleaned_unique_count	Comprehended
0	BBC	31.25	7.66	19.7	42.8	20.0	3.865500	204	2922	630	1701	520	0
1	Harvard Book Store	43.12	8.11	13.9	27.1	13.0	0.964833	34	745	267	428	213	1
2	Wired	40.79	7.58	14.6	30.8	13.0	1.711667	49	1339	403	745	314	1
3	Ebay	32.26	7.40	19.6	41.5	16.0	5.492333	201	4183	836	2325	680	0
4	YouTube	30.91	8.80	16.7	32.0	15.0	0.768500	42	571	248	337	186	0
...	...	...	...	...	...	...	...	...	...	...	...	...	...
120	wnep	36.02	7.42	17.2	37.1	15.0	3.571167	126	2758	636	1474	505	0
121	wsmsn	36.12	7.76	17.3	37.1	14.0	3.010500	72	2337	599	1268	473	0
122	yahoo	40.79	7.97	15.4	29.0	13.0	1.880000	81	1406	447	805	358	1
123	yard	36.32	7.29	17.0	36.6	15.0	4.118833	60	3198	679	1802	557	0
124	zacks	49.35	7.47	14.7	29.4	12.0	1.400167	21	1110	313	638	237	1

Figure 5.6: Screenshot of the dataset

Procedure

1. Pre-processing : Logistic regression can handle categorical data as well as large data sets. In the first phase, we separated the data into a test data set and a train data set (30% to 70%). Furthermore, the dataset was checked for duplicates and missing values. The ratio of policies being comprehended compared to not being is 48.28% to 51.72%. Then we used stratify in order to have test subsets that have the same proportions of class labels as the input dataset. Stratify in this context means that

the train / test split returns training and test subsets with the same proportions of class labels as the input dataset.

2. Creating the pipeline : The next step it was the creation of the pipeline object. The pipeline enables the combination of several operations into a single estimator. Like any other estimator, the pipeline class contains fit, predict, and score methods. We used StandardScaler to achieve scaling, which subtracts the mean from each feature and then scales to unit variance.

3. Run logistic regression model: Step three was to run a logistic regression model on the final data set.

4. Creating confusion matrix:

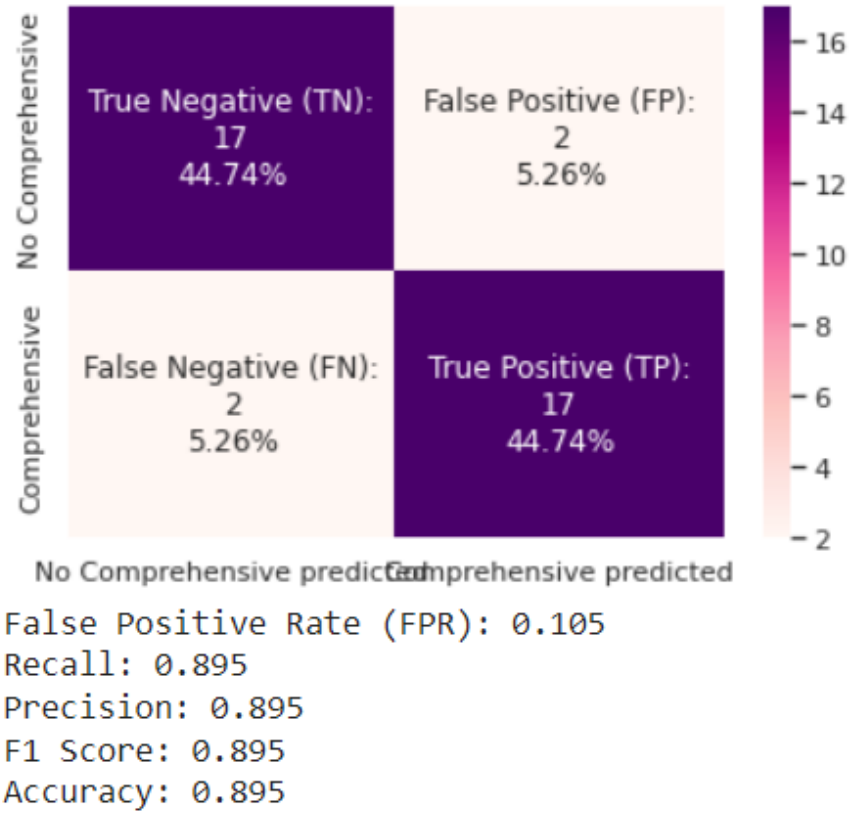


Figure 5.7: Confusion Matrix

The confusion matrix shows how the error splits in the different types. A confusion matrix is a tabular breakdown of a classifier's accurate and incorrect predictions. It is used to assess the effectiveness of a categorization model. It may be used to assess the performance of a classification model by computing performance measures such as accuracy, precision, recall, and F1-score.

TN - correct prediction of no comprehensible

FP - model predicts comprehensible but the policy is not

FN - model predicts no comprehensive but the policy is comprehensible

TP - correct prediction of comprehensible policy

5. Discussion of confusion matrix:
   The model is a logistic regression model, using balanced classes in order to account for the ratio of the response variable. The plot above shows the confusion matrix which is used to evaluate the performance of the classification. The precision measure shows the proportion of policies that were correctly predicted as comprehended to the total policies predicted to not be comprehended. Here the ratio is 0.895 , meaning that about most of the policies predicted to be comprehended were indeed comprehended. The predictions of most of the policies that were indeed comprehended correctly and the predictions of no comprehend that were comprehended, are few.

6. Feature Influence

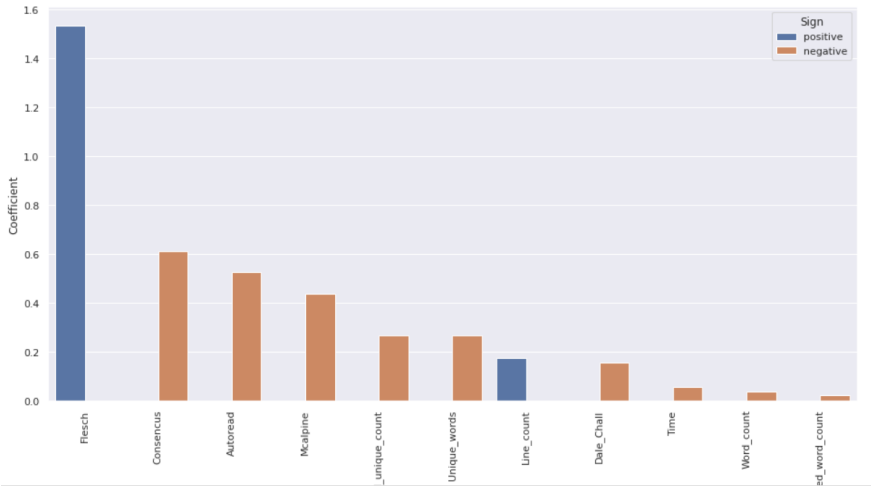


Figure 5.8: Feature Influence

The plot presented in Figure 5.8, shows the influence of the features on a policy being either comprehended or not comprehended. The graph specifically looks at the most influential coefficients and whether they are affecting a policy's comprehension positively or negatively. The blue bar plots show features less likely to lead to a policy being comprehended, whilst the orange bar plots show features that are more likely to lead to a policy not being comprehended. The blue bar plot show features that as they increase is it more likely to predicted comprehended policies.

7. Conclusions:

   As we previously stated, the analysis and results we obtained are based on the collected policies which are currently in plain text format, so we cannot obtain results based on the model for our policies in their user-friendly format. To accomplish this, the model must be retrained. As the results indicate for now, the policies have comprehensibility and readability issues, which should be investigated further.

Chapter 6

Evaluation

6.1 Introduction

At the completion of the implementation of all system functions, it was determined that correctness should be examined and tested. Furthermore, because we were particularly interested in the system's control and assessment in terms of effectiveness, we separated the evaluation into three parts. We initially reviewed the system based on usability and design rules, then we utilized the cognitive-walk-through approach on a group of 10 individuals, to whom we then administered a questionnaire to evaluate the system, and finally we examined the data we were given.

6.2 Defining design and usability rules

One of the goals set throughout the design of the system was to make the platform, especially the interfaces, easy to understand and easy for all users to learn. In order to achieve this, when designing the system we set down some usability goals described in Section 4.2.8. The following are the design and usability guidelines that were created and applied on the platform. For this evaluation, we used Nielsen's heuristic evaluation approach using Nielsen's 10 rules [41].

1. Visibility of system status : Users when using the system have the opportunity to be informed about the functions of the system with an understandable and visible state that appears on the screen within a reasonable time.In the event of a failed result, an useful feedback message is provided at the end of most functions, as seen in Figure 6.1.

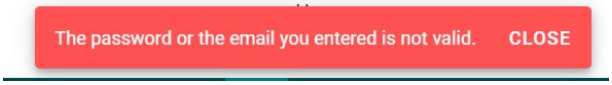


Figure 6.1: Informative feedback message

Furthermore, because we wanted to provide the user sufficient feedback about the functions, there is a bar at the point of the generator that informs user when a step is done. The bar can be seen in the Figure 6.2

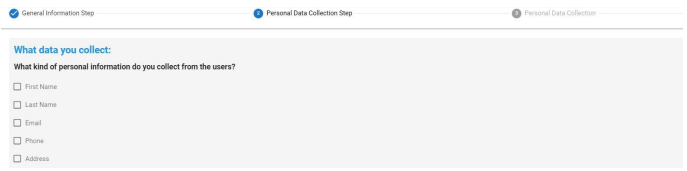


Figure 6.2: Informative feedback bar

2. Match between system and the real world. : In general, we attempted to align the system's language and concepts with the user's actual world. To accomplish this, we used a lot of symbols as metaphors throughout the system, so that users' expectations are formed from their real-world experiences. Each symbol represents a real-world concept. For example, in the policy edit page, the user can remove the policy by selecting the bin icon; the user understands the semantics of the operation without much effort.

3. Control and user freedom: Users can navigate backwards in the system, including undoing and redoing past activities. Figure 6.3 depicts such a feature, here, the user validates whether he/she truly wishes to delete the account or return to the screen.

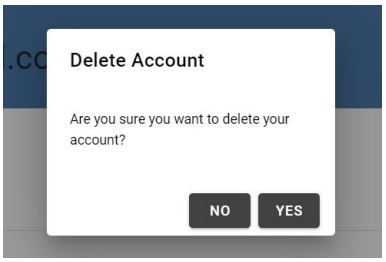


Figure 6.3: Delete account

4. Consistency and standards: In the design, we attempted to keep both the graphic components and the terminology consistent across comparable interfaces. For example, the appearance of the Sign In page is quite similar to that of the Sign Up page; in this way, we ensure that the user's mental model remains consistent and is not confused. In addition, we endeavored to have each interface use the same font and colours.

5. Error prevention: The design was done in such a way that potential mistakes were minimized . What we have tried is to create error messages that are informative and use basic language to convey the issues. In order to prevent disinformation, we also provided the user with some list-style options in order to avoid having to handle to many information.

6. Recognition rather than recall: We considered it critical to reduce cognitive load by keeping work information on the screen as users explored the UI. All of the features are self-explanatory for the user, and to further assist him/her, we added the tutorial option,

which is accessible from all screens at the toolbar.
7. Flexibility and efficiency of use: As illustrated in the figures below, the system adjusts to different browsers and screen sizes. Furthermore, the platform is available via a Firebase hyperlink from any device connected to the network.

8. Aesthetic and minimalist design: We attempted to make the system as abstract as possible, giving the user simply the functions that needed without requiring too much knowledge and detail. Furthermore, we attempted to provide users with a user-friendly and intelligible system design that is also useful.

9/10. Help users recognize, diagnose and recover from errors / Help documentation: Mistakes and errors were avoided mainly to the feedback messages indicated above and the assistance offered by the tutorial option.

6.3 Cognitive walk-through

We examined the system's usability and operation using the cognitive walk-through approach. It is based on tasks that involved an inter-operable group of potential users walking through each step of a workflow while answered a set of predefined questions to identify aspects of the interface that may be difficult for new users as well as aspects where the system could be improved.

Tasks defined:

Number	Task
1	Sign up to the system
2	Check authentication in the email
3	Sign in to the system
4	Try forgot password
5	Check email for forgot password
6	Create a policy
7	Delete a policy
8	Create a new policy
9	Edit the policy
10	Create Template
11	See account details
12	Change password
13	Log out

The cognitive walk-through was primarily completed with the assistance of some colleagues and friends. The procedure included describing the system to them, trying the activities outlined above, and completing a questionnaire following their experience with the system. We was observing their reactions following decisions during their mobility and contact with the system, and we noticed when they might experience problems.

Conclusions:
Overall, the approach produced promising outcomes. However, based on the data, we were able to identify several of the system's flaws that we could address. These flaws were as follows:

1. More information needed to the part of the generator.
2. At the generator part, some buttons were difficult to be used.
3. The print button is unnecessary.

Those suggestions were taken into account and reviewed :

1. In order to be able to provide additional information, we added additional questions to the generator point, so that the information needed by the user can be better understood.

2. Indeed, at the point of the generator there was an issue with the selection of the check-box. Specifically, it took 2 clicks to press an option, which was not immediately understood by the user. The user had a hard time pressing it to a point where he was angry at the many options. Therefore we modified the choice to reflect what the users requested.

3. The print button does not perform as planned, in that margins are altered, however its function can be enhanced.

6.4 Evaluation questionnaire results

The evaluation questionnaire and the results can be found at the appendix. The following are the general questionnaire results:

- Users received an account confirmation message, although it is limited and takes time for non-Google accounts.

- The various criteria provided to users for evaluation, such as system aesthetic and information accuracy, were mostly rated as very good or perfect by the users.

- The majority of users reported that the system did not require any upgrades and that navigating through the sites was simple. There was one user, that stated that the system was very complicated but we considered that this user did not understand the question, because then at the next question he/she stated that it was very easy.
- The system is relatively straightforward to learn, according to the majority of users (60 percent), with a rating of 4 out of 5.
- The majority of users (70 percent) rated the system's usability as 5 out of 5.
- All the uses selected that they were free of choices, meaning that they had the freedom to choose whether they want to disagree, cancel and continue when they wanted to while using the system.
- The system was judged to be useful by all users.

6.5 Limitations of the system

The system's most serious limitation is the amount of concurrent users it can support. This is limited by the Firebase's database and can be enlarged by purchasing a new package. Another minor restriction for the time is that the system cannot give the user extra options for modifying the policy that appears. Furthermore due to a minimal change at the framework, a package is not supported anymore so the download option is available but does not produce the output that we wanted to.

Chapter 7

Conclusion

7.1 Thesis review

The thesis's goal was to improve the way a privacy policy is presented to the ordinary user. We consider this goal to have been met to a significant part by the end of the thesis because it took a long time to figure out how to accomplish it and we developed a system with fully implemented functionalities and the platform can be utilized without any programming problems. The platform that was designed is simple to use and modernized with new technology seen in similar applications, and it responds to user requests pretty quickly. During the system's implementation, we followed good programming practices that we learned in the courses EPL343 - Software Technology , EPL425 - Internet technologies, as well as the course EPL435 - Human Computer Interaction, which contributed to the development of an easy-to-use system with good design principles and proper screen layout.

We cannot deny that the thesis was a huge part of the last year at the university, during which we spent time first understanding what was going on, then coming to the topic and learning the technologies required to get to this point today. To get to this moment, there were several problems and hours of effort. The main challenge, I believe, was completing the template and becoming acquainted with development technologies for the first time.

7.2 Future work

In terms of the system we implemented, it is totally done and ready to use based on the specifications we established. Due to the time constraints for thesis preparation, it was not possible to incorporate extra elements that would make the system even more useful. As a result, the existing system may be upgraded with additional features in the future, providing users with more functionality and flexibility. The key item that

may be added is to further develop the user's ability to modify the policy template and option to adapt policy in a different language. Furthermore, an empirical examination of the system's GDPR compliance can be performed, which can contain an addition of a policy language. Part of the study of different policies can be developed by adding more policies and discovering new metrics. Furthermore, a graphical tool that analyzes the user-friendliness of a policy can be constructed as an add-on. Concerning the policy template established in this thesis, we believe that the research was broad and could not be expanded upon further.

7.3 General Conclusions

I believe I learned a lot of new information as a result of the application of this thesis, which makes me extremely happy. The thesis provided a one-of-a-kind chance for me to learn knowledge and problem-solving skills. After finishing my thesis, I believe I am a more complete programmer, as well as having implemented a reasonably substantial project that has teach me a lot.

A big period of our lives, our undergraduate years, come to a conclusion, with greater knowledge and power for our future.

Bibliography

[1] W3C Web Accessibility Initiative (WAI). *Web Accessibility Initiative*. URL: https://www.w3.org/WAI/standards-guidelines/wcag/ (visited on 11/12/2021).

[2] Andrej and Bluesky. *Privacy policy generator*. Mar. 2021. URL: https://www.termsfeed.com/privacy-policy-generator/.

[3] *California Consumer Privacy Act (CCPA)*. Mar. 2022. URL: https://oag.ca.gov/privacy/ccpa.

[4] *CSS: Cascading Style Sheets*. URL: %5Curl%7Bhttps://developer.mozilla.org/en-US/docs/Web/CSS%7D (visited on 03/03/2022).

[5] *Data and Tools*. URL: https://usableprivacy.org/data.

[6] *Data breach*. Sept. 2021. URL: https://www.cyberark.com/what-is/data-breach/.

[7] *Developments on penalties imposed for GDPR violations in 2021*. URL: https://www.harriskyriakides.law/insights/news/developments-on-penalties-imposed-for-gdpr-violations-in-2021#:~:text=What%5C%20are%5C%20the%5C%20GDPR%5C%20fines,financial%5C%20year%5C%2C%5C%20whichever%5C%20is%5C%20higher..

[8] *Eur-Lex-Document-31995L0046*. URL: %5Curl%7Bhttps://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%5C%3A31995L0046&from=EN%7D (visited on 03/02/2022).

[9] *Eur-Lex-Document-Europa*. URL: %5Curl%7Bhttps://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046%7D (visited on 03/02/2022).

[10] *European Convention on human rights*. URL: %5Curl%7Bhttps://www.echr.coe.int/Documents/Convention_ENG.pdf%7D (visited on 04/02/2022).

[11] *Flesch reading ease and the Flesch Kincaid grade level*. July 2021. URL: https://readable.com/readability/flesch-reading-ease-flesch-kincaid-grade-level/.

[12] *GDPR Enforcement Tracker*. URL: https://www.enforcementtracker.com/ (visited on 04/04/2022).

[13] *GDPR summary: Overview of 10 key requirements*. Oct. 2020. URL: %5Curl%7Bhttps://advisera.com/eugdpracademy/knowledgebase/a-summary-of-10-key-gdpr-requirements/%7D (visited on 04/02/2022).

[14] *Google Firebase*. https://firebase.google.com/. (Visited on 03/03/2022).

[15] *How GDPR changed the world, and Privacy Regulation's future*. Dec. 2021. URL: https://kfp.kaspersky.com/news/how-gdpr-changed-the-world-and-privacy-regulations-future/.

[16] *How to create a Seaborn Correlation heatmap in python?* Nov. 2020. URL: https://www.geeksforgeeks.org/how-to-create-a-seaborn-correlation-heatmap-in-python/.

[17] *HTML Tutorial*. URL: %5Curl%7Bhttps://www.w3schools.com/html/%7D (visited on 03/03/2022).

[18] *Information to be provided where personal data have not been obtained from the data subject - Article 14*. Oct. 2016. URL: https://gdpr-info.eu/art-14-gdpr/ (visited on 02/12/2021).

[19] *ISO 9241-110:2020 - Usability*. URL: https://www.iso.org/obp/ui/#iso:std:iso:9241:-110:ed-2:v1:en (visited on 11/12/2021).

[20] Daniel Serrano Design Lead et al. *Prototyping for all*. URL: https://proto.io/.

[21] *McAlpine EFLAW readability score*. Apr. 2009. URL: https://strainindex.wordpress.com/2009/04/30/mcalpine-eflaw-readability-score/.

[22] Merriam-Webster. *Privacy definition*. URL: %5Curl%7Bhttps://www.merriam-webster.com/dictionary/privacy/%7D (visited on 01/10/2022).

[23] *NLTK python library*. URL: https://www.nltk.org/.

[24] Node.js. *Node.js*. URL: https://nodejs.org/en/about/ (visited on 04/25/2022).

[25] Jonathan A. Obar and Anne Oeldorf-Hirsch. "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services". In: *Information, Communication, Society* 23.1 (2018), pp. 128–147. DOI: 10.1080/1369118x.2018.1486870.

[26] The Premerger Notification Office. *Children's Online Privacy Protection Rule ("coppa")*. Dec. 2020. URL: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

[27] *Pandas*. URL: https://pandas.pydata.org/.

[28] *Principles relating to processing of personal data - Article 5*. Nov. 2018. URL: https://gdpr.eu/article-5-how-to-process-personal-data/ (visited on 02/12/2021).

[29] *Privacy by design*. Oct. 2021. URL: https://gdpr-info.eu/issues/privacy-by-design/ (visited on 01/04/2022).

[30] *Privacypolicies.com*. URL: https://www.privacypolicies.com/privacy-policy-generator/ (visited on 04/25/2022).

[31] Priviness. *Lessons from the Greeks: Privacy in Aristotelian thought*. https://www.priviness.eu/blog/lessons-from-the-greeks-privacy-in-aristotelian-thought. Mar. 2018. (Visited on 01/10/2022).

[32] *Python.org*. URL: %5Curl%7Bhttps://www.python.org/%7D%20urldate=%7B2022-03-03%7D.

[33] Neil Readshaw and Chief Security Officer. *How we apply the 7 principles of privacy by design*. Feb. 2021. URL: https://anonyome.com/2020/05/how-we-apply-the-7-principles-of-privacy-by-design/#:~:text=%5C%20by%5C%20Design%5C%20is%5C%20based%5C%20on%5C%207%5C%20principles&text=Privacy%5C%20as%5C%20the%5C%20default%5C%20setting,end%5C%20security%5C%E2%5C%80%5C%94full%5C%20lifecycle%5C%20protection (visited on 01/04/2022).

[34] Termify. *Customized privacy policies and terms amp; conditions in seconds*. URL: https://termify.io/privacy-policy-generator?.

[35] *Textstat*. URL: https://pypi.org/project/textstat/.

[36] *The new Dale Chall readability formula*. July 2021. URL: https://readable.com/readability/new-dale-chall-readability-formula/.

[37] *Transparent Information, communication and modalities for the exercise of the rights of the data subject - Article 12*. Mar. 2018. URL: https://gdpr-info.eu/art-12-gdpr/ (visited on 02/12/2021).

[38] European Union. *Official Legal Text, General Data Protection Regulation (GDPR)*. Sept. 2019. URL: %5Curl%7Bhttps://gdpr-info.eu/%7D.

[39] AgileTech Vietnam. *Top 6 software development life cycle (SDLC) models amp; methodologies*. July 2020. URL: https://agiletech.medium.com/top-6-software-development-life-cycle-sdlc-models-methodologies-14e421bb4dd1.

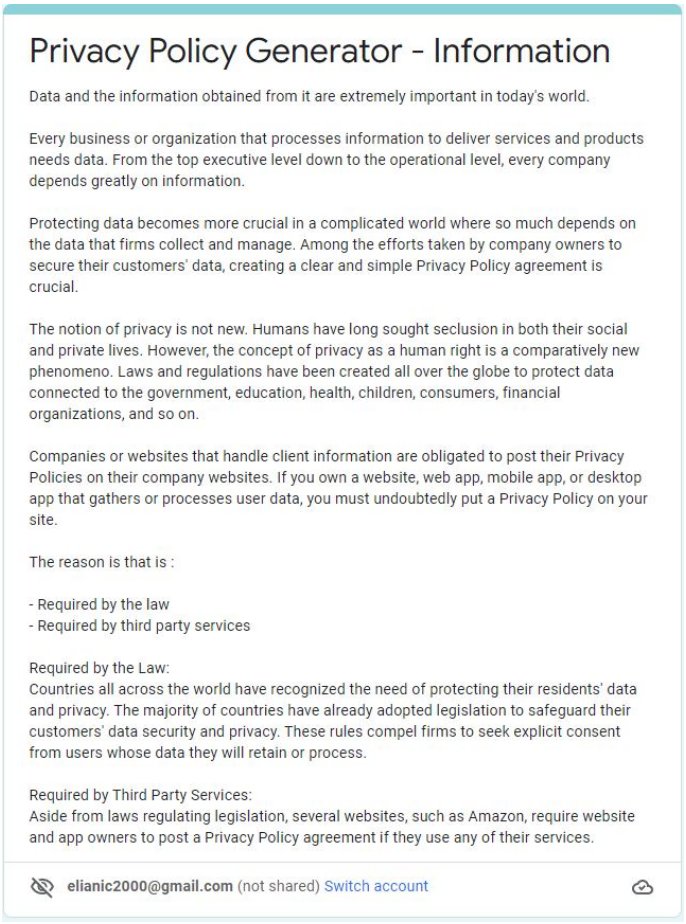
[40] Vue.js. *The Progressive JavaScript Framework*. URL: %5Curl%7Bhttps://vuejs.org/%7D (visited on 03/03/2022).

[41] Euphemia Wong. *User interface design guidelines: 10 rules of thumb*. URL: https://www.interaction-design.org/literature/article/user-interface-design-guidelines-10-rules-of-thumb.

[42] *Writing a GDPR-compliant privacy notice (template included)*. Feb. 2019. URL: https://gdpr.eu/privacy-notice/ (visited on 04/15/2021).

Appendices

Questionnaire



Privacy Policy Generator - Information

Data and the information obtained from it are extremely important in today's world.

Every business or organization that processes information to deliver services and products needs data. From the top executive level down to the operational level, every company depends greatly on information.

Protecting data becomes more crucial in a complicated world where so much depends on the data that firms collect and manage. Among the efforts taken by company owners to secure their customers' data, creating a clear and simple Privacy Policy agreement is crucial.

The notion of privacy is not new. Humans have long sought seclusion in both their social and private lives. However, the concept of privacy as a human right is a comparatively new phenomeno. Laws and regulations have been created all over the globe to protect data connected to the government, education, health, children, consumers, financial organizations, and so on.

Companies or websites that handle client information are obligated to post their Privacy Policies on their company websites. If you own a website, web app, mobile app, or desktop app that gathers or processes user data, you must undoubtedly put a Privacy Policy on your site.

The reason is that is :

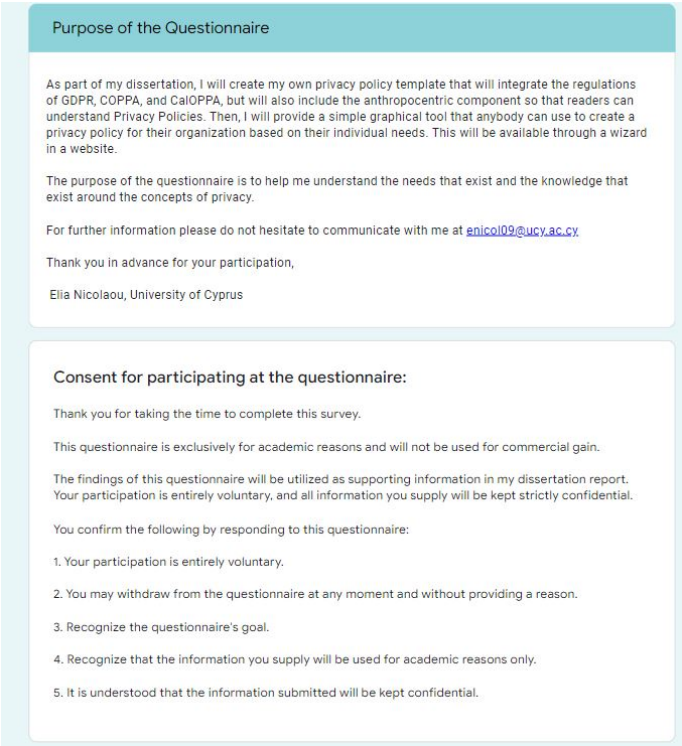
- Required by the law
- Required by third party services

Required by the Law:
Countries all across the world have recognized the need of protecting their residents' data and privacy. The majority of countries have already adopted legislation to safeguard their customers' data security and privacy. These rules compel firms to seek explicit consent from users whose data they will retain or process.

Required by Third Party Services:
Aside from laws regulating legislation, several websites, such as Amazon, require website and app owners to post a Privacy Policy agreement if they use any of their services.

elianic2000@gmail.com (not shared) Switch account

Questionnaire Information



Purpose of the Questionnaire

As part of my dissertation, I will create my own privacy policy template that will integrate the regulations of GDPR, COPPA, and CalOPPA, but will also include the anthropocentric component so that readers can understand Privacy Policies. Then, I will provide a simple graphical tool that anybody can use to create a privacy policy for their organization based on their individual needs. This will be available through a wizard in a website.

The purpose of the questionnaire is to help me understand the needs that exist and the knowledge that exist around the concepts of privacy.

For further information please do not hesitate to communicate with me at enicol09@ucy.ac.cy

Thank you in advance for your participation,

Elia Nicolaou, University of Cyprus

Consent for participating at the questionnaire:

Thank you for taking the time to complete this survey.

This questionnaire is exclusively for academic reasons and will not be used for commercial gain.

The findings of this questionnaire will be utilized as supporting information in my dissertation report. Your participation is entirely voluntary, and all information you supply will be kept strictly confidential.

You confirm the following by responding to this questionnaire:

1. Your participation is entirely voluntary.

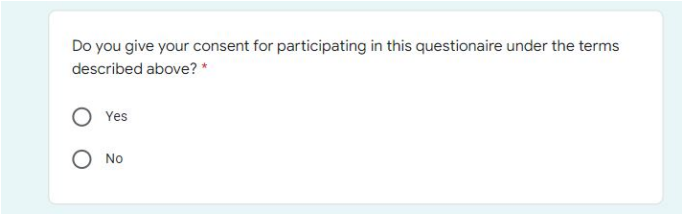
2. You may withdraw from the questionnaire at any moment and without providing a reason.

3. Recognize the questionnaire's goal.

4. Recognize that the information you supply will be used for academic reasons only.

5. It is understood that the information submitted will be kept confidential.

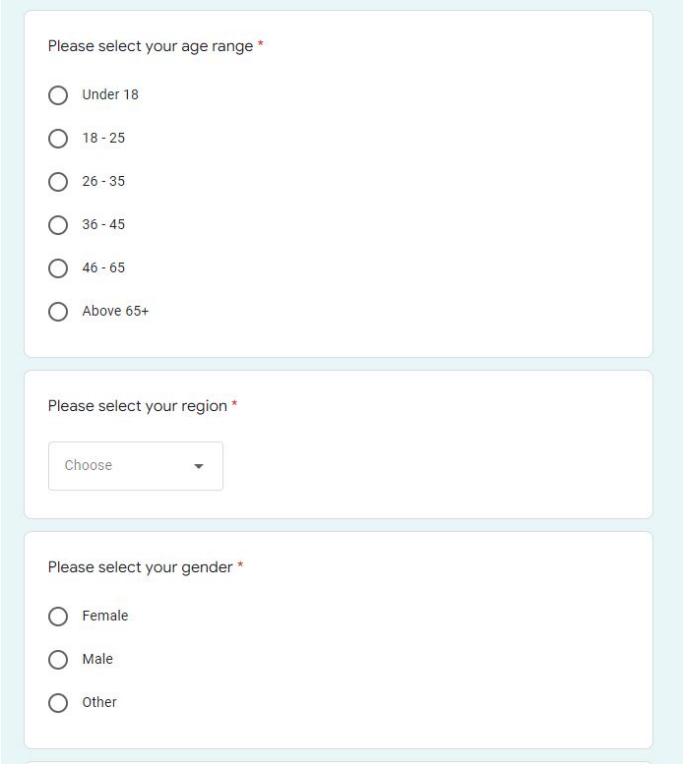
Questionnaire questions



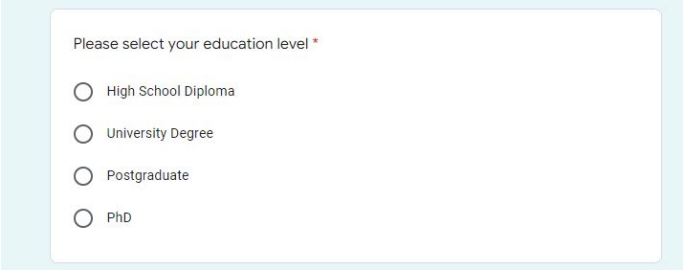
Do you give your consent for participating in this questionaire under the terms described above? *

- ◯ Yes
- ◯ No

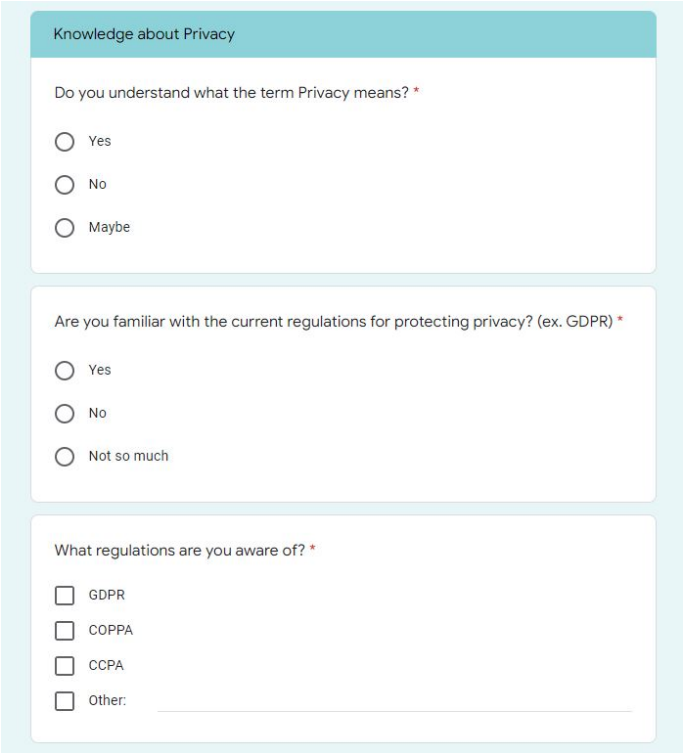
Questionnaire questions



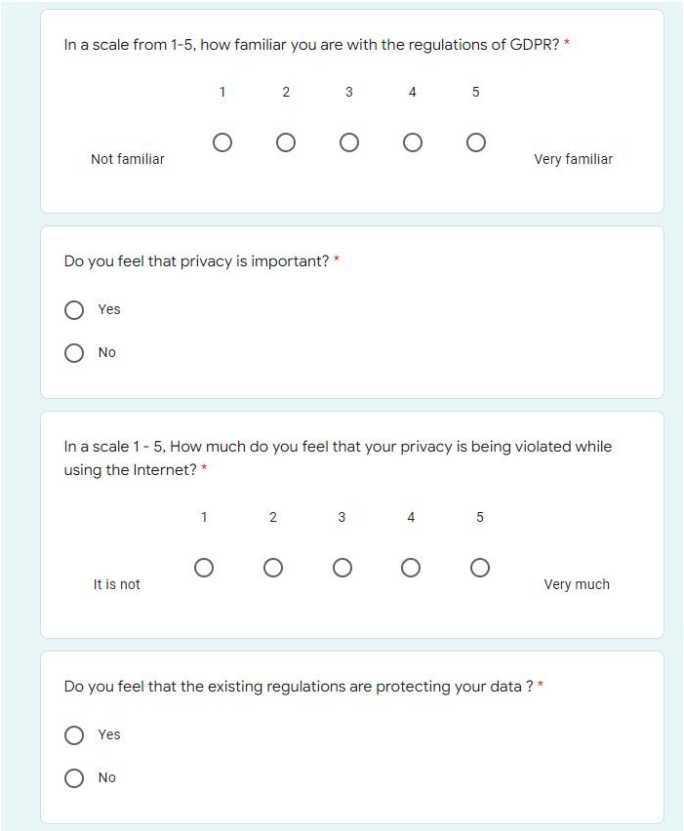
Questionnaire questions



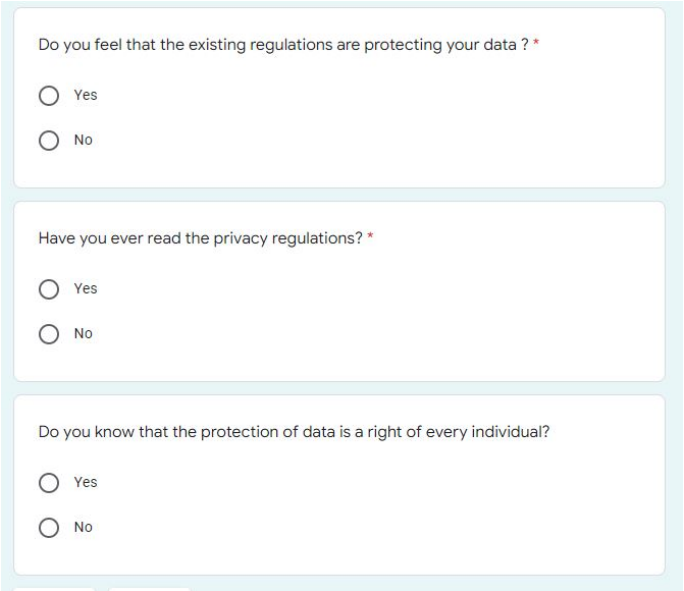
Questionnaire questions



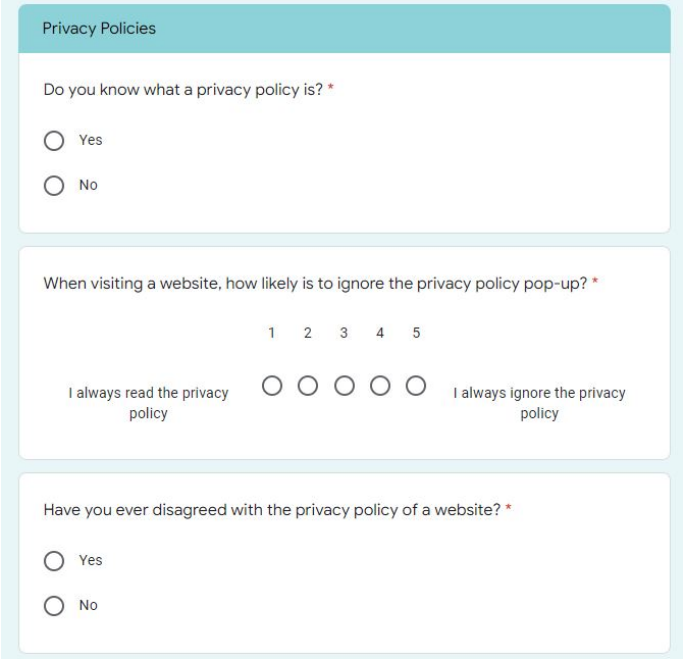
Questionnaire questions



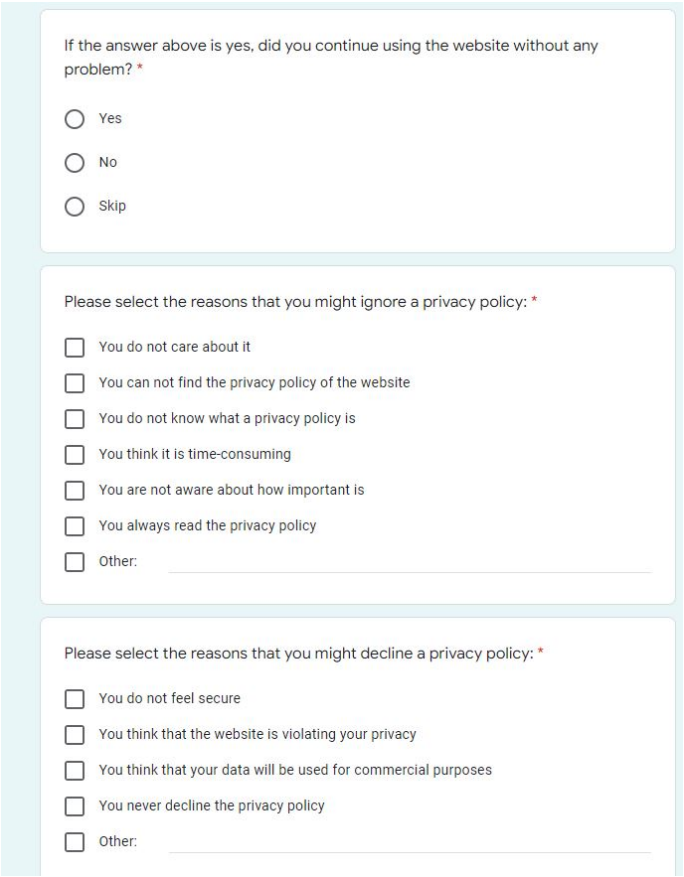
Questionnaire questions



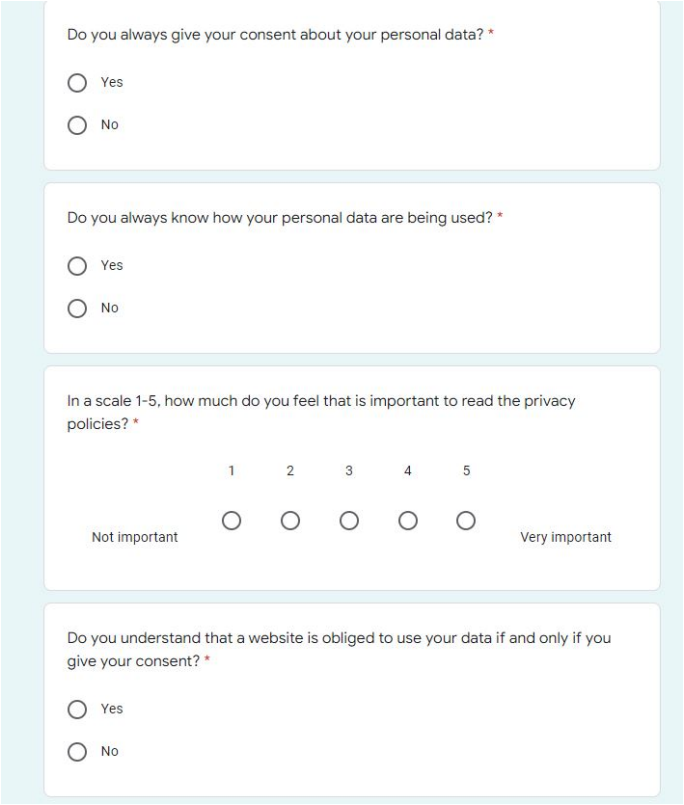
Questionnaire questions



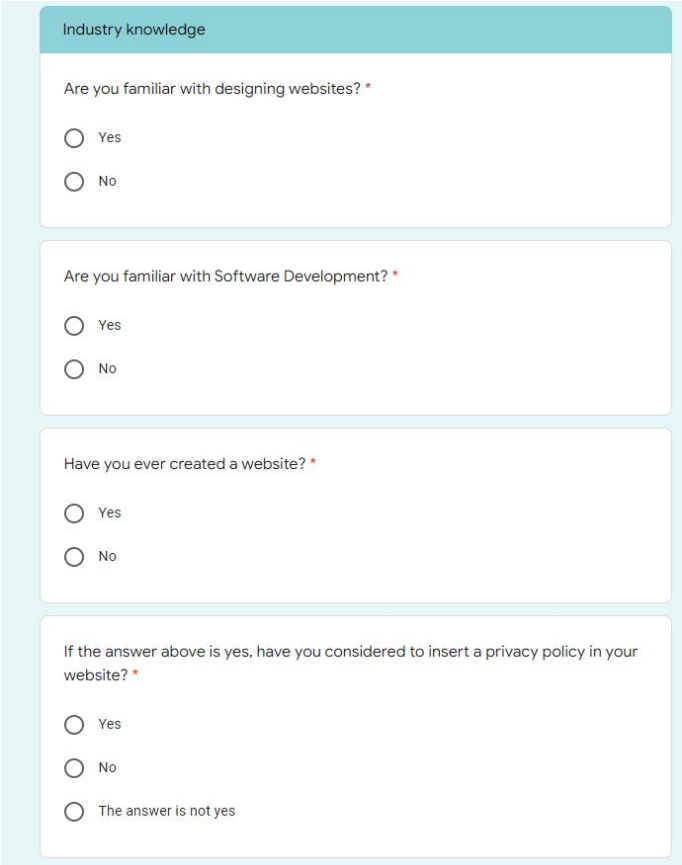
Questionnaire questions



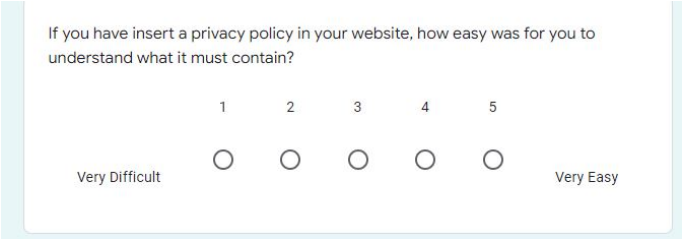
Questionnaire questions



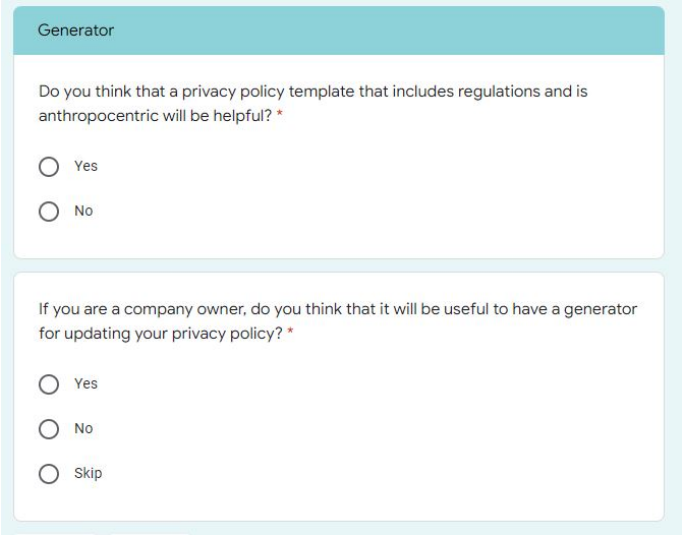
Questionnaire questions



Questionnaire questions

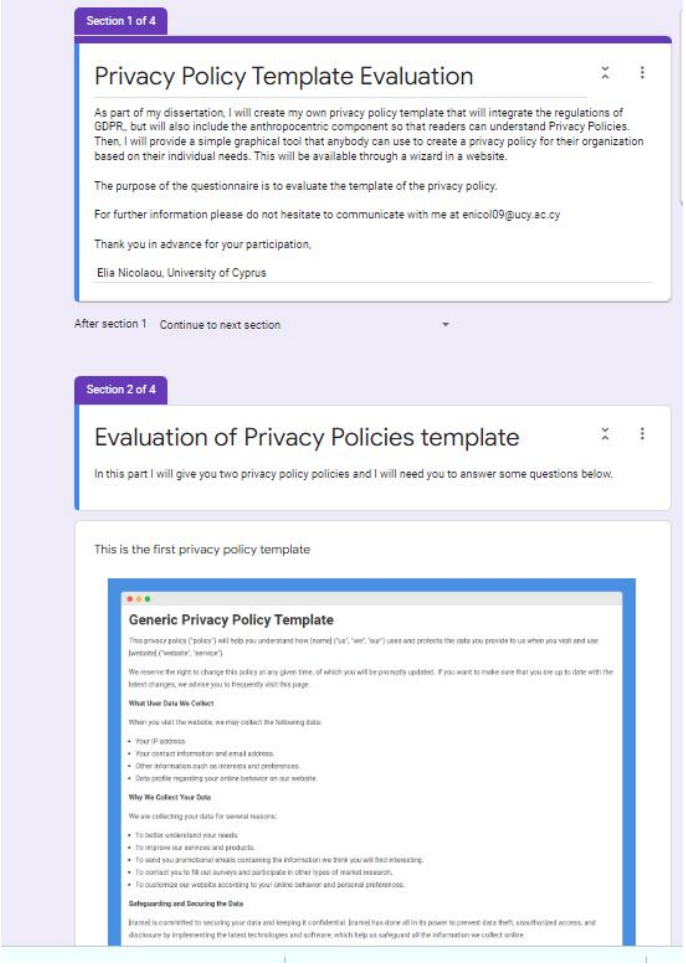


Questionnaire questions

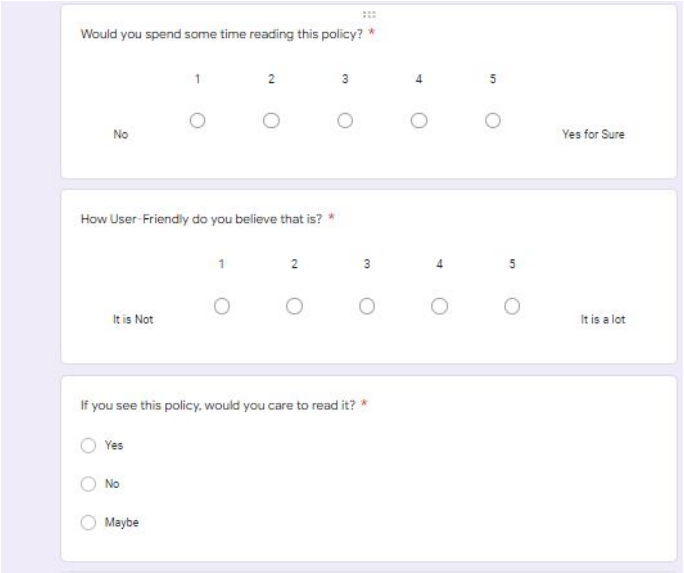


Questionnaire questions

Template evaluation questionnaire

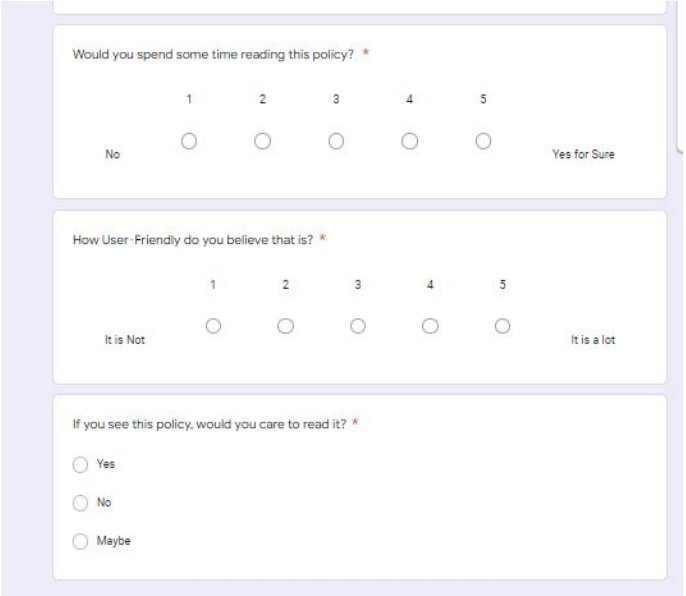


Questionnaire-Template Evaluation questions

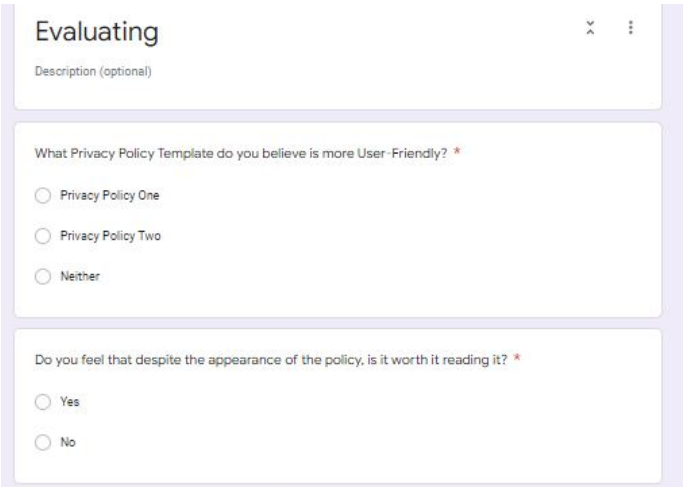


Questionnaire-Template Evaluation questions

Questionnaire-Template Evaluation questions



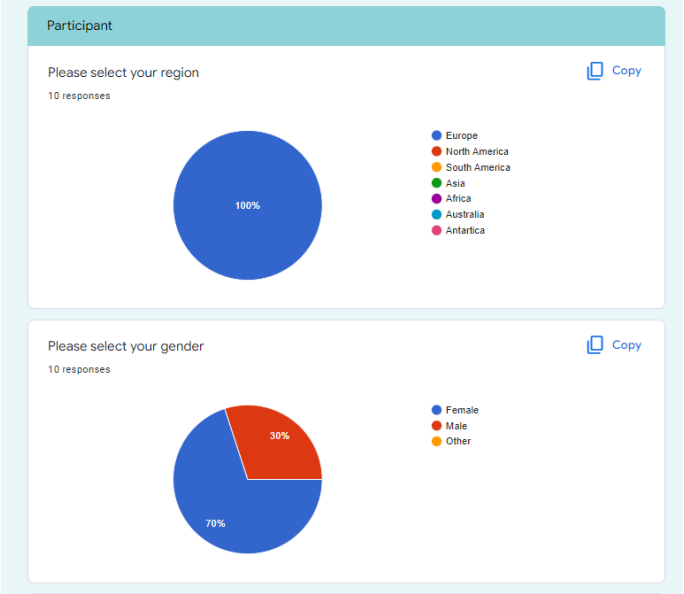
Questionnaire-Template Evaluation questions



Questionnaire-Template Evaluation questions

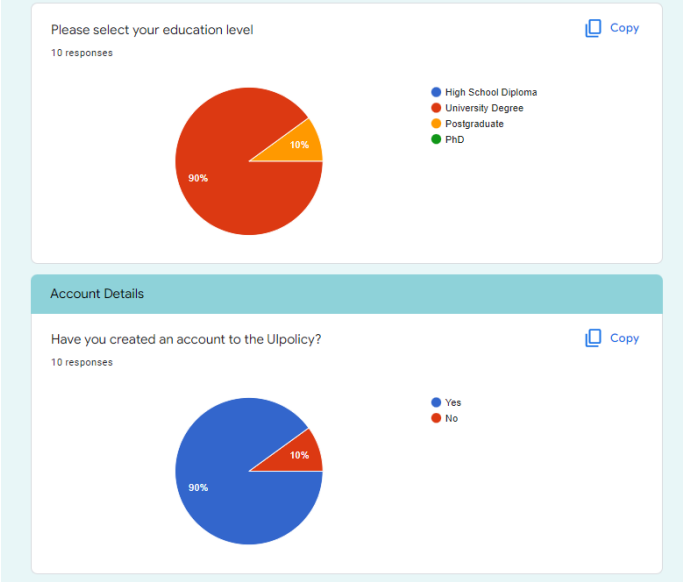
Evaluation questionnaire

Questionnaire- Evaluation answers

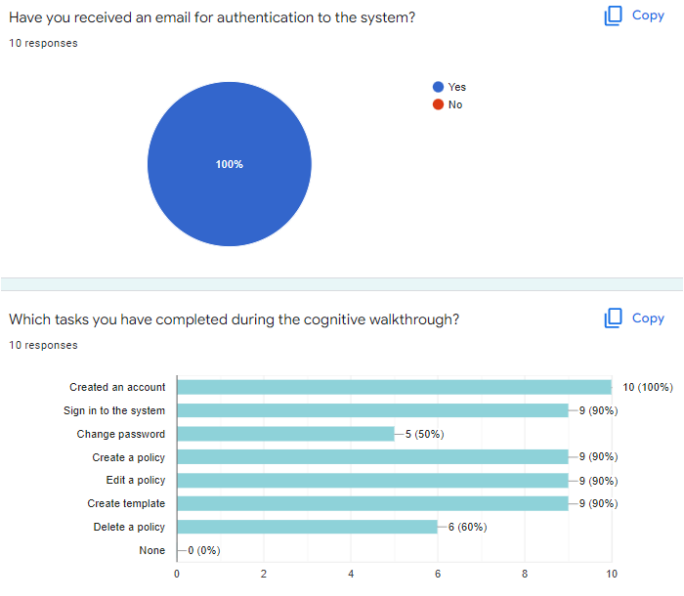


Questionnaire- Evaluation answers

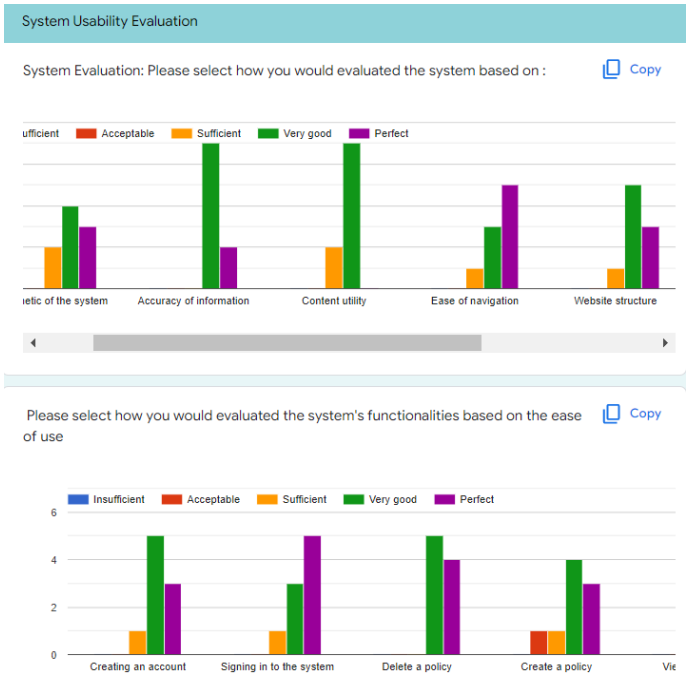
]



Questionnaire- Evaluation answers

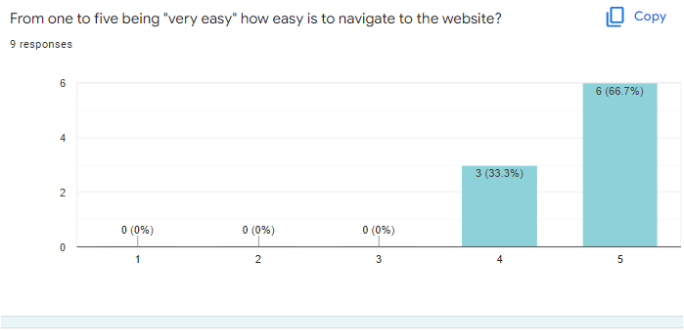


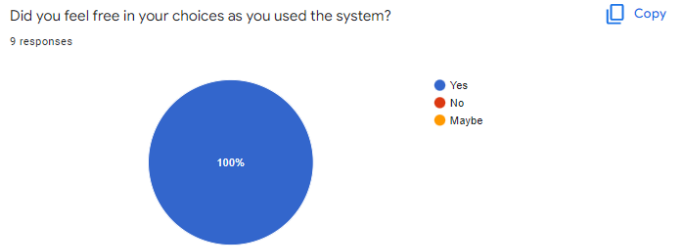
Questionnaire- Evaluation answers



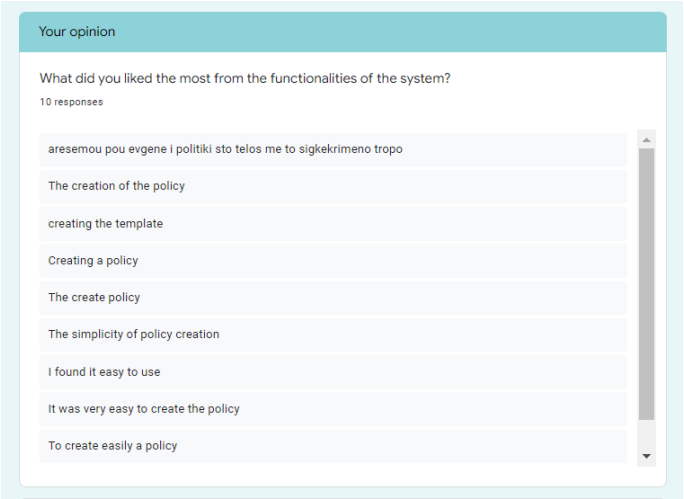
Questionnaire- Evaluation answers

Questionnaire- Evaluation answers

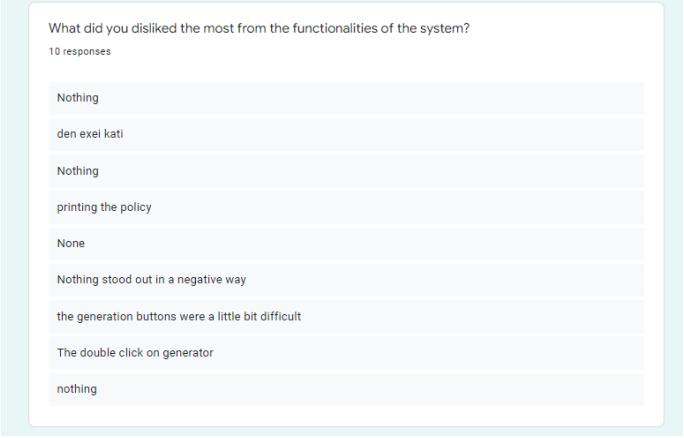




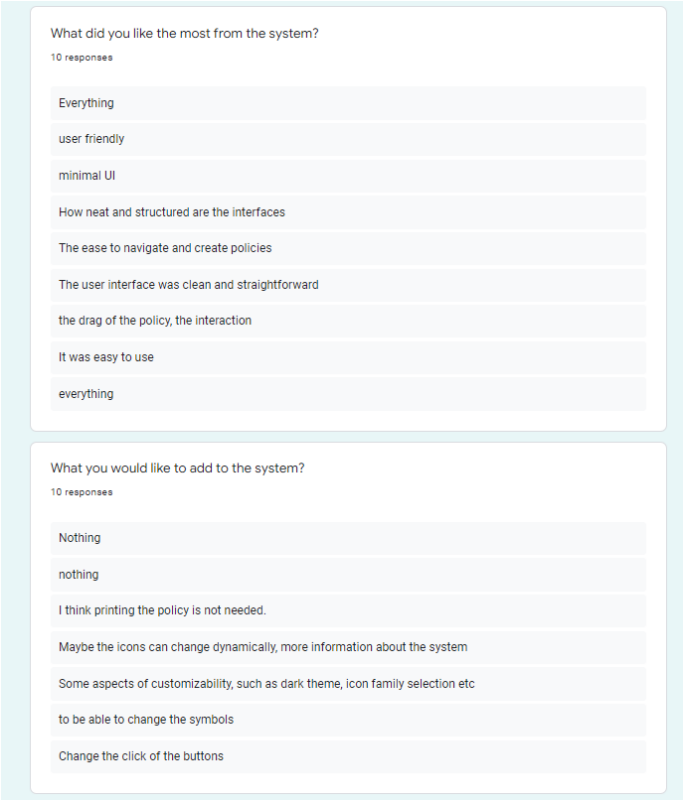
Questionnaire- Evaluation answers



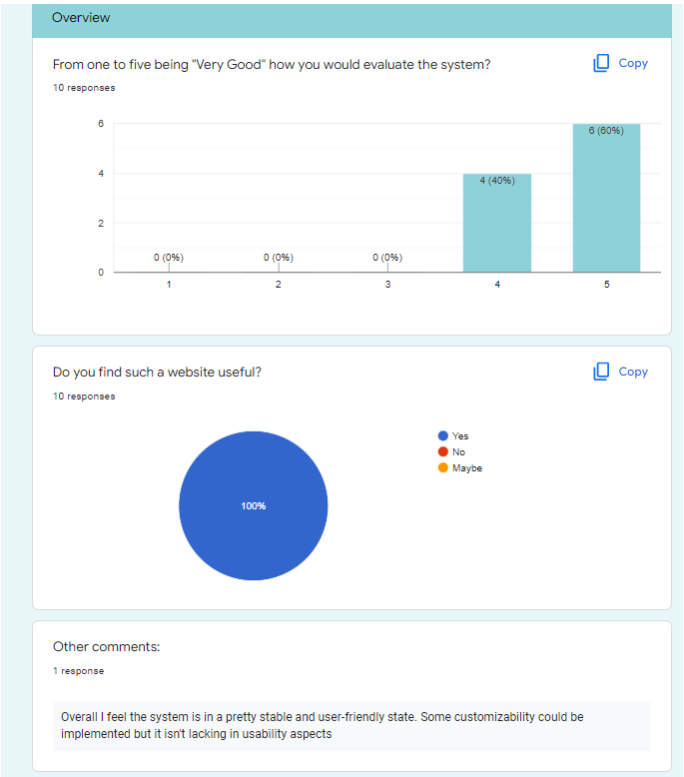
Questionnaire- Evaluation answers



Questionnaire- Evaluation answers



Questionnaire- Evaluation answers



Questionnaire- Evaluation answers