Dissertation

“MAKING DATA COLLECTION TRANSPARENT, USABLE & GDPR-COMPLIANT: ANNOTATING WEB FORMS WITH PROCESSING PURPOSES”

Anna Vasiliou

UNIVERSITY OF CYPRUS

DEPARTMENT OF COMPUTER SCIENCE

May 2025

UNIVERSITY OF CYPRUS

DEPARTMENT OF COMPUTER SCIENCE

MAKING DATA COLLECTION TRANSPARENT: A TOOL FOR ANNOTATING PRIVACY PURPOSES IN WEB FORMS

Anna Vasiliou

Supervisors
Dr. George Papadopoulos

Co-supervisor
Evangelia Vanezi

The Individual Diploma Thesis was submitted towards partially meeting the requirements for obtaining the degree of Computer Science of the Department of Computer Science of the University of Cyprus

May 2025

Acknowledgements

This thesis would not have been possible without the valuable support, guidance, and encouragement I received along the way.

First, I would like to sincerely thank my Supervisor, Dr. Giorgos Papadopoulos, who trusted me and gave me the opportunity to work on this topic. I would also like to express my heartfelt gratitude to my Co-Supervisor and Researcher, Evangelia Vanezi, for her support and excellent collaboration during the preparation of this thesis. Their advice and guidance greatly helped me achieve my goals successfully.

Finally, I wish to thank my family, as well as my friends and colleagues, for their constant psychological support and love.

Abstract

This thesis addresses the challenge of making data collection practices more transparent and usable for users interacting with web forms. Although privacy policies transparency and clarity is required by laws like the GDPR, they are often too long or complex for users to read, leaving many unaware of how their personal data will be used. To help solve this problem, this research explores ways to display privacy information directly at the point of data entry.

The study begins with a large-scale analysis of how websites across five major domains communicate the purposes of their form fields collecting personal data. The findings reveal that most websites fail to provide field-level explanations. To respond to this gap, a user-centered design process was followed to test different annotation styles, and a structured database was created with short, clear purpose descriptions for common input fields. This database was validated through expert feedback, i.e., legal experts and web developers.

A browser-based tool was then developed to allow web developers to apply these annotations easily to HTML forms, in their under development or already existing websites. The tool works fully on the client side, supports two annotation styles (short descriptions and info icons), and allows real-time editing and preview. Finally, a usability evaluation with 40 participants showed that the tool is efficient, easy to use, and positively received.

Overall, this thesis offers a practical solution that supports privacy transparency and usability in a way that is both legally sound and user-friendly, combining insights from law, design, and web development.

Table of Contents

Chapter 1

1. Introduction

1.1 General Idea

The main goal of this thesis is to make it easier for users to understand how their personal data is collected and used when they fill out web forms. Privacy policies are supposed to explain this, but they are often long, complicated, and not read by users. To address this, the thesis explores how to present privacy information directly within the form, next to the fields where users enter their data. This approach aims to provide clear and immediate explanations about why certain information is requested.

The research includes an analysis of existing websites to see how they currently communicate data collection purposes. This helped identify common problems, such as missing or unclear explanations about how user data will be used.

It also involves designing and testing different ways to display this privacy information, i.e., the processing purposes for collected personal data, such as short texts or icons, to find out which methods users prefer and understand best. A survey was used to collect feedback, and the results were used to guide the design of simple and clear annotation styles.

In addition, a database was created that links common form fields (like name, email, or phone number) to suggested privacy-purpose texts. This database was reviewed by both legal and technical experts to ensure the descriptions were accurate and appropriate.

All these efforts come together in a browser-based tool that allows developers and legal experts to add, edit, and manage privacy annotations easily. The tool is user-friendly, works entirely in the browser, and helps make web forms more transparent, usable, and trustworthy.

By combining legal requirements, user experience design, and technical solutions, this thesis offers a practical way to improve privacy communication in online forms and support better data protection practices.

1.2 Motivation

In today's digital world, users often provide personal information online without fully understanding how it will be used. Although regulations like the General Data Protection Regulation (GDPR) mandate that websites clearly explain the reasons for data collection, many platforms still present this information in lengthy, complex privacy policies that are seldom read by users [2]. These notices are frequently buried in legal jargon and positioned far from the actual data entry points, making it challenging for users to make informed decisions [3].

At the same time, developers require solutions that are quick to implement, user-friendly, and do not disrupt the overall design of web forms [14]. This thesis was motivated by the need to assist both users and developers. It aims to create a tool that enhances the visibility and clarity of privacy information for users while remaining practical and lightweight for developers to use. By integrating principles from web development, user experience design, and privacy law, this project supports more ethical and user-friendly data collection practices.

1.3 About the Tool

The Privacy Annotation Tool developed in this thesis is a browser-based application that allows users to upload a ZIP file containing a web form, preview the form with annotations, edit those annotations, and download the updated version. It offers two annotation styles—short descriptions and info icon pop-ups—and is supported by a custom-built annotation database. The tool is fully client-side, works in any browser, and is aimed at helping both developers and legal experts collaborate in creating transparent web forms.

1.4 Structure of the Thesis

This thesis is divided into eight chapters. In the first chapter, we present the general idea, the motivation behind the project, and a brief overview of the tool. The second chapter reviews related work, covering key literature on usability, transparency, and existing privacy-enhancing technologies and tools. Chapter 3 presents an analysis of how websites across different domains inform users about the purposes of data collection, based on a large-scale manual audit of real registration and account pages.

The fourth chapter focuses on the design of transparent forms, exploring how privacy purpose annotations can be integrated at the interface level. It includes the results of a user survey comparing different annotation styles and leads to the development of interactive prototypes. Chapter 5 introduces the construction and expert validation of a database of privacy annotations tailored to common form fields, which supports the core functionality of the tool. Chapter 6 describes the design and full implementation of the Privacy Annotation Tool, explaining key components such as ZIP file handling, iframe rendering, and annotation injection logic. The seventh chapter presents the results of the tool's usability evaluation using the UEQ framework, highlighting participant feedback and overall user experience. Finally, Chapter 8 offers concluding remarks and suggests future directions for extending this work both technically and practically.

Chapter 2

2. Related Work and Tools

2.1 Introduction

As digital platforms become increasingly embedded in daily life, concerns about privacy and data transparency continue to rise. Users frequently share personal information without fully understanding how it is collected, processed, or shared. While privacy policies are intended and mandated by regulations to provide transparency, they are often lengthy, full of legal jargon, and difficult to interpret [13]. This creates a gap between compliance requirements and users' ability to make informed privacy decisions [3].

This chapter examines research on privacy policy transparency, usability heuristics, and GDPR compliance. It explores the challenges users face in understanding privacy policies and highlights strategies designed to improve clarity and accessibility. Additionally, it reviews technological solutions such as policy simplification tools, chatbot-based privacy assistants, and visual privacy indicators that aim to enhance user comprehension.

The chapter is structured as follows: Section 2.2 discusses transparency in privacy policies and GDPR compliance, focusing on challenges related to policy complexity. Section 2.3 introduces usability heuristics that support clearer communication of privacy-related information. Section 2.4 reviews existing tools designed to improve privacy transparency, including PriX and chatbot-assisted solutions. Sections 2.5 and 2.6 explore alternative approaches and summarize key findings from the reviewed literature.

2.2 Transparency in Privacy Policies and GDPR Compliance

2.2.1 The Challenge of Privacy Policy Transparency

One of the main challenges in online privacy is the complexity of privacy policies. Research has shown that privacy policies tend to be lengthy, filled with legal jargon, and difficult for users to understand, making it harder for them to grasp how their personal data is handled [13]. To address these issues, studies such as those presented in *Six Privacy and Usability Heuristics* [14] propose usability principles like improving readability, avoiding technical jargon, and enhancing accessibility to help users better comprehend privacy policies and make informed decisions.

A study presented in the book *Six Privacy and Usability Heuristics* [14] highlights this issue by outlining key principles that enhance the usability of privacy policies. One of these heuristics—Readability of Privacy Policies—addresses the problem that privacy policies are often written in complex legal language, making them inaccessible to most users. The study suggests that privacy policies should be clear, concise, and free of unnecessary jargon to improve user comprehension and decision-making. Additionally, the book discusses the importance of providing help features and avoiding overly technical terms, reinforcing the idea that privacy policies should cater to non-expert users.

These findings are particularly relevant to this research, as they align with the Purpose Limitation Principle of GDPR (Article 5-1b), which mandates that users must be clearly informed about how their personal data is being collected and processed. However, as the study suggests, compliance alone is not enough—organizations must also prioritize usability to ensure that users truly understand their privacy rights.

2.2.2 GDPR and the Purpose Limitation Principle

The General Data Protection Regulation (GDPR) mandates that organizations provide clear and accessible information regarding the collection and processing of personal data. The Purpose Limitation Principle (GDPR Article 5-1b) requires platforms to explicitly state why data is being collected and how it will be used. However, many websites fail to communicate this effectively, leading to compliance issues and a lack of user trust [5].

A study on the Solid Application Interoperability Specification [1] explored these challenges by designing and testing a user interface (UI) aimed at giving users more control over their personal data. The study developed a prototype UI based on a new access control specification called INTEROP, combined with the Data Privacy Vocabulary (DPV), which aligns with GDPR. This UI was designed to help users understand and control who can access their data and for what purposes. The study found that while the UI enabled users to define access policies, it was not user-friendly. Usability tests revealed that many users struggled to navigate the interface, with task completion accuracy ranging between 37% and 72% [1]. The findings suggest that the interface needs improvements to make it simpler and more intuitive, especially for non-expert users.

These findings highlight that merely providing privacy information is insufficient—platforms must ensure that users can easily interpret and act upon the provided data usage disclosures. Without intuitive and accessible privacy interfaces, users may struggle to make informed decisions, ultimately reducing the effectiveness of GDPR's transparency requirements. This study reinforces the importance of designing GDPR-compliant systems that also prioritize usability, ensuring that all users, regardless of technical expertise, can effectively manage their privacy settings.

2.3 Usability Heuristics for Privacy and Transparency

Ensuring privacy and transparency in digital platforms requires well-defined usability heuristics that facilitate user comprehension and interaction. The book *Six Privacy and Usability Heuristics* [14] introduces six key principles aimed at improving privacy interfaces, particularly for non-technical users. These heuristics help address common usability issues and enhance user control over privacy settings:

1. Readability of Privacy Policies: Privacy policies should be clear and easy to understand, allowing users to make informed decisions about their data.
2. Users' Doubt and Precaution: Users should be able to assess risks and consequences related to their privacy choices, encouraging careful decision-making.
3. Provide Help and Avoid Jargon: Privacy interfaces should offer guidance and avoid technical terms, ensuring accessibility for all users.
4. Discretionary Access Control: Users should be informed about who has access to their data and be able to manage permissions accordingly.
5. Fast Interaction and Human Error Vulnerabilities: Privacy settings should be designed for quick interactions while minimizing the likelihood of mistakes.
6. Unstable Choices and Appropriate Symbols: Privacy settings should accommodate changes over time, and symbols should be intuitive to help users easily interpret their choices.

These heuristics align with GDPR principles by ensuring that privacy-related information is not only available but also usable. Poor usability in privacy settings can lead to unintended data sharing, confusion, and diminished user trust. Research suggests that many platforms fail to implement these heuristics effectively, leading to opaque privacy settings and uninformed decision-making.

By adopting these usability heuristics, platforms can improve privacy transparency and user trust, ensuring that individuals can confidently manage their personal data. The next sections will explore practical tools and methods that leverage these principles to enhance privacy usability.

2.4 Existing Tools to Improve Privacy Transparency

2.4.1 PriX: The Online Privacy Policy Explainer

A notable effort to enhance privacy transparency is the PriX tool, introduced by Brunotte et al. in their paper *What About My Privacy? Helping Users Understand Online Privacy Policies* [2]. This tool aims to address the issue of overly complex privacy policies by providing users with simplified explanations and visual representations of key privacy information. PriX identifies the challenge that privacy policies are often lengthy, difficult to understand, and filled with legal jargon, making it hard for users to find relevant information about how their personal data is collected and used. Given that users expose personal data daily through digital interactions, ensuring transparency is crucial. A lack of clear privacy communication erodes user trust and limits their ability to control their personal data.

As a solution, PriX functions as a browser extension that automatically analyzes privacy policies, providing visual explanations to make key privacy information more accessible. It helps users quickly locate privacy policies and understand their contents more effectively. A user study with 65 participants demonstrated that PriX significantly improved users' ability to find privacy policies faster, identify specific privacy-related information, understand key privacy terms through visual explanations, and increase their overall awareness and trust in online services. These findings suggest that tools like PriX can play a crucial role in bridging the gap between regulatory requirements and user comprehension.

2.4.2 Chatbot-Assisted Privacy Management

Another approach to improving privacy transparency is the use of chatbot-based solutions. Vanezi et al. introduced a chatbot-based privacy assistant in *Saving the Day for Users in Web Platforms: A Chatbot-based Solution for Privacy* [17]. This chatbot provides users with a conversational interface to navigate privacy policies, manage personal data, and exercise their GDPR-defined rights.

The study found that users often struggle to locate and understand privacy settings. The chatbot, developed as a WordPress plugin and tested on an e-commerce platform, assists users by guiding them through privacy settings and providing explanations of GDPR-imposed privacy rights, such as data access, rectification, and deletion. It helps users better understand privacy policies by offering clear and direct responses to their concerns, eliminating the need to read through long documents.

The chatbot was evaluated using the User Experience Questionnaire (UEQ) with 27 participants, showing positive usability ratings, including a 2.01 score for attractiveness (excellent) and 1.91 for perspicuity (good) [20]. These results indicate that chatbot-based solutions can significantly improve privacy usability and user trust, making GDPR rights more accessible and easier to exercise.

2.5 Other Approaches to Enhancing Privacy Transparency

In addition to PriX, several other approaches have been explored to improve privacy transparency, including:

- Machine Learning-Based Privacy Policy Analysis: Tools such as Polisis [8] and PriBot [9], which use natural language processing to summarize and answer questions about privacy policies.
- Privacy Icons and Labels: Efforts to develop standardized icons that visually represent key privacy terms, similar to nutrition labels for food packaging [15].
- User Education and Awareness Campaigns: Initiatives aimed at improving digital literacy regarding data privacy [7].

2.6 Summary and Conclusions

This chapter has provided an overview of the key challenges in privacy policy transparency, the role of GDPR compliance, and usability heuristics aimed at improving user comprehension. The discussion highlighted that while legal compliance with GDPR is necessary, usability remains a major challenge in ensuring users can effectively manage their privacy settings.

The review of related works demonstrates that various tools and methods have been proposed to enhance privacy transparency, including the PriX tool, chatbot-based privacy assistants, and machine learning-based policy analysis. Despite these efforts, significant usability barriers still exist, particularly regarding the readability of privacy policies, user control over data access, and the accessibility of privacy-related information.

These findings reinforce the need for user-centered design approaches that integrate clear, interactive, and adaptive privacy controls. Future research should focus on developing hybrid solutions that combine automated compliance checks, AI-driven personalization, and usability-enhancing techniques to further improve privacy transparency and empower users in managing their personal data.

Chapter 3

3. Examining the Transparency of Personal Data Usage Across Online Platforms

3.1 Purpose of Research

The objective of this research is to examine how effectively various platforms/websites communicate the processing purposes of personal data they collect from users. Our analysis focuses on assessing whether these platforms explicitly inform users about the purpose of processing their personal data in alignment with the Purpose Limitation principle of the GDPR and a combination of usable privacy heuristics [14][5]. For this analysis, specific pages common to all selected platforms were chosen to investigate whether these platforms explicitly describe the purpose and use of all fields requiring personal data from users, ensuring clarity in their communication through web UIs.

3.2 Methodology and Data Collection

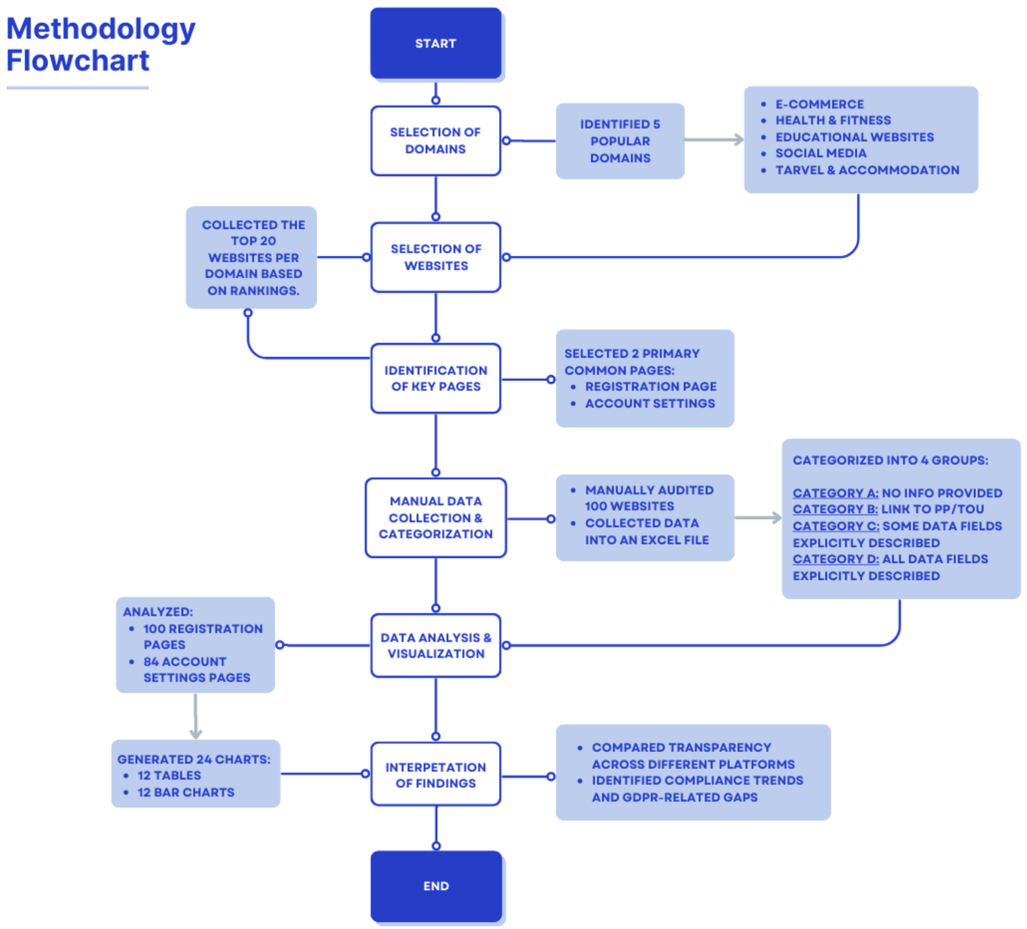

Methodology Flowchart
START
SELECTION OF DOMAINS
IDENTIFIED 5 POPULAR DOMAINS
• E-COMMERCE
• HEALTH & FITNESS
• EDUCATIONAL WEBSITES
• SOCIAL MEDIA
• TARVEL & ACCOMMODATION
COLLECTED THE TOP 20 WEBSITES PER DOMAIN BASED ON RANKINGS.
SELECTION OF WEBSITES
IDENTIFICATION OF KEY PAGES
SELECTED 2 PRIMARY COMMON PAGES:
• REGISTRATION PAGE
• ACCOUNT SETTINGS
MANUAL DATA COLLECTION & CATEGORIZATION
• MANUALLY AUDITED 100 WEBSITES
• COLLECTED DATA INTO AN EXCEL FILE
CATEGORIZED INTO 4 GROUPS:
CATEGORY A: NO INFO PROVIDED
CATEGORY B: LINK TO PP/TOU
CATEGORY C: SOME DATA FIELDS EXPLICITLY DESCRIBED
CATEGORY D: ALL DATA FIELDS EXPLICITLY DESCRIBED
ANALYZED:
• 100 REGISTRATION PAGES
• 84 ACCOUNT SETTINGS PAGES
DATA ANALYSIS & VISUALIZATION
GENERATED 24 CHARTS:
• 12 TABLES
• 12 BAR CHARTS
INTERPETATION OF FINDINGS
• COMPARED TRANSPARENCY ACROSS DIFFERENT PLATFORMS
• IDENTIFIED COMPLIANCE TRENDS AND GDPR-RELATED GAPS
END

Figure 3.1 - Methodology Flowchart for Domain Selection and Data Collection

Our methodology is presented in Figure 3.1.

First, we identified the five most popular domains based on available data[1]. These domains were selected by considering a combination of factors, such as the popularity of each domain and its relevance to how personal data is collected and managed. This approach ensures that the analysis covers platforms that not only have high user engagement but also exhibit varying practices in handling personal data. The selected domains are:

1. E-commerce platforms

[1] Stefanski, R. (2024, January 30). *10 Most Popular Types of Websites*. Verpex. Retrieved from https://verpex.com/blog/marketing-tips/10-most-popular-types-of-websites

2. Health and fitness platforms
3. Educational websites
4. Social media websites
5. Travel and accommodation platforms

For each domain, we collected the 20 most popular websites based on rankings from various sources [2] [3] [4] [5] [6]. After analyzing pages from the five selected domains, we observed that all these websites share two common main pages collecting personal data: the **Registration Page** and the **Account Settings/Edit Profile Page**. They often include multiple fields or forms requiring users to input their personal information, making them critical for evaluating how clearly and effectively the purpose of data collection is communicated.

We analyzed these 100 websites with a manual auditing procedure and collected the data in an Excel file. While the initial dataset comprised 100 websites, the final set of analyzed pages included 100 Registration Pages and 84 Account Settings/Edit Profile Pages. The reduction in the number of Account Settings pages was due to the following reasons:

1. The website does not provide an option for managing account settings.
2. Registration requires a foreign mobile number, which we could not provide.
3. The website does not require account creation, only email subscription, so no Account Settings page exists.
4. The website does not require any additional information and does not allow edits to existing information.
5. Account creation requires payment.

The investigation was guided by the following criteria:

[2] **Health and Fitness:** *Best Fitness Websites, Aelieve.* Retrieved from https://aelieve.com/rankings/websites/category/health-and-fitness/best-fitness-websites/
[3] **E-commerce and Retail**: *Top E-commerce and Retail Websites*, SEMrush. Retrieved from https://www.semrush.com/website/top/global/e-commerce-and-retail/
[4] **Educational Websites**: *Top Science and Education Websites*, Similarweb. Retrieved from https://www.similarweb.com/top-websites/science-and-education/education/
[5] **Social Media Platforms**: *Top Social Media Platforms*, Backlinko. Retrieved from https://backlinko.com/social-media-platforms
[6] **Travel and Accommodation**: *Top Accommodation and Hotels Websites*, Similarweb. Retrieved from https://www.similarweb.com/top-websites/travel-and-tourism/accommodation-and-hotels/

- The platform/website must clearly state how the user's personal data will be used (i.e., the purpose of collecting the data).
- This information must be accessible to users before they provide their personal data, either through a link or directly in text form.

It is important to note that some websites do not provide any information at all regarding the use of personal data. Identifying these cases is crucial to understanding the extent of transparency and compliance across different platforms.

We categorized the 100 Registration Pages and 84 Account Settings Pages from these websites into four groups. A website could belong to one or more categories. This categorization was based on data collected through a structured table, which included researcher observations and notes about the information relevant to our analysis[7]. Using these observations, a qualitative analysis was conducted, leading to the identification of the four groups. Some pages were associated with more than one category due to overlapping features, ensuring a systematic and comprehensive classification of the data.

- **Category A:** The website does not provide any information (neither a link nor text) about how or why personal data is collected.
- **Category B:** The website provides a link to its Privacy Policy or Terms of Use before users enter their personal data.
- **Category C:** The website explicitly describes the usage of at least some fields that require personal data.
- **Category D:** The website explicitly describes the usage of all fields that require personal data.

We also examined whether a website belonged only to Category C or Category D and found that such websites typically do not provide a Privacy Policy (Category B), which indicates non-compliance with GDPR requirements for offering clear information about personal data usage.

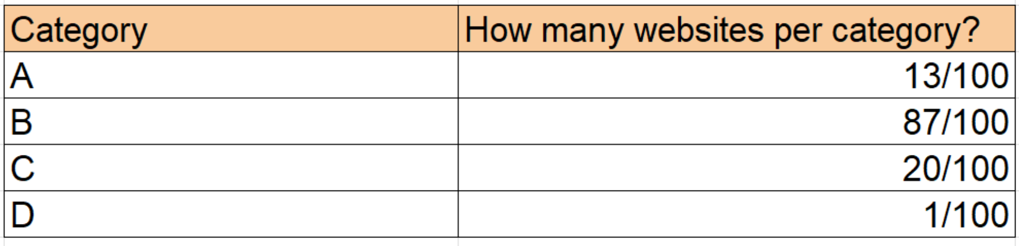
We then summarized the results in tables and graphs that follow.

[7] Data collected and categorized using a structured Excel table. Available at: Google Sheets

3.3 Results

We created 24 data representations to summarize the findings: 12 tables and their corresponding bar graphs.

1. The first two tables present the distribution of all the websites across the categories (A, B, C, D) for Registration Pages and Account Settings Pages. The counts are shown as fractions (e.g., x/100 for Registration Pages and x/84 for Account Settings Pages). The respective bar graphs display these distributions, with categories on the vertical axis and the number of websites per category on the horizontal axis.



Category	How many websites per category?
A	13/100
B	87/100
C	20/100
D	1/100

Figure 3.2 - Table 1 corresponds to the data shown in Chart 1

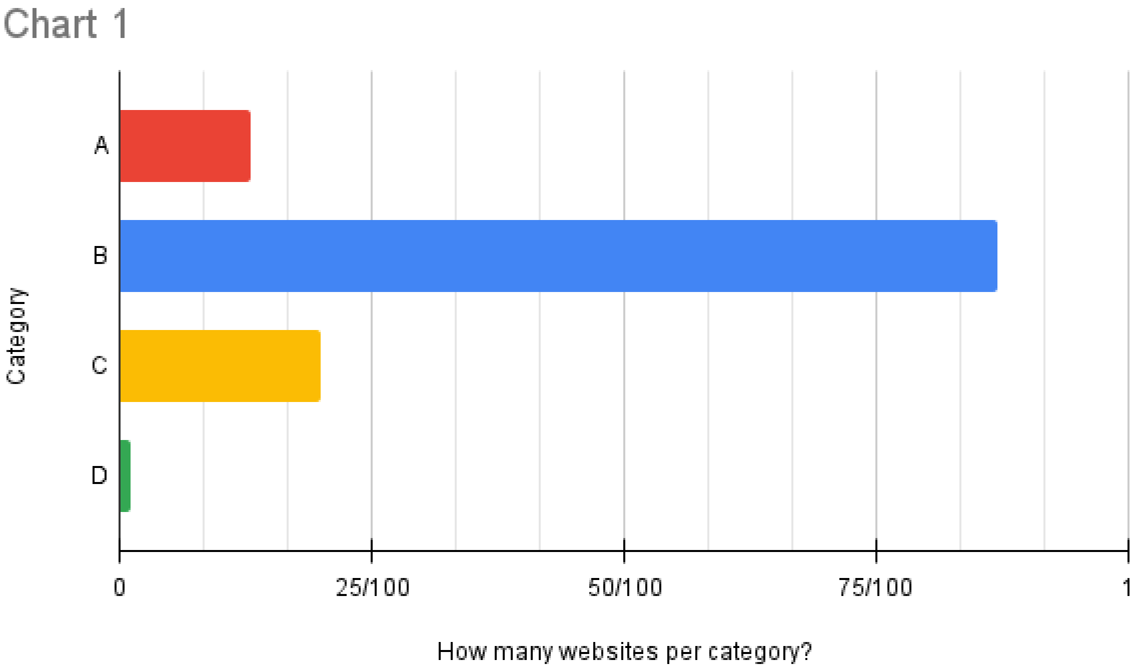
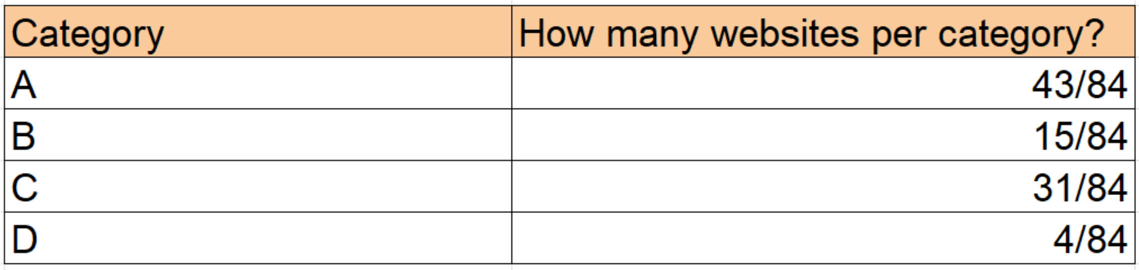


Figure 3.3 - Chart 1 shows the number of websites' Registration page that fit in each category for all five domains

The majority of websites (87 out of 100) provide a link to their Privacy Policy or Terms of Use before users submit their personal data. Among these, 20 websites also explicitly describe the purpose of at least some fields requiring personal information. However, 13 out of 100 Registration Pages offer no explanation regarding the purpose of data collection. Notably, only one Registration Page explicitly details the use of all requested personal data fields, highlighting a significant gap in transparency across platforms.



Category	How many websites per category?
A	43/84
B	15/84
C	31/84
D	4/84

Figure 3.4 - Table 2 corresponds to the data shown in Chart 2

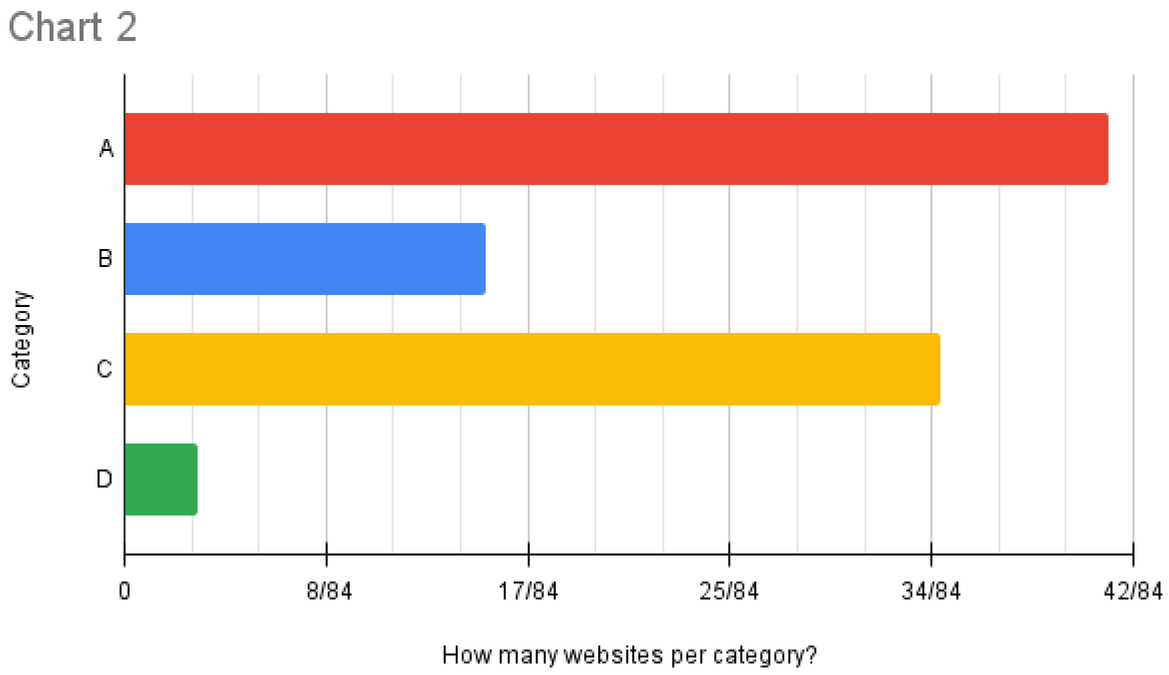


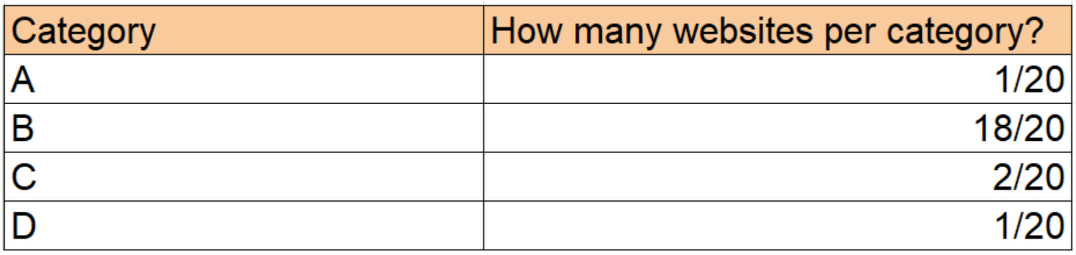
Figure 3.5 - Chart 2 shows the number of websites' Account Settings page that fit in each category for all five domains

Out of the 100 websites analyzed, only 84 Account Settings pages could be examined due to the limitations outlined in Section 3.2. Among these, only 3 out of 84 pages explicitly describe the purpose of all fields requiring personal data, placing them in Category D.

In contrast to the Registration Page results, the number of Account Settings pages that provide no information at all regarding data usage is significantly higher (43 out of 84). However, a substantial portion (34 out of 84) explicitly describes the purpose of at least some fields, while only 15 out of 84 provide a link to their Privacy Policy or Terms of Use before users submit personal data.

This discrepancy can be attributed to the assumption that users have already encountered privacy-related information during registration. As a result, many websites do not find it necessary to reiterate this information on Account Settings pages, even though these pages often involve data modifications and management.

2. The following ten tables present the distribution of Registration Pages and Account Settings Pages across the defined categories for each domain, analyzed separately. Each table contains a total of 20 pages for Registration Pages, while the count for Account Settings Pages may be lower. The corresponding bar graphs follow the same format as the first two graphs for consistency and ease of comparison.



Category	How many websites per category?
A	1/20
B	18/20
C	2/20
D	1/20

Figure 3.6 - Table 3 corresponds to the data shown in Chart 3

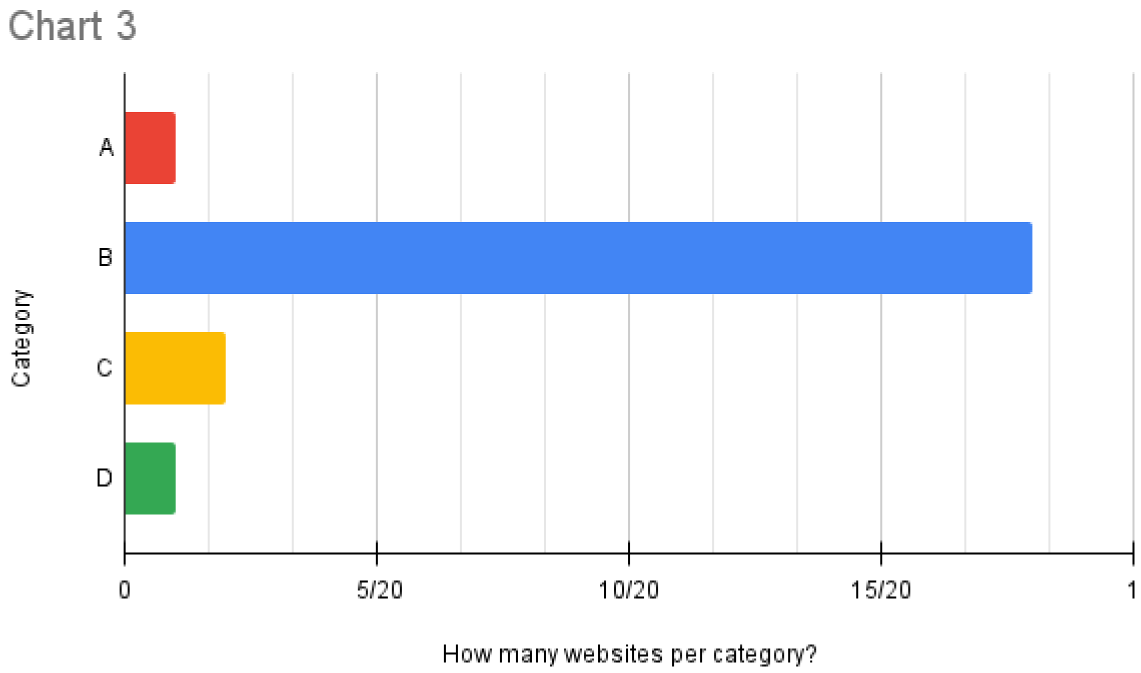
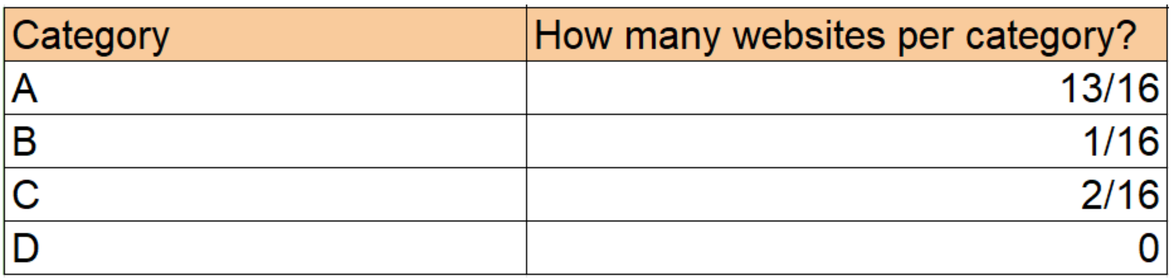


Figure 3.7 - Chart 3 shows the number of websites' Registration page that fit in each category for "E-shops" domain.

Among the 20 e-shop Registration Pages analyzed, 18 provide a link to their Privacy Policy or Terms of Use before users enter their personal data. Of these, 3 pages also explicitly describe the purpose of at least some fields requiring personal information. However, one website does not provide any information, neither a link nor textual explanation, about the purpose of data collection. Notably, only 1 out of 20 websites explicitly details the usage of all collected personal data fields, highlighting a significant gap in transparency within this domain.



Category	How many websites per category?
A	13/16
B	1/16
C	2/16
D	0

Figure 3.8 - Table 4 corresponds to the data shown in Chart 4

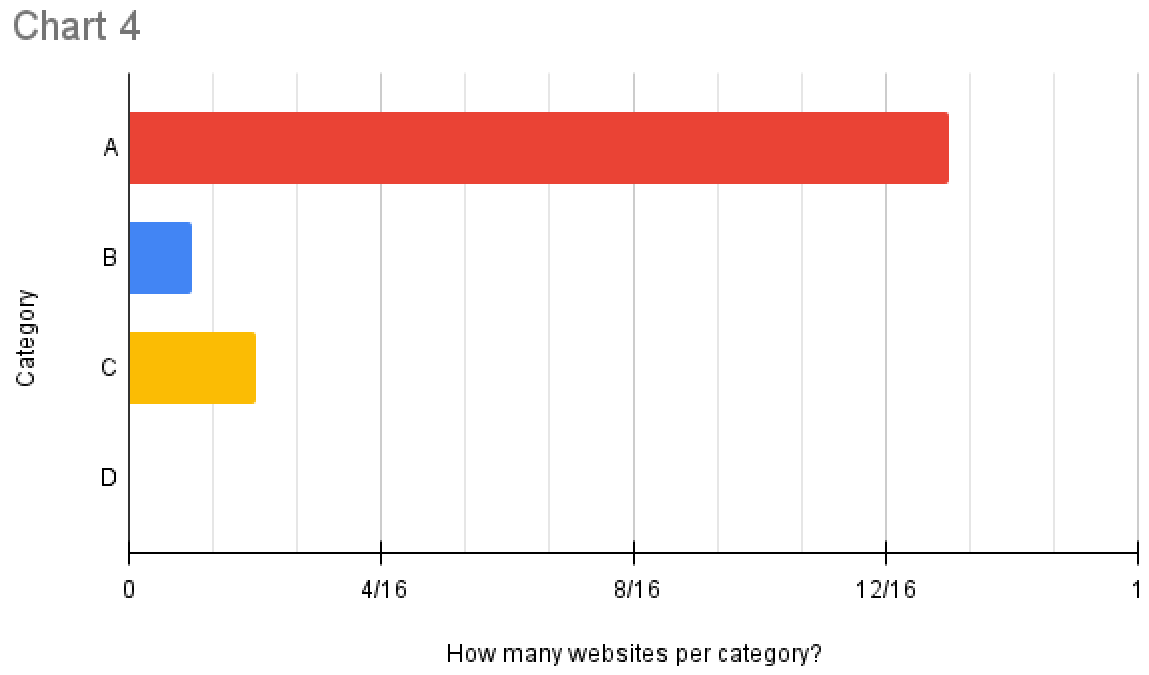
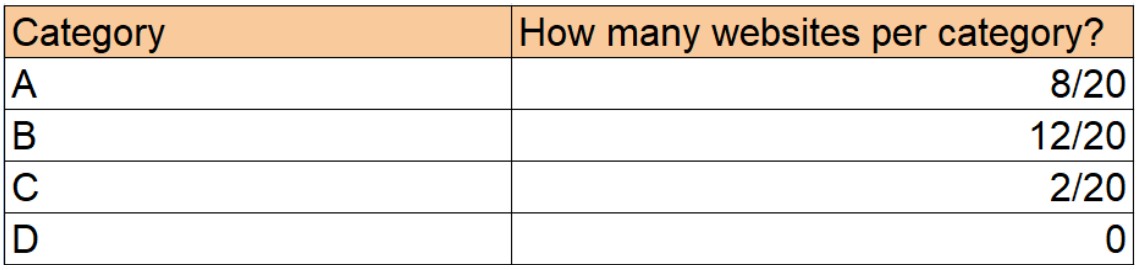


Figure 3.9 - Chart 4 shows the number of websites' Account Settings page that fit in each category for "E-shops" domain

In contrast to e-shop Registration Pages, nearly all Account Settings Pages (13 out of 16) provide no information-neither a link nor textual explanation - regarding the purpose of personal data collection. Only 2 out of 16 explicitly describe the purpose of at least some fields requiring personal data, while just one Account Settings Page includes a link to its Privacy Policy or Terms of Use before users submit their data.

A notable observation is that one Account Settings Page describes the purpose of some data fields but does not provide any related privacy policy links, meaning it belongs only to Category C. As previously mentioned, this lack of clear information indicates non-compliance with GDPR requirements, which mandate transparency in personal data usage



Category	How many websites per category?
A	8/20
B	12/20
C	2/20
D	0

Figure 3.10 - Table 5 corresponds to the data shown in Chart 5

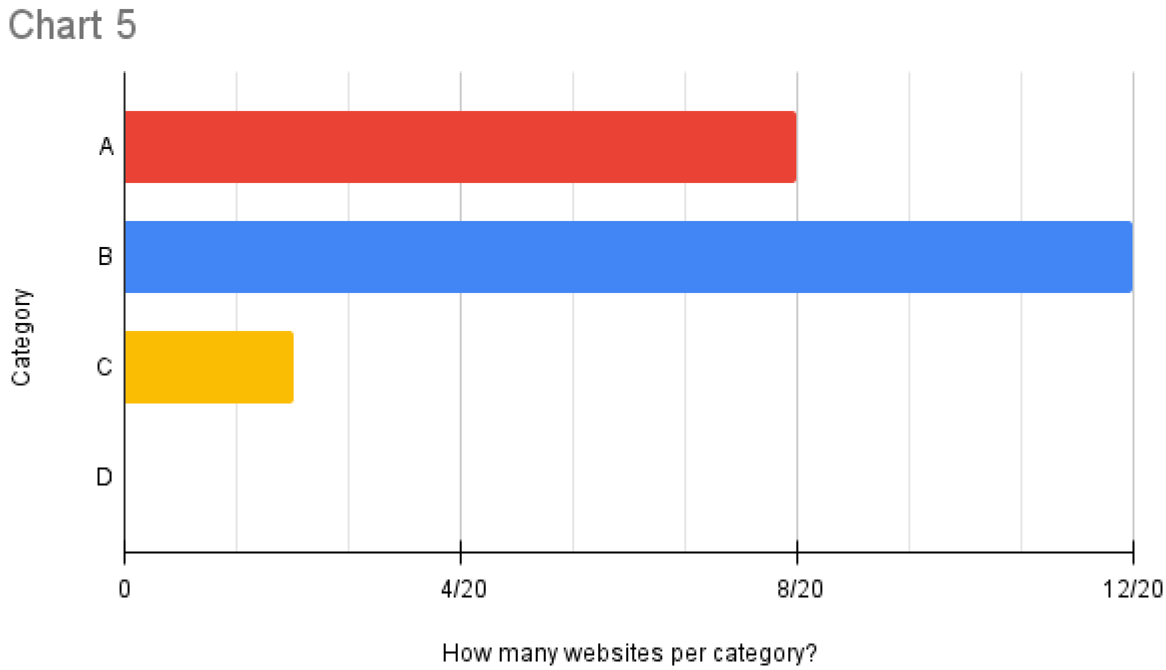
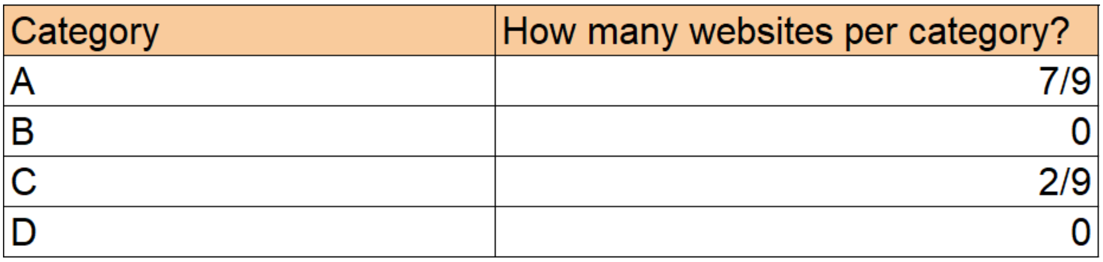


Figure 3.11 - Chart 5 shows the number of websites' Registration page that fit in each category for "Health and Fitness" domain

More than half of the Health and Fitness Registration Pages (12 out of 20) provide a link to their Privacy Policy or Terms of Use before users submit their personal data. However, only 2 pages explicitly describe the purpose of at least some fields requiring personal data.

In contrast, 8 out of 20 pages fail to provide any information-neither a link nor textual explanation-regarding how or why personal data is collected. This highlights a significant gap in transparency within the Health and Fitness sector, as many platforms rely solely on general privacy policies rather than explicitly clarifying data collection purposes during user registration.



Category	How many websites per category?
A	7/9
B	0
C	2/9
D	0

Figure 3.12 - Table 6 corresponds to the data shown in Chart 6

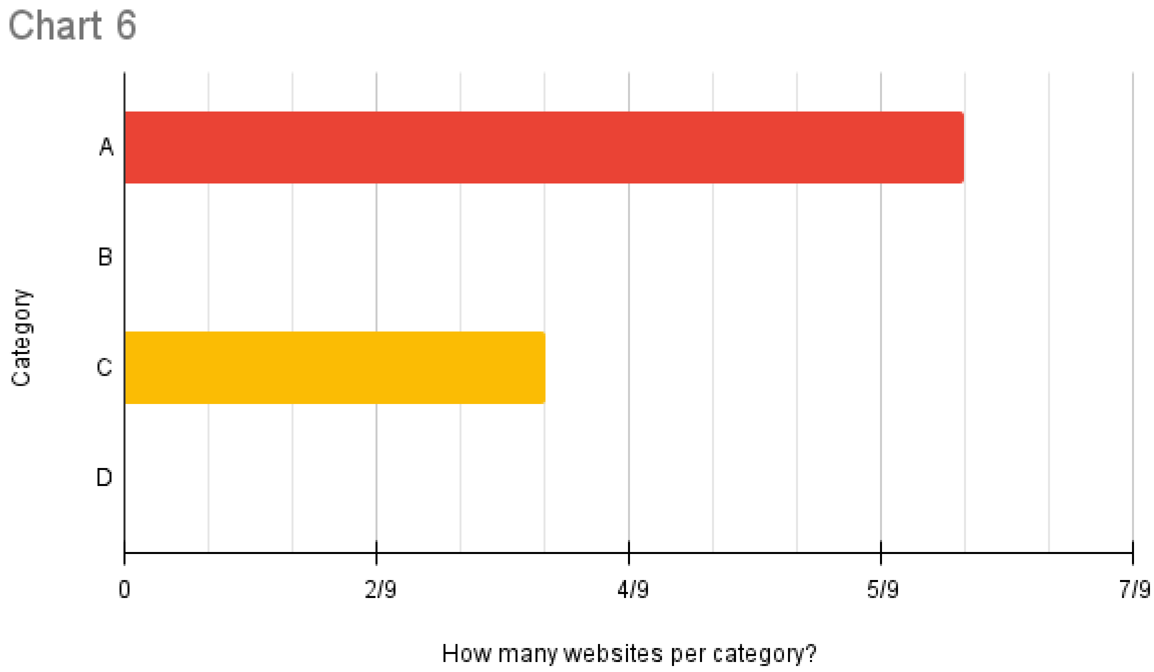
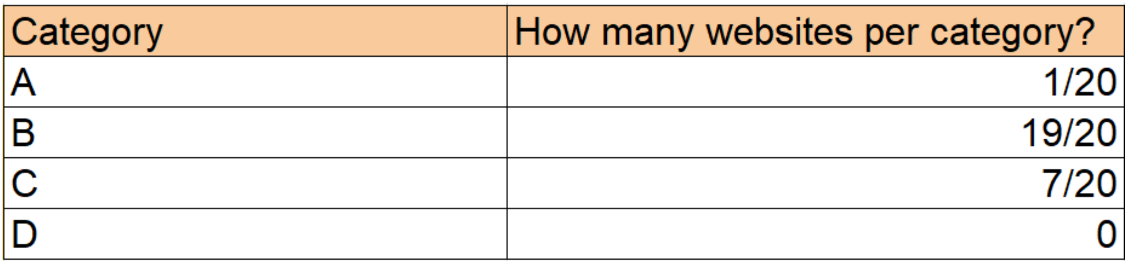


Figure 3.13 - Chart 6 shows the number of websites' Account Settings page that fit in each category for "Health and Fitness" domain

A total of 9 Account Settings Pages from the Health and Fitness domain were analyzed. Notably, none of these pages provide a link to their Privacy Policy or Terms of Use before users enter their personal data.

Most of these pages (6 out of 9) fail to offer any information-neither a link nor textual explanation-about how or why personal data is collected. In contrast, only 3 out of 9 pages explicitly describe the purpose of at least some fields requiring personal data.

These findings indicate a considerable lack of transparency in Health and Fitness platforms' Account Settings Pages, reinforcing the need for improved compliance with privacy regulations and clearer communication regarding data usage.



Category	How many websites per category?
A	1/20
B	19/20
C	7/20
D	0

Figure 3.14 - Table 7 corresponds to the data shown in Chart 7

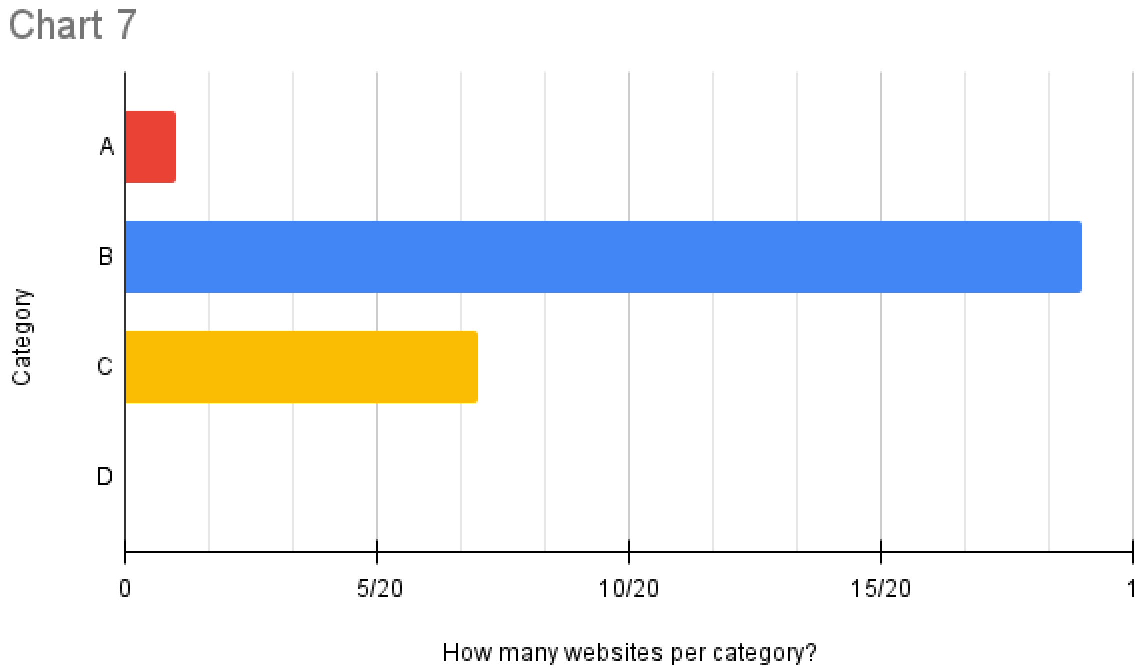
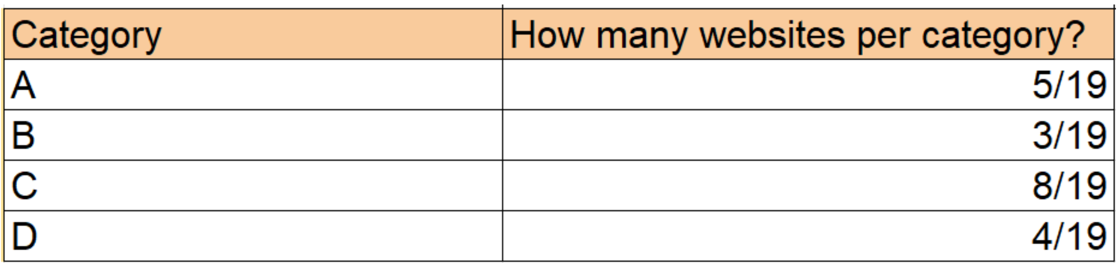


Figure 3.15 - Chart 7 shows the number of websites' Registration page that fit in each category for "Social Media" domain

Nearly all Social Media Registration Pages (19 out of 20) provide a link to their Privacy Policy or Terms of Use before users submit their personal data.

However, only 7 out of 20 pages explicitly describe the purpose of at least some fields requiring personal data.

Conversely, one Registration Page fails to offer any information-neither a link nor textual explanation-regarding how or why personal data is collected. These findings suggest that while Social Media platforms generally provide access to privacy policies, many still lack explicit, field-specific explanations for data collection.



Category	How many websites per category?
A	5/19
B	3/19
C	8/19
D	4/19

Figure 3.16 - Table 8 corresponds to the data shown in Chart 8

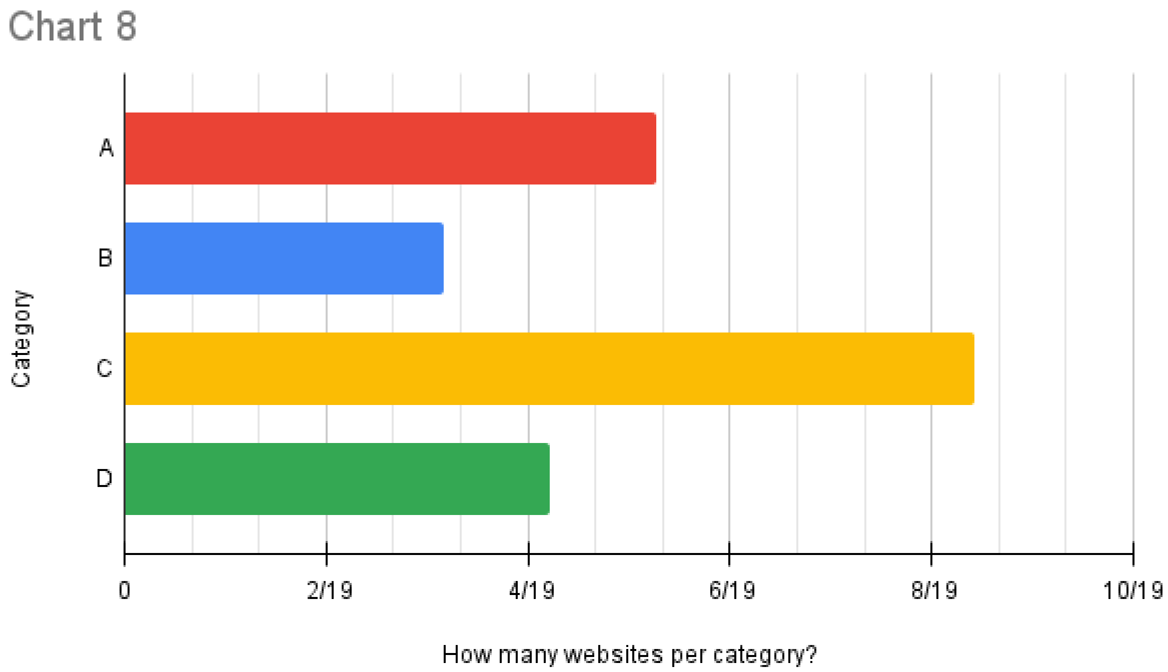
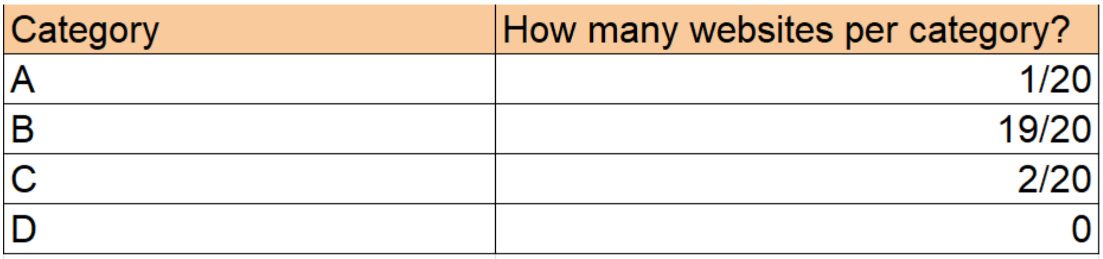


Figure 3.17 - Chart 8 shows the number of websites' Account Settings page that fit in each category for "Social Media" domain

Out of the 19 Social Media Account Settings Pages analyzed, only 5 pages provide no information, neither a link nor textual explanation, regarding how or why personal data is collected. Additionally, just 3 out of 19 pages include a link to their Privacy Policy or Terms of Use before users enter their data.

Nearly half of these pages (9 out of 19) explicitly describe the purpose of at least some fields requiring personal data. Notably, only 4 Account Settings Pages from the Social Media domain belong to Category D, meaning they fully describe the purpose of all collected personal data fields. This finding underscores the fact that only a small fraction of Social Media platforms achieves the highest level of transparency regarding data usage in their Account Settings Pages.



Category	How many websites per category?
A	1/20
B	19/20
C	2/20
D	0

Figure 3.18 - Table 9 corresponds to the data shown in Chart 9

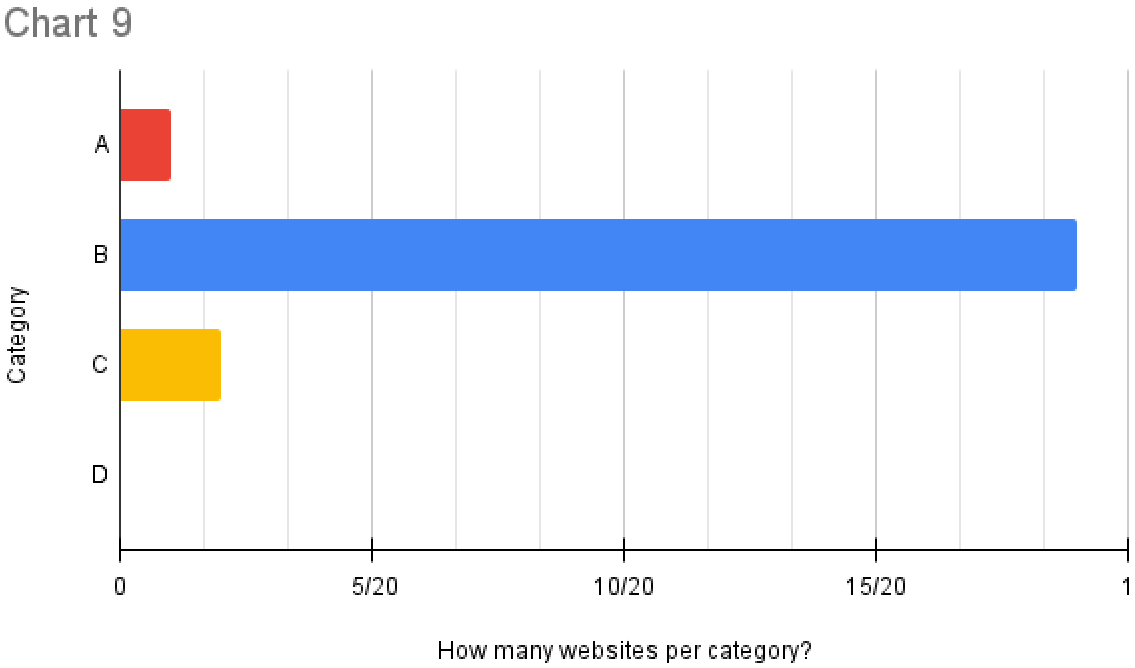
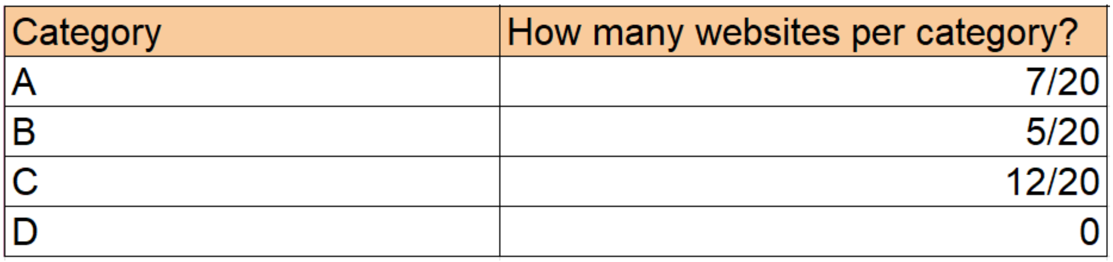


Figure 3.19 - Chart 9 shows the number of websites' Registration page that fit in each category for "Travel and Accommodation" domain

Nearly all Travel and Accommodation Registration Pages (19 out of 20) provide a link to their Privacy Policy or Terms of Use before users submit their personal data. However, only 2 out of 20 pages explicitly describe the purpose of at least some fields requiring personal data.

In contrast, one Registration Page fails to offer any information, neither a link nor textual explanation, about how or why personal data is collected. These findings suggest that while most platforms provide general privacy policies, very few offer detailed, field-specific explanations for data collection during user registration.



Category	How many websites per category?
A	7/20
B	5/20
C	12/20
D	0

Figure 3.20 - Table 10 corresponds to the data shown in Chart 10

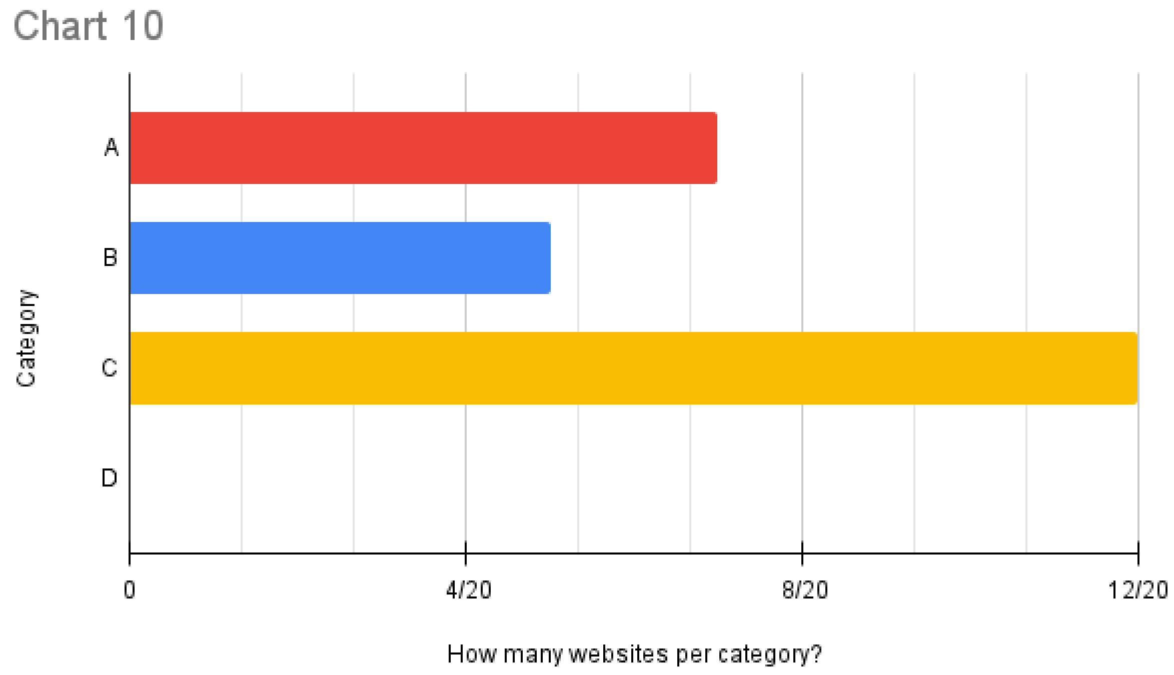
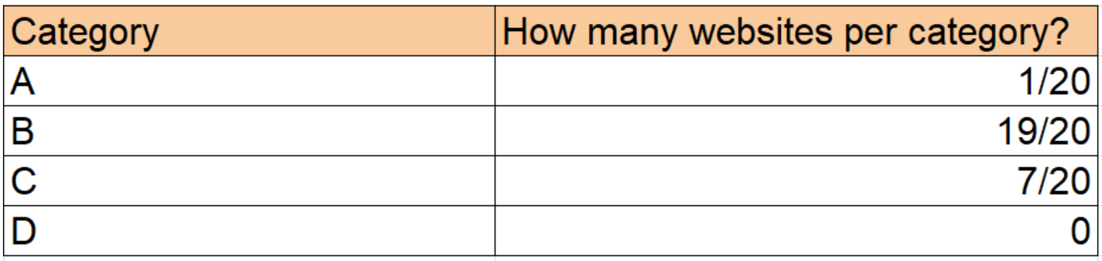


Figure 3.21 - Chart 10 shows the number of websites' Account Settings page that fit in each category for "Travel and Accommodation" domain

Among the 20 Travel and Accommodation Account Settings Pages analyzed, 13 pages explicitly describe the purpose of at least some fields requiring personal data. However, a significant portion of these pages lack sufficient transparency.

Specifically, 7 out of 20 pages provide no information, neither a link nor textual explanation, regarding how or why personal data is collected. Additionally, only 5 out of 20 pages include a link to their Privacy Policy or Terms of Use before users submit their personal data.

These findings indicate that while Travel and Accommodation platforms demonstrate some effort in explaining data collection within their Account Settings Pages, many still fail to provide a comprehensive overview of how personal information is managed, potentially affecting user awareness and compliance with data protection standards.



Category	How many websites per category?
A	1/20
B	19/20
C	7/20
D	0

Figure 3.22 - Table 11 corresponds to the data shown in Chart 11

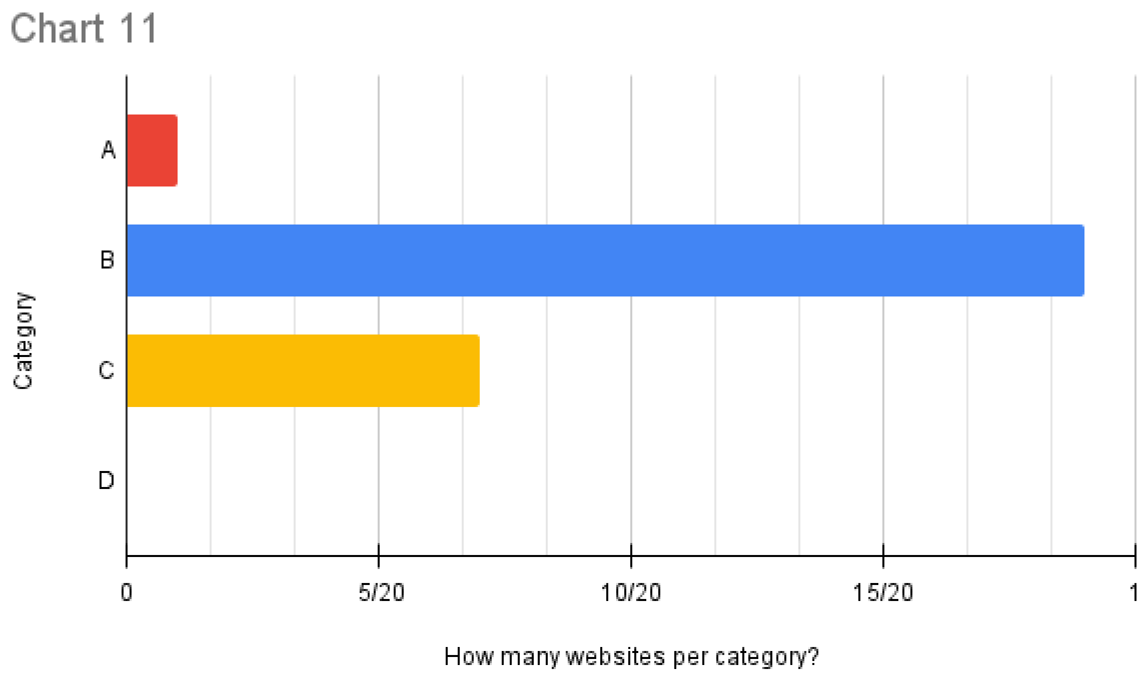
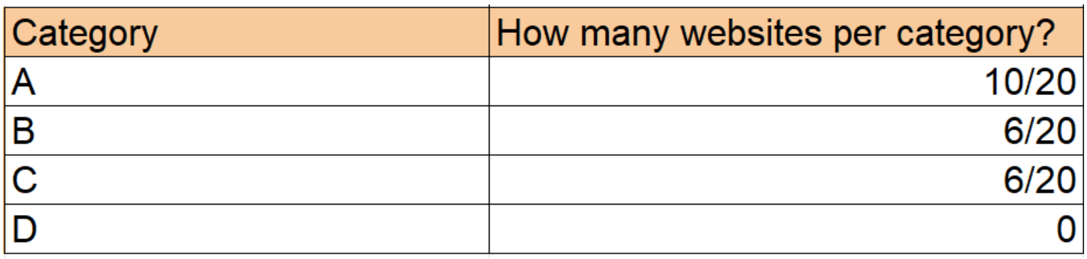


Figure 3.23 - Chart 11 shows the number of websites' Registration page that fit in each category for "Educational Websites" domain

Nearly all Educational Website Registration Pages (19 out of 20) provide a link to their Privacy Policy or Terms of Use before users submit their personal data. However, only 7 out of 20 pages explicitly describe the purpose of at least some fields requiring personal data.

In contrast, one Registration Page does not provide any information, neither a link nor textual explanation, regarding how or why personal data is collected. These findings indicate that while most Educational Websites ensure users have access to general privacy policies, a significant portion still lacks detailed, field-specific explanations of data collection during the registration process.



Category	How many websites per category?
A	10/20
B	6/20
C	6/20
D	0

Figure 3.24 - Table 12 corresponds to the data shown in Chart 12

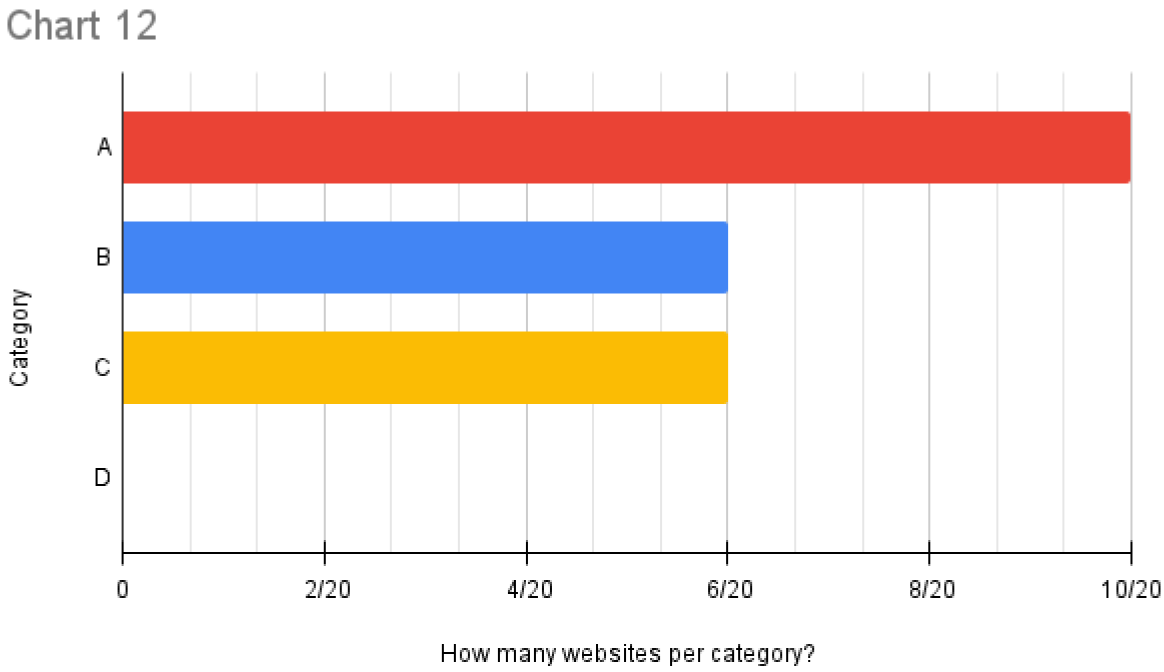


Figure 3.25 - Chart 12 shows the number of websites' Account Settings page that fit in each category for "Educational Websites" domain

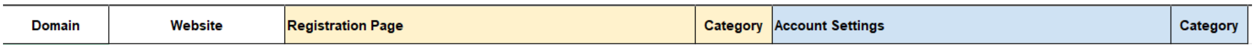
Among the 20 Educational Website Account Settings Pages analyzed, half (10 out of 20) provide no information, neither a link nor textual explanation, regarding how or why personal data is collected.

The remaining 10 pages offer some degree of transparency: 6 out of 20 pages include a link to their Privacy Policy or Terms of Use before users submit their personal data, while another 6 pages explicitly describe the purpose of at least some fields requiring personal information.

These findings suggest that while some Educational Websites provide privacy-related information, a significant portion still lacks comprehensive transparency regarding data collection and usage within their Account Settings Pages.

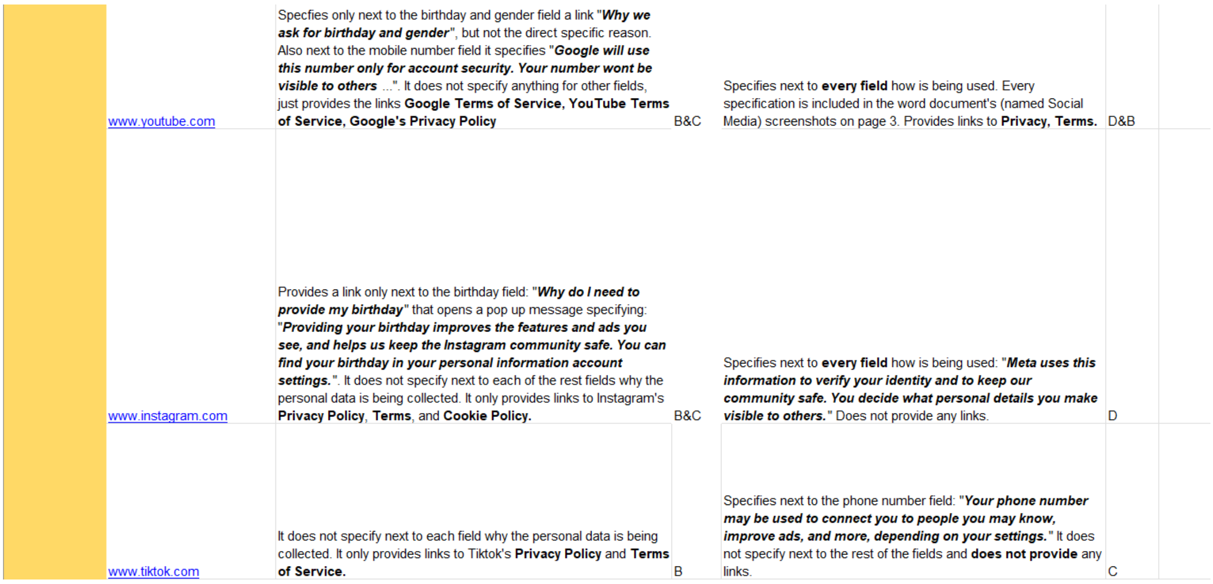
3.4 Analyzing Results Across Platforms

When looking at how different platforms explain their use of personal data, Social Media websites stood out. This was the only domain where its pages belonged to Category D. Specifically, 3 out of the 19 account settings pages that could be examined belonged to Category D, meaning they clearly explained how every piece of personal data would be used. This makes sense because Social Media platforms are often watched closely to make sure they follow GDPR rules.

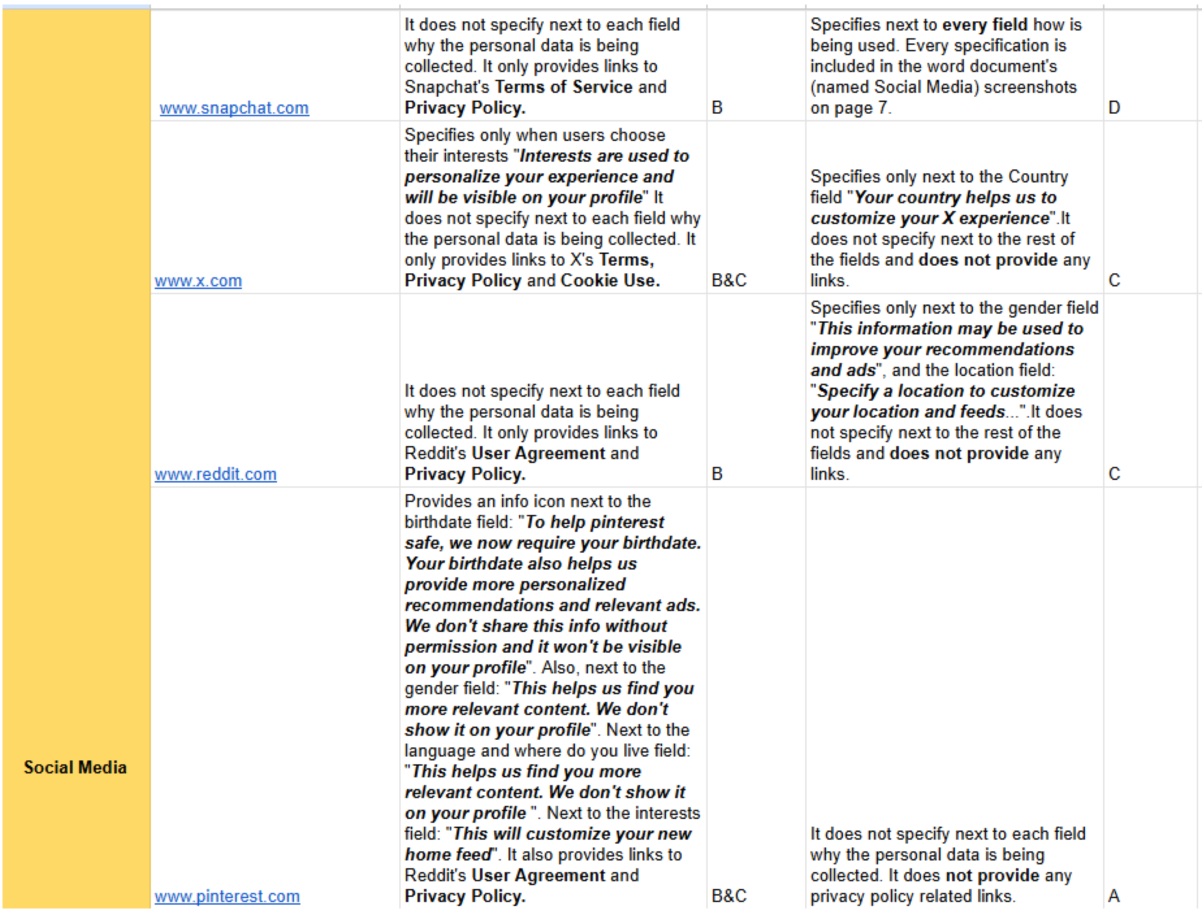


Domain	Website	Registration Page	Category	Account Settings	Category

This table shows the column headings used in the Excel file to organize and analyze the platforms based on their domains, Registration Pages, Account Settings, and their respective categories.



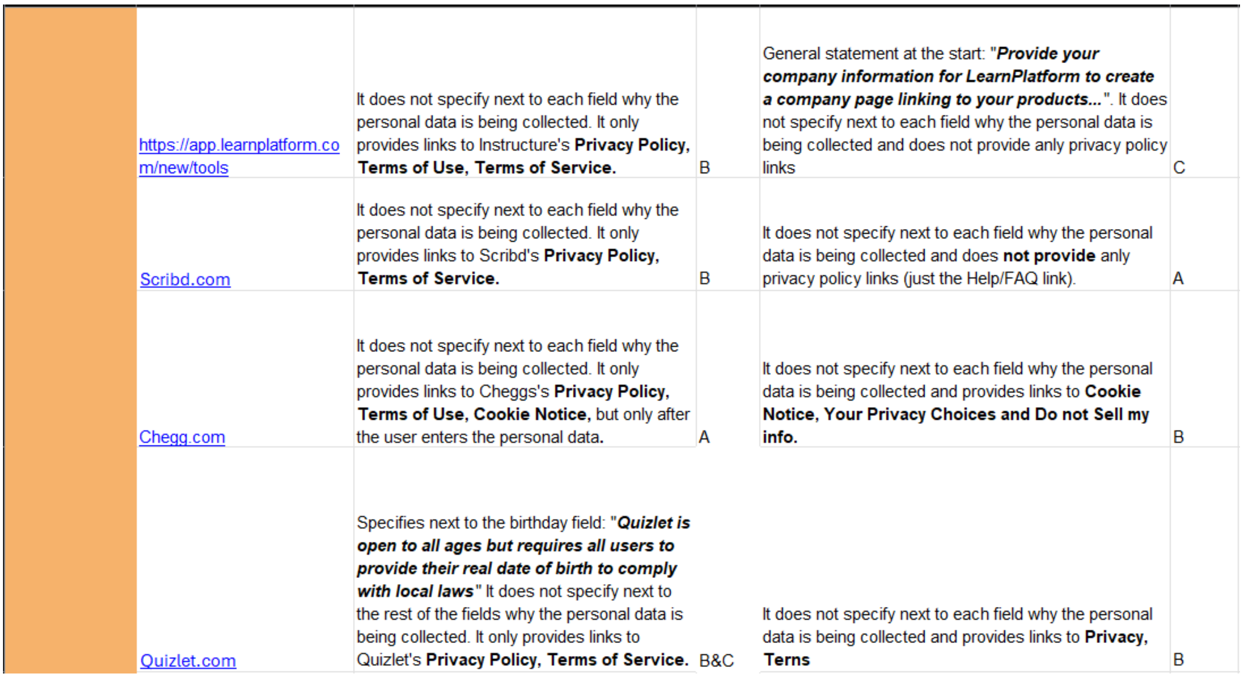
	www.youtube.com	Specfies only next to the birthday and gender field a link "***Why we ask for birthday and gender***", but not the direct specific reason. Also next to the mobile number field it specifies "***Google will use this number only for account security. Your number wont be visible to others*** ...". It does not specify anything for other fields, just provides the links **Google Terms of Service, YouTube Terms of Service, Google's Privacy Policy**	B&C	Specifies next to **every field** how is being used. Every specification is included in the word document's (named Social Media) screenshots on page 3. Provides links to **Privacy, Terms.**	D&B
	www.instagram.com	Provides a link only next to the birthday field: "***Why do I need to provide my birthday***" that opens a pop up message specifying: "***Providing your birthday improves the features and ads you see, and helps us keep the Instagram community safe. You can find your birthday in your personal information account settings.***". It does not specify next to each of the rest fields why the personal data is being collected. It only provides links to Instagram's **Privacy Policy**, **Terms**, and **Cookie Policy.**	B&C	Specifies next to **every field** how is being used: "***Meta uses this information to verify your identity and to keep our community safe. You decide what personal details you make visible to others.***" Does not provide any links.	D
	www.tiktok.com	It does not specify next to each field why the personal data is being collected. It only provides links to Tiktok's **Privacy Policy** and **Terms of Service.**	B	Specifies next to the phone number field: "***Your phone number may be used to connect you to people you may know, improve ads, and more, depending on your settings.***" It does not specify next to the rest of the fields and **does not provide** any links.	C



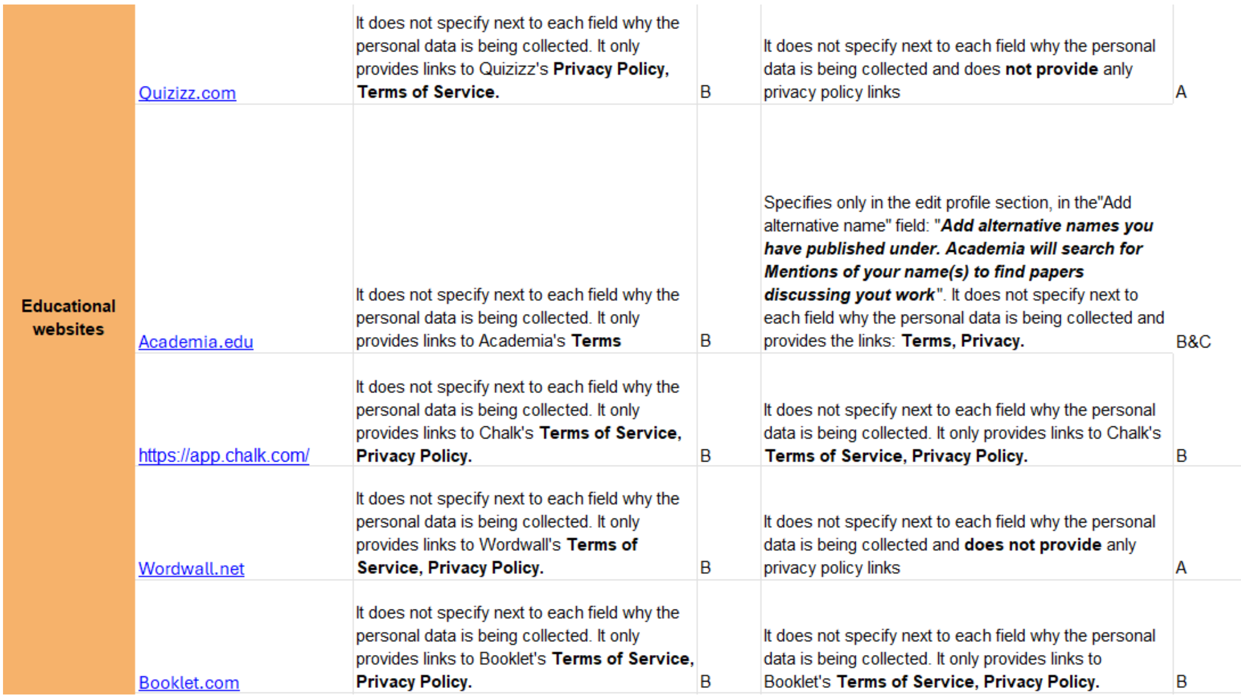
Social Media	www.snapchat.com	It does not specify next to each field why the personal data is being collected. It only provides links to Snapchat's **Terms of Service** and **Privacy Policy.**	B	Specifies next to **every field** how is being used. Every specification is included in the word document's (named Social Media) screenshots on page 7.	D
	www.x.com	Specifies only when users choose their interests "***Interests are used to personalize your experience and will be visible on your profile***" It does not specify next to each field why the personal data is being collected. It only provides links to X's **Terms, Privacy Policy** and **Cookie Use.**	B&C	Specifies only next to the Country field "***Your country helps us to customize your X experience***".It does not specify next to the rest of the fields and **does not provide** any links.	C
	www.reddit.com	It does not specify next to each field why the personal data is being collected. It only provides links to Reddit's **User Agreement** and **Privacy Policy.**	B	Specifies only next to the gender field "***This information may be used to improve your recommendations and ads***", and the location field: "***Specify a location to customize your location and feeds***...".It does not specify next to the rest of the fields and **does not provide** any links.	C
	www.pinterest.com	Provides an info icon next to the birthdate field: "***To help pinterest safe, we now require your birthdate. Your birthdate also helps us provide more personalized recommendations and relevant ads. We don't share this info without permission and it won't be visible on your profile***". Also, next to the gender field: "***This helps us find you more relevant content. We don't show it on your profile***". Next to the language and where do you live field: "***This helps us find you more relevant content. We don't show it on your profile*** ". Next to the interests field: "***This will customize your new home feed***". It also provides links to Reddit's **User Agreement** and **Privacy Policy.**	B&C	It does not specify next to each field why the personal data is being collected. It does **not provide** any privacy policy related links.	A

In contrast, Travel and Accommodation platforms, along with Educational Websites, performed less effectively. A significant number of these websites fell into Category A or B, indicating a lack of detailed transparency. Instead of providing field-specific explanations, many relied solely on general Privacy Policies (Category B). Additionally, some websites in Category C also belonged to Category B, meaning they offered partial explanations for certain data fields while still relying on a general privacy policy for broader details.

Travel and accommodation platforms	https://www.lufthansa.com/cy/en/homepage	It does not specify next to each field why the personal data is being collected. It only provides links to Lufthansa's **Travel ID Terms and Conditions of use, Travel ID Privacy Policy.**	B	Next to the telephone number field specifies: "***How can we contact you (eg. with information about your flight)***" "***Your preferred telephone number will be used for messages about your flight.***" "***We will inform you by SMS about changes to your booked flight***". Next to the Wallet field (saved payment method): "***Select your preferred payment method and save valuable time when paying. If you have already saved your credit card details and they are not visible, enter them again once. This step is necessary for data protection reasons.***" It does not specify next to the rest of the fields why the personal data is being collected. It does not provide any privacy policy related links.	C
	www.tripadvisor.com	It does not specify next to each field why the personal data is being collected. It only provides links to Tripadvisor's **Terms of use, Privacy and Cookie Statement, Privacy Policy, Terms of Service.**	B	It does not specify next to each field why the personal data is being collected. Provides the links **Terms of Use**, **Privacy and Cookies Statement**, **Cookie Consent**.	B
	www.trip.com	It does not specify next to each field why the personal data is being collected. It only provides links to Trip's **Terms and Conditions, Privacy Statement.**	B	Specifies next to the phone number "***Once you've linked a phone number to your account, you'll be able to use it to sign in to Trip.com***". Next to the DIsplay name field "***Your display name will be shown when you post reviews or other content on Trip.com...***".It does not provide any privacy policy related links.	C
	www.ryanair.com	It does not specify next to each field why the personal data is being collected. It only provides links to Ryanair's **Privacy Policy, Terms of Use.**	B	General statement at the start Your personal information: "***We'll use this to automatically fill yout booking details and keep you informed***". General statements for travel documents: "***This information will be used to autofill your travel documents information during check-in***". General statement at Travel companions field: "***Add friends and family to your myRyanair account and make it easy to add them to your booking*** ". On My Wallet field: "***Welcome to your Wallet. Refunds requested for flight disruptions will be deposited here. You can withdraw your refund from your Wallet to the original payment method used to make the booking (within 5 working days) in one click by choosing "Withdraw Refund" or you can simply use your Wallet balance to book a new flight on the Ryanair website, by selecting "Access your Wallet" as your preferred payment method. Click here to read Terms of Use and FAQ***." Also, a link is provided in every field: **Ryanair Privacy Policy.**	B&C
	www.skyscanner.com	It does not specify next to each field why the personal data is being collected. It only provides links to Skyscanner's **Όρους Παροχής Υπηρεσιών, Πολιτική Απορρήτου.**	B	It does not specify next to each field why the personal data is being collected. It does **not provide** any privacy policy related links.	A

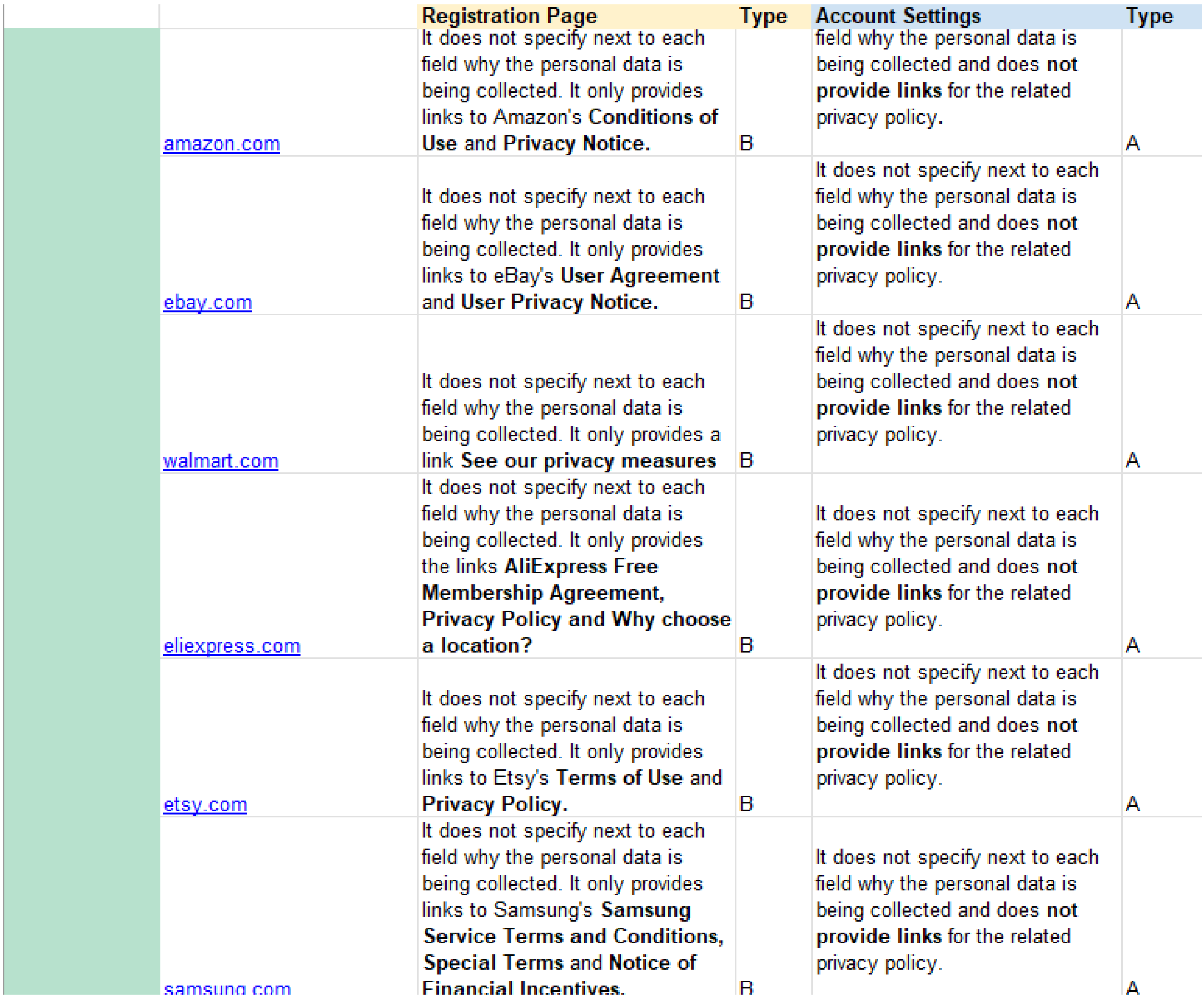


	https://app.learnplatform.com/new/tools	It does not specify next to each field why the personal data is being collected. It only provides links to Instructure's **Privacy Policy, Terms of Use, Terms of Service.**	B	General statement at the start: "***Provide your company information for LearnPlatform to create a company page linking to your products...***". It does not specify next to each field why the personal data is being collected and does not provide anly privacy policy links	C
	Scribd.com	It does not specify next to each field why the personal data is being collected. It only provides links to Scribd's **Privacy Policy, Terms of Service.**	B	It does not specify next to each field why the personal data is being collected and does **not provide** anly privacy policy links (just the Help/FAQ link).	A
	Chegg.com	It does not specify next to each field why the personal data is being collected. It only provides links to Cheggs's **Privacy Policy, Terms of Use, Cookie Notice,** but only after the user enters the personal data.	A	It does not specify next to each field why the personal data is being collected and provides links to **Cookie Notice, Your Privacy Choices and Do not Sell my info.**	B
	Quizlet.com	Specifies next to the birthday field: "***Quizlet is open to all ages but requires all users to provide their real date of birth to comply with local laws***" It does not specify next to the rest of the fields why the personal data is being collected. It only provides links to Quizlet's **Privacy Policy, Terms of Service.**	B&C	It does not specify next to each field why the personal data is being collected and provides links to **Privacy, Terns**	B

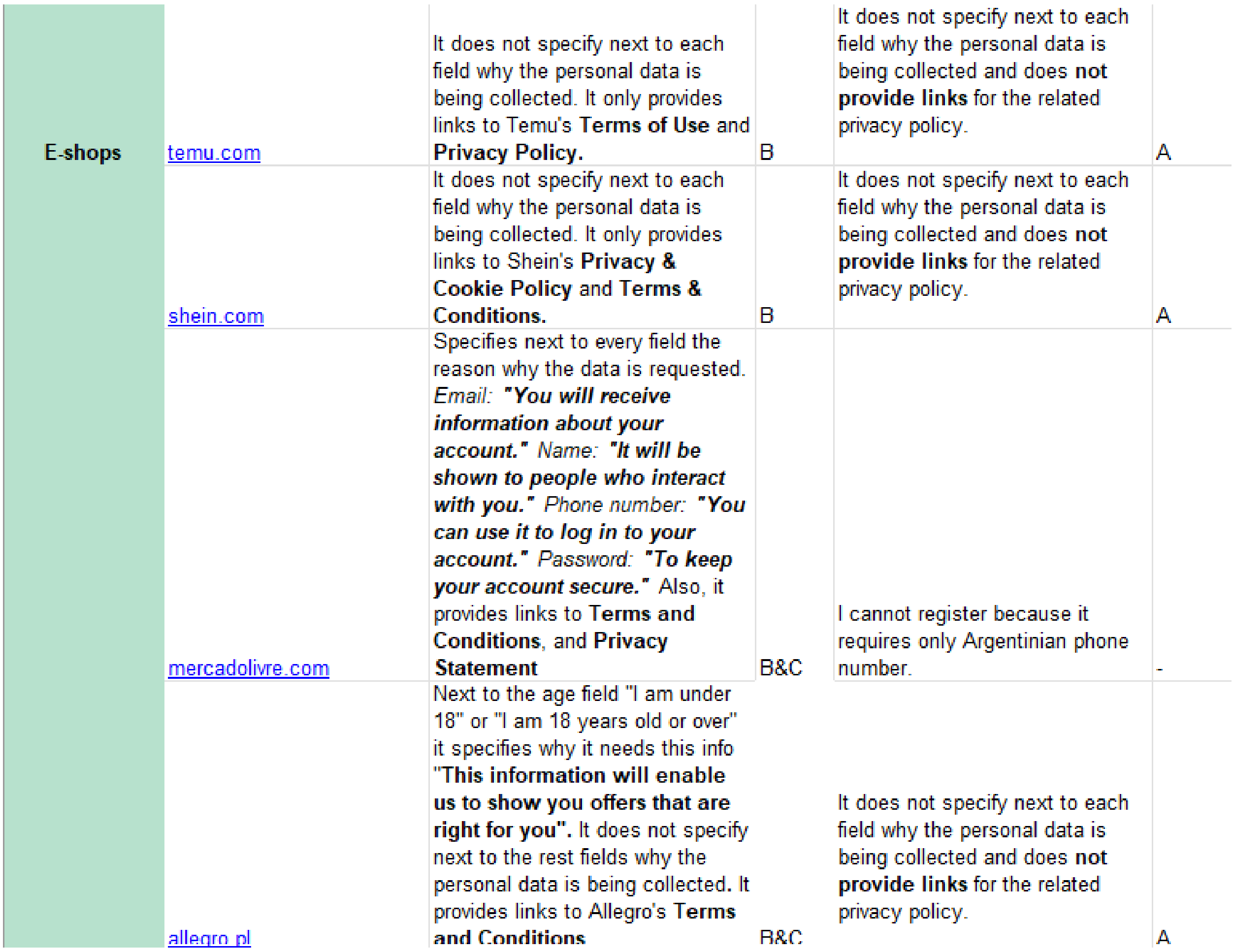


Educational websites	Quizizz.com	It does not specify next to each field why the personal data is being collected. It only provides links to Quizizz's **Privacy Policy, Terms of Service.**	B	It does not specify next to each field why the personal data is being collected and does **not provide** anly privacy policy links	A
	Academia.edu	It does not specify next to each field why the personal data is being collected. It only provides links to Academia's **Terms**	B	Specifies only in the edit profile section, in the"Add alternative name" field: "***Add alternative names you have published under. Academia will search for Mentions of your name(s) to find papers discussing yout work***". It does not specify next to each field why the personal data is being collected and provides the links: **Terms, Privacy.**	B&C
	https://app.chalk.com/	It does not specify next to each field why the personal data is being collected. It only provides links to Chalk's **Terms of Service, Privacy Policy.**	B	It does not specify next to each field why the personal data is being collected. It only provides links to Chalk's **Terms of Service, Privacy Policy.**	B
	Wordwall.net	It does not specify next to each field why the personal data is being collected. It only provides links to Wordwall's **Terms of Service, Privacy Policy.**	B	It does not specify next to each field why the personal data is being collected and **does not provide** anly privacy policy links	A
	Booklet.com	It does not specify next to each field why the personal data is being collected. It only provides links to Booklet's **Terms of Service, Privacy Policy.**	B	It does not specify next to each field why the personal data is being collected. It only provides links to Booklet's **Terms of Service, Privacy Policy.**	B

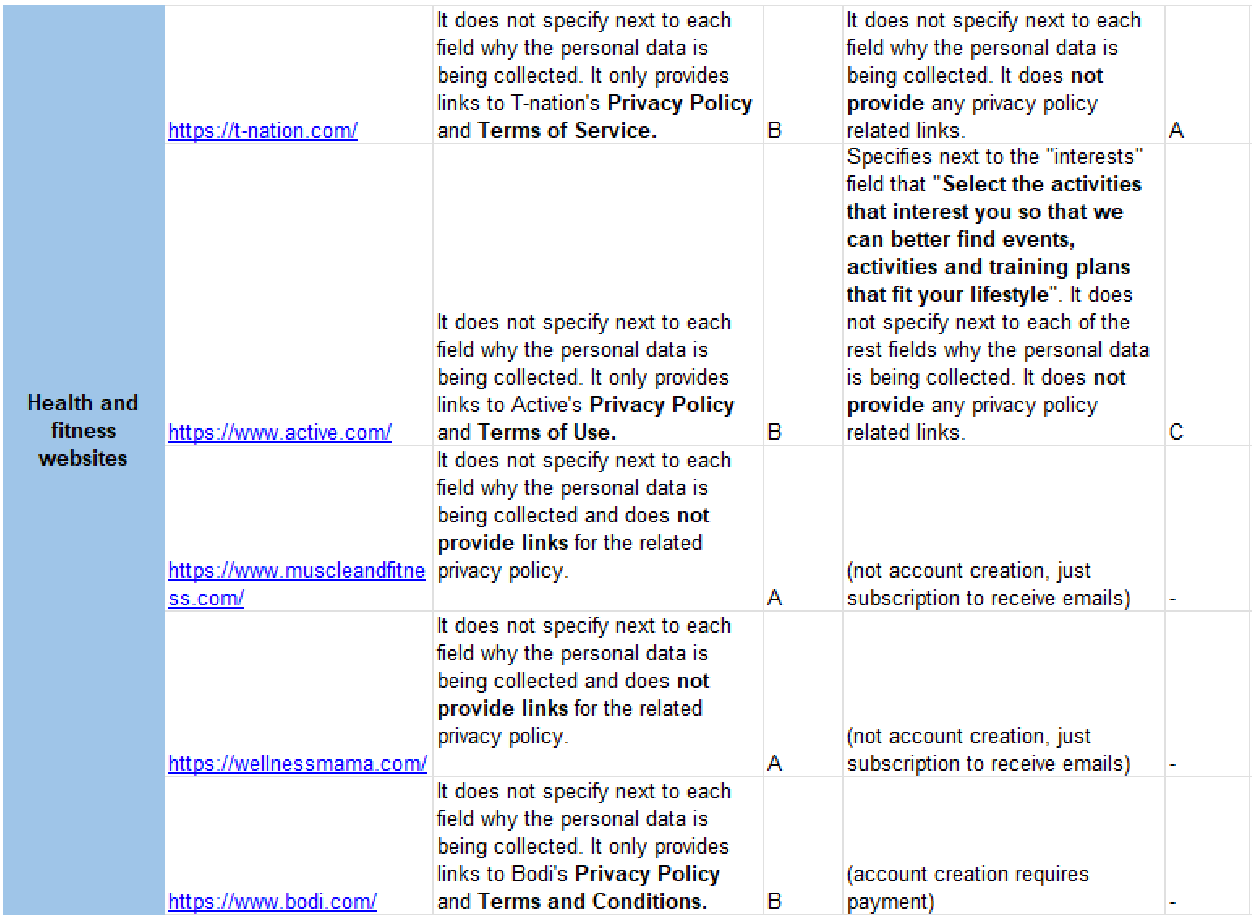
E-commerce and Health & Fitness platforms exhibited mixed results but failed to reach Category D. Their Registration Pages primarily relied on Privacy Policies (Category B), with only some providing limited explanations for specific data fields (Category C). This indicates a need for greater transparency. The Account Settings Pages performed even worse, with many offering no explanation of data usage at all (Category A).



		Registration Page	Type	Account Settings	Type
	amazon.com	It does not specify next to each field why the personal data is being collected. It only provides links to Amazon's **Conditions of Use** and **Privacy Notice.**	B	field why the personal data is being collected and does **not provide links** for the related privacy policy**.**	A
	ebay.com	It does not specify next to each field why the personal data is being collected. It only provides links to eBay's **User Agreement** and **User Privacy Notice.**	B	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A
	walmart.com	It does not specify next to each field why the personal data is being collected. It only provides a link **See our privacy measures**	B	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A
	eliexpress.com	It does not specify next to each field why the personal data is being collected. It only provides the links **AliExpress Free Membership Agreement, Privacy Policy and Why choose a location?**	B	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A
	etsy.com	It does not specify next to each field why the personal data is being collected. It only provides links to Etsy's **Terms of Use** and **Privacy Policy.**	B	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A
	samsung.com	It does not specify next to each field why the personal data is being collected. It only provides links to Samsung's **Samsung Service Terms and Conditions, Special Terms** and **Notice of Financial Incentives.**	B	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A



E-shops	temu.com	It does not specify next to each field why the personal data is being collected. It only provides links to Temu's **Terms of Use** and **Privacy Policy.**	B	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A
	shein.com	It does not specify next to each field why the personal data is being collected. It only provides links to Shein's **Privacy & Cookie Policy** and **Terms & Conditions.**	B	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A
	mercadolivre.com	Specifies next to every field the reason why the data is requested. *Email:* ***"You will receive information about your account."*** *Name:* ***"It will be shown to people who interact with you."*** *Phone number:* ***"You can use it to log in to your account."*** *Password:* ***"To keep your account secure."*** Also, it provides links to **Terms and Conditions**, and **Privacy Statement**	B&C	I cannot register because it requires only Argentinian phone number.	-
	allegro.pl	Next to the age field "I am under 18" or "I am 18 years old or over" it specifies why it needs this info "**This information will enable us to show you offers that are right for you".** It does not specify next to the rest fields why the personal data is being collected**.** It provides links to Allegro's **Terms and Conditions**	B&C	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A



Health and fitness websites	https://t-nation.com/	It does not specify next to each field why the personal data is being collected. It only provides links to T-nation's **Privacy Policy** and **Terms of Service.**	B	It does not specify next to each field why the personal data is being collected. It does **not provide** any privacy policy related links.	A
	https://www.active.com/	It does not specify next to each field why the personal data is being collected. It only provides links to Active's **Privacy Policy** and **Terms of Use.**	B	Specifies next to the "interests" field that "**Select the activities that interest you so that we can better find events, activities and training plans that fit your lifestyle**". It does not specify next to each of the rest fields why the personal data is being collected. It does **not provide** any privacy policy related links.	C
	https://www.muscleandfitness.com/	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A	(not account creation, just subscription to receive emails)	-
	https://wellnessmama.com/	It does not specify next to each field why the personal data is being collected and does **not provide links** for the related privacy policy.	A	(not account creation, just subscription to receive emails)	-
	https://www.bodi.com/	It does not specify next to each field why the personal data is being collected. It only provides links to Bodi's **Privacy Policy** and **Terms and Conditions.**	B	(account creation requires payment)	-

Overall, Registration Pages were more effective in explaining data usage compared to Account Settings Pages. Most websites prioritized transparency during the sign-up process but provided less information when users managed their data later. This trend was particularly evident in Travel and E-commerce platforms, where post-registration data management appeared to be a lower priority.

Among all domains, Social Media platforms demonstrated the highest level of transparency, with most pages falling into Categories C or D. In contrast, E-commerce websites performed the worst, with many failing to provide even basic Privacy Policies or clear explanations of how they use personal information.

Chapter 4

4. Designing Transparent Forms

4.1 Problem Statement

Research in the fields of usable privacy and human-computer interaction (HCI) has consistently emphasized the need for clear, context-sensitive explanations about data practices [10]. Despite the GDPR's emphasis on transparency and the principle of purpose limitation, there remains a substantial gap in how this transparency is operationalized in the design of user interfaces.

This problem is especially pronounced during post-registration interactions—such as updating profiles or account settings—where transparency tends to decline. Users often assume that previously stated privacy notices still apply, even though they may be modifying or providing new information. In this context, the lack of form-level and field-level guidance represents a missed opportunity to reinforce trust and ensure ongoing informed consent [4].

4.2 Objective

This chapter addresses the identified transparency gap by exploring user-centered design strategies for online forms. The aim is to develop practical, design-oriented solutions that make the purpose of each data field explicit. Through a combination of survey-based research and prototyping, this chapter investigates how form designs can enhance user awareness, promote meaningful informed consent, and align with both usability principles and data protection regulations [4][19].

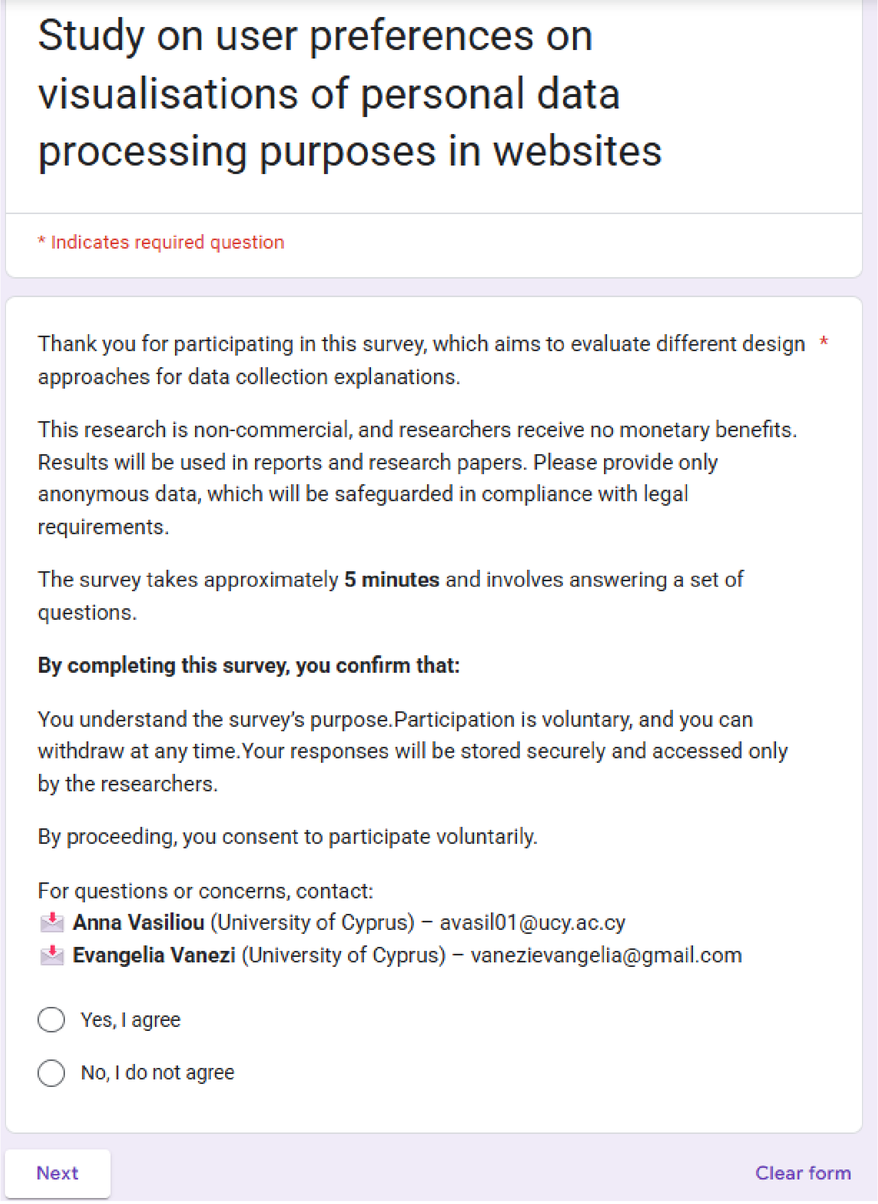
By examining user preferences, analyzing their reactions to various form design patterns, and translating these insights into interactive prototypes, the chapter proposes a set of design guidelines for building transparent, trustworthy forms. Ultimately, the goal is to empower users to make informed decisions about the data they share while helping organizations meet regulatory and ethical obligations [4][19].

4.3 Methodology

4.3.1 Survey Design

To assess how users perceive transparency in online forms, a structured questionnaire was created using Google Forms. The survey aimed to compare user reactions to different interface design approaches that attempt to explain the purpose of personal data collection [12].

The survey began with an informed consent section, outlining the study’s objective, assuring participants that their participation was voluntary, and confirming that responses would remain anonymous and used exclusively for research purposes. It also stated the estimated time required to complete the survey (approximately 5 minutes) and provided contact details for the research team.



Study on user preferences on visualisations of personal data processing purposes in websites

* Indicates required question

Thank you for participating in this survey, which aims to evaluate different design approaches for data collection explanations. *

This research is non-commercial, and researchers receive no monetary benefits. Results will be used in reports and research papers. Please provide only anonymous data, which will be safeguarded in compliance with legal requirements.

The survey takes approximately **5 minutes** and involves answering a set of questions.

By completing this survey, you confirm that:

You understand the survey's purpose.Participation is voluntary, and you can withdraw at any time.Your responses will be stored securely and accessed only by the researchers.

By proceeding, you consent to participate voluntarily.

For questions or concerns, contact:
📩 **Anna Vasiliou** (University of Cyprus) – avasil01@ucy.ac.cy
📩 **Evangelia Vanezi** (University of Cyprus) – vanezievangelia@gmail.com

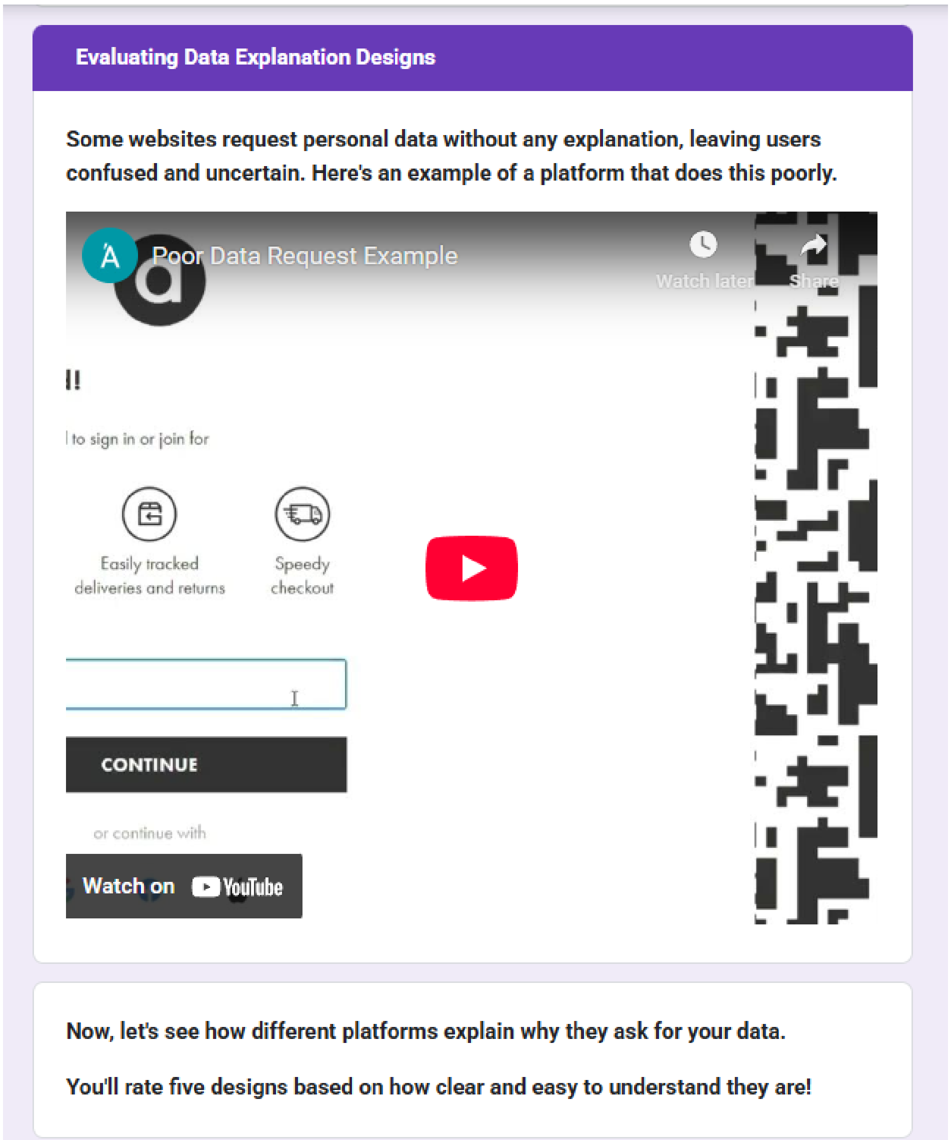
○ Yes, I agree

○ No, I do not agree

The main focus of the questionnaire was quantitative evaluation, using primarily closed-ended questions and Likert-scale ratings. Participants were shown five different examples of online forms, each representing a different transparency strategy:

1. **Icon pop-up messages**
2. **Short explanation next to the field**
3. **One general explanation for all fields**
4. **Clickable link to more information**
5. **Pop-up from a clickable link**

Each design was presented with a real-life example (with identifying elements removed), followed by a 1–5 star rating scale. Participants were asked to evaluate each design based on clarity and ease of understanding. After rating each design individually, respondents were prompted to select which design they believed most effectively communicated the purpose of data collection [6].

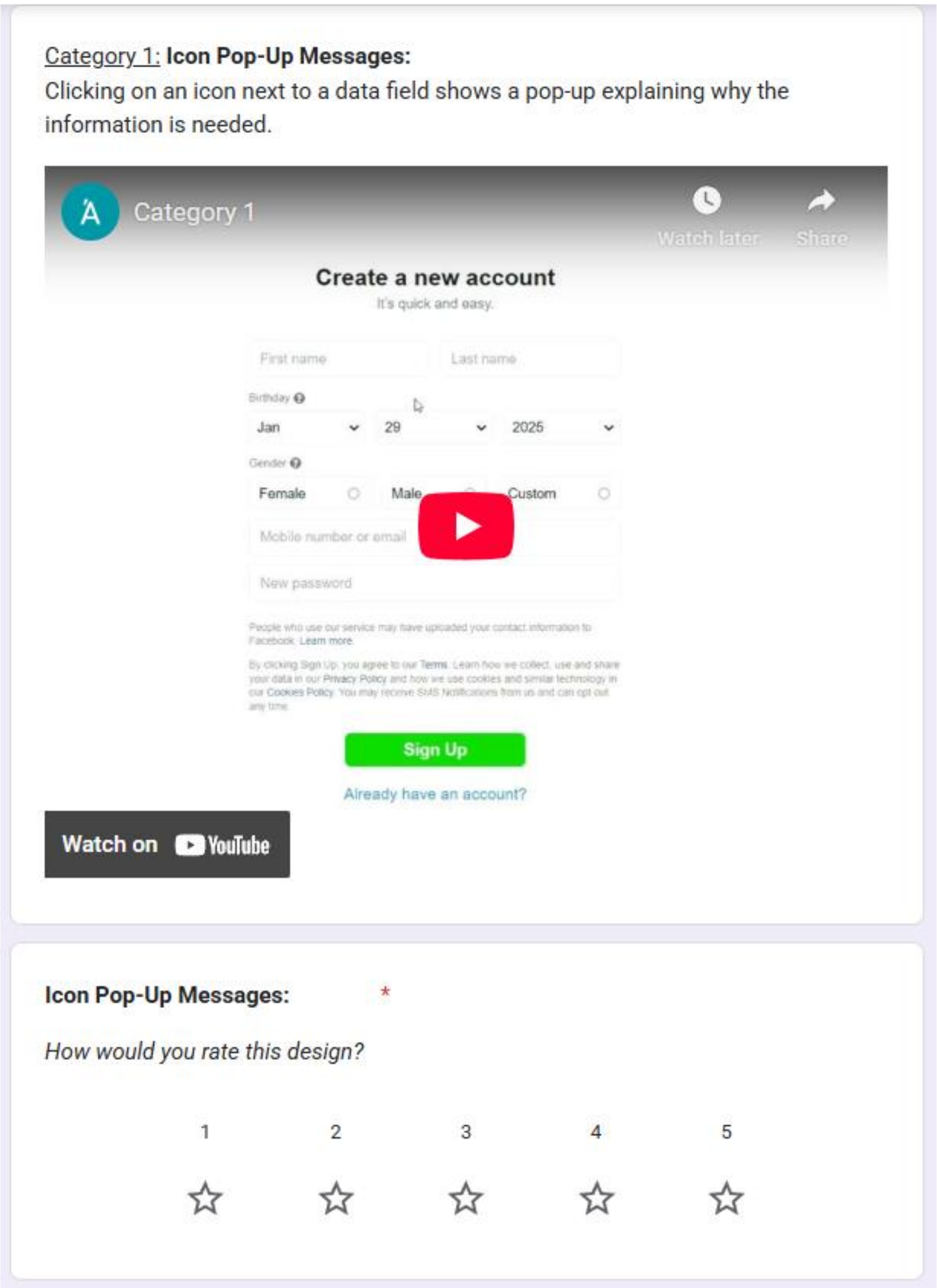


Evaluating Data Explanation Designs

Some websites request personal data without any explanation, leaving users confused and uncertain. Here's an example of a platform that does this poorly.

Now, let's see how different platforms explain why they ask for your data.

You'll rate five designs based on how clear and easy to understand they are!



Category 1: **Icon Pop-Up Messages:**
Clicking on an icon next to a data field shows a pop-up explaining why the information is needed.

Create a new account

It's quick and easy.

First name

Last name

Birthday

Jan 29 2025

Gender

Female ○ Male ○ Custom ○

Mobile number or email

New password

People who use our service may have uploaded your contact information to Facebook. Learn more.

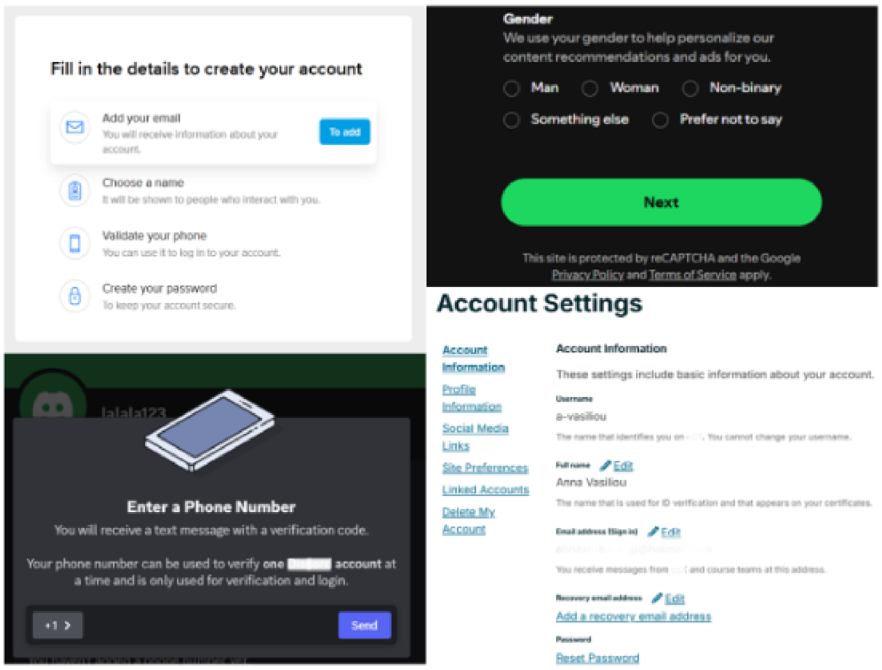
By clicking Sign Up, you agree to our Terms. Learn how we collect, use and share your data in our Privacy Policy and how we use cookies and similar technology in our Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

Icon Pop-Up Messages: *

How would you rate this design?

1	2	3	4	5
☆	☆	☆	☆	☆

Category 2: **Short Explanation Next to the Field:**
A brief reason is shown directly above, below, or beside each data field.



Fill in the details to create your account

Add your email
You will receive information about your account.
To add

Choose a name
It will be shown to people who interact with you.

Validate your phone
You can use it to log in to your account.

Create your password
To keep your account secure.

lalala123

Enter a Phone Number
You will receive a text message with a verification code.

Your phone number can be used to verify **one** [redacted] **account** at a time and is only used for verification and login.

+1 › Send

Gender
We use your gender to help personalize our content recommendations and ads for you.

○ Man ○ Woman ○ Non-binary
○ Something else ○ Prefer not to say

Next

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Account Settings

Account Information
Profile Information
Social Media Links
Site Preferences
Linked Accounts
Delete My Account

Account Information
These settings include basic information about your account.

Username
a-vasiliou
The name that identifies you on [redacted]. You cannot change your username.

Full name Edit
Anna Vasiliou
The name that is used for ID verification and that appears on your certificates.

Email address (Sign in) Edit
[redacted]
You receive messages from [redacted] and course teams at this address.

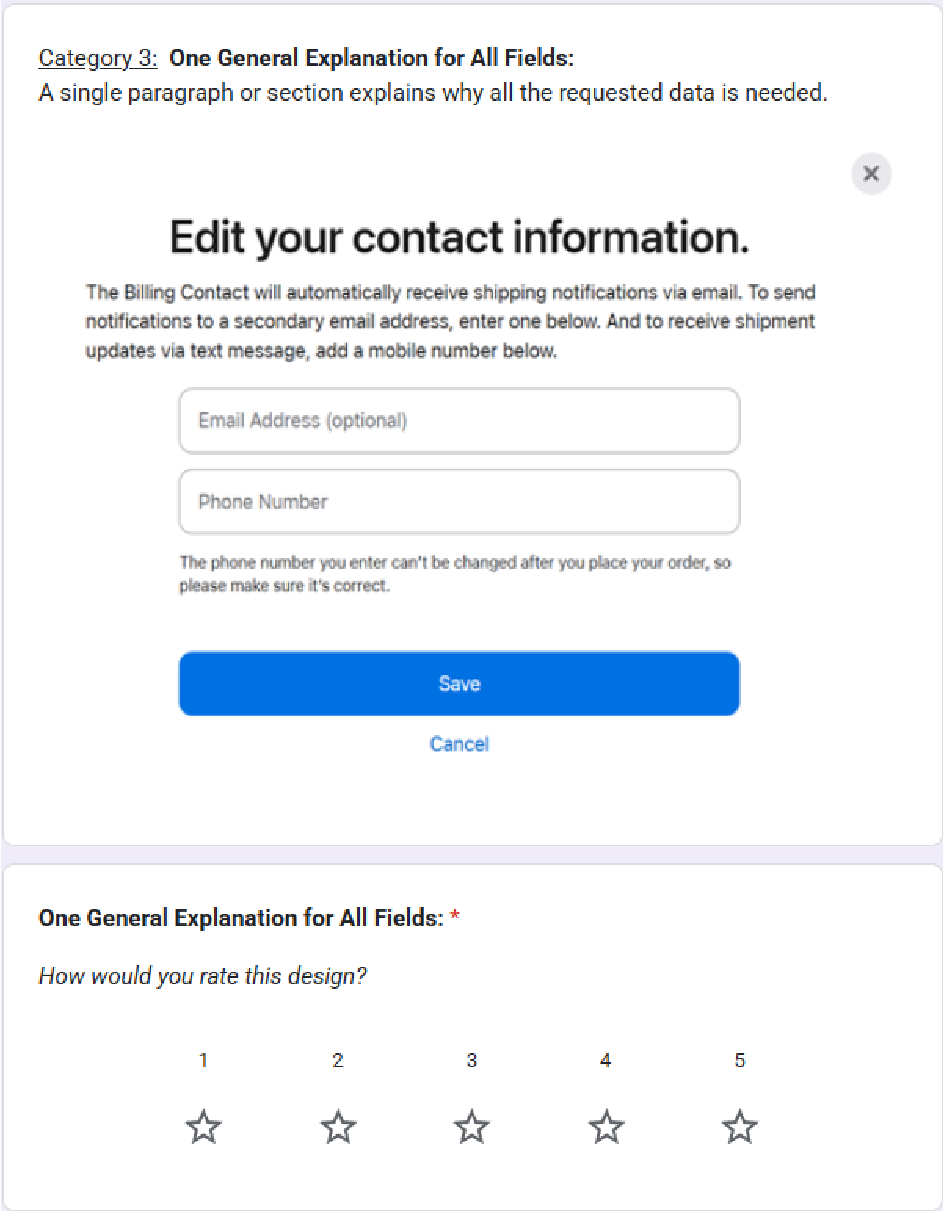
Recovery email address Edit
Add a recovery email address

Password
Reset Password

Short Explanation Next to the Field: *

How would you rate this design?

1	2	3	4	5
☆	☆	☆	☆	☆



Category 3: **One General Explanation for All Fields:**
A single paragraph or section explains why all the requested data is needed.

✕

Edit your contact information.

The Billing Contact will automatically receive shipping notifications via email. To send notifications to a secondary email address, enter one below. And to receive shipment updates via text message, add a mobile number below.

Email Address (optional)

Phone Number

The phone number you enter can't be changed after you place your order, so please make sure it's correct.

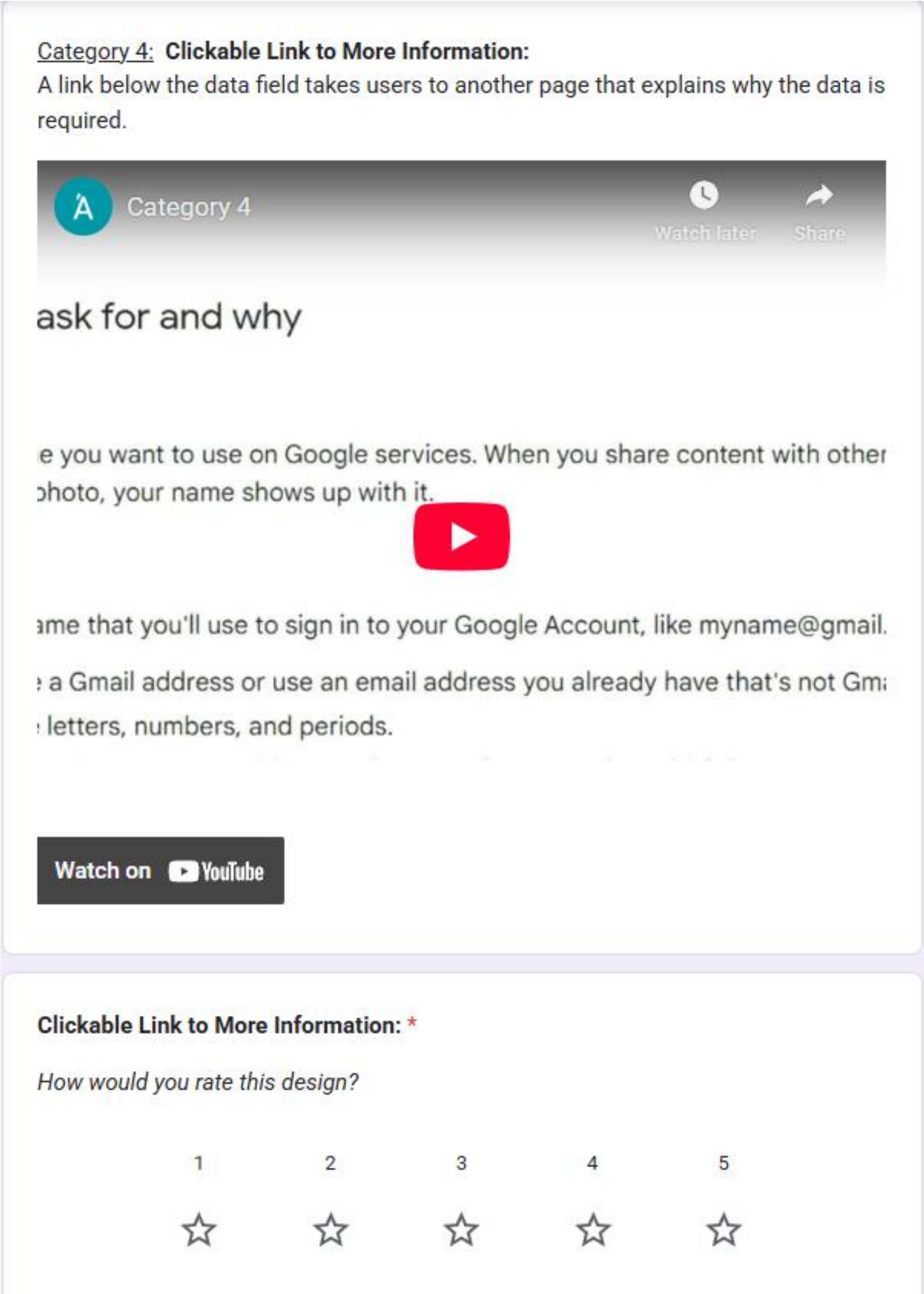
Save

Cancel

One General Explanation for All Fields: *

How would you rate this design?

1	2	3	4	5
☆	☆	☆	☆	☆



Category 4: **Clickable Link to More Information:**

A link below the data field takes users to another page that explains why the data is required.

Category 4

ask for and why

e you want to use on Google services. When you share content with other
ɔhoto, your name shows up with it.

ɪme that you'll use to sign in to your Google Account, like myname@gmail.

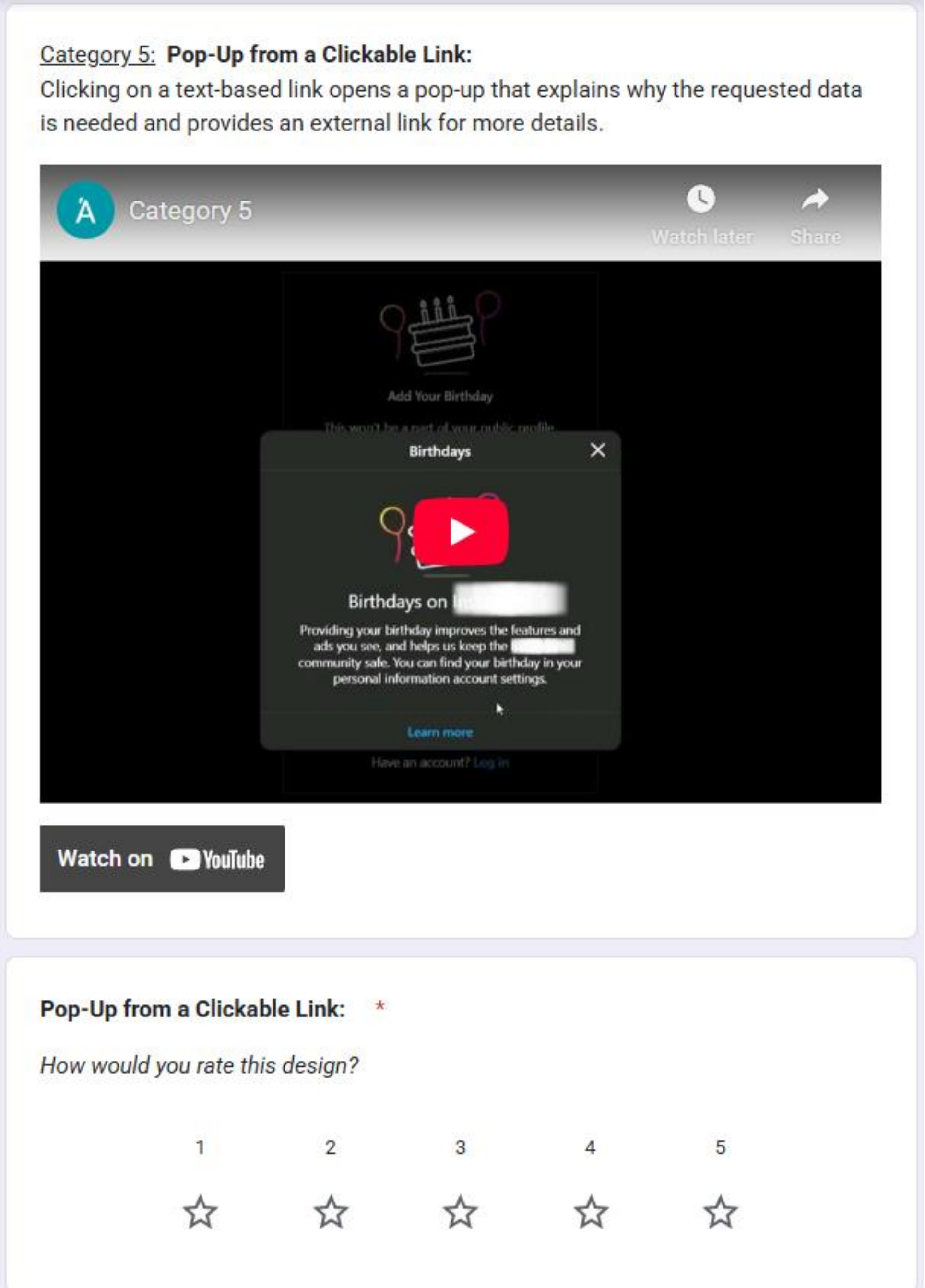
: a Gmail address or use an email address you already have that's not Gmɛ

: letters, numbers, and periods.

Clickable Link to More Information: *

How would you rate this design?

1	2	3	4	5
☆	☆	☆	☆	☆



Category 5: **Pop-Up from a Clickable Link:**
Clicking on a text-based link opens a pop-up that explains why the requested data is needed and provides an external link for more details.

Add Your Birthday

This won't be a part of your public profile.

Birthdays

Birthdays on [redacted]

Providing your birthday improves the features and ads you see, and helps us keep the [redacted] community safe. You can find your birthday in your personal information account settings.

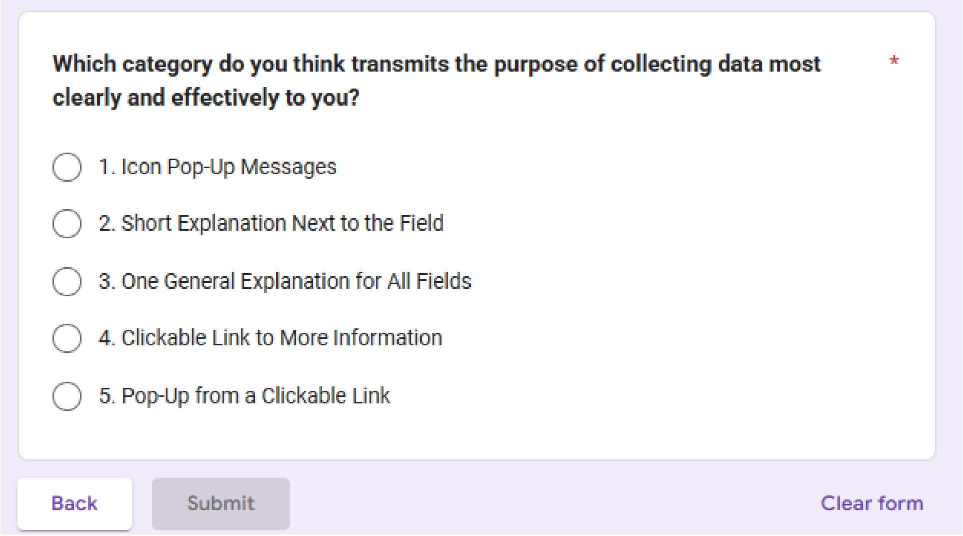
Learn more

Have an account? Log in

Pop-Up from a Clickable Link: *

How would you rate this design?

1	2	3	4	5
☆	☆	☆	☆	☆



Which category do you think transmits the purpose of collecting data most clearly and effectively to you? *

○ 1. Icon Pop-Up Messages

○ 2. Short Explanation Next to the Field

○ 3. One General Explanation for All Fields

○ 4. Clickable Link to More Information

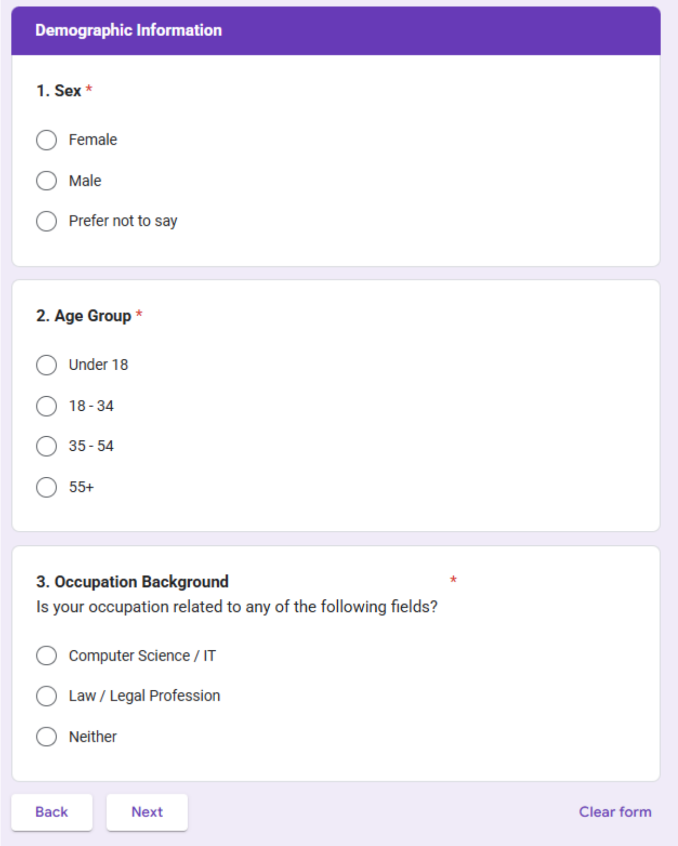
○ 5. Pop-Up from a Clickable Link

The survey did not include open-ended questions or comment fields for qualitative input. Instead, it prioritized quantitative responses to facilitate direct comparison between the presented design approaches.

4.3.2 Participants

The survey was distributed through academic channels and social networks in order to reach a broad and diverse audience. Participants were not restricted to any specific group, but rather included individuals from a range of age groups, educational backgrounds, and occupational domains. The survey included a demographic section in which participants were asked to indicate:

- Their age group (Under 18, 18–34, 35–54, or 55+)
- Their sex
- Whether their occupation was related to Computer Science/IT, Law/Legal professions, or neither



Demographic Information

1. Sex *

○ Female

○ Male

○ Prefer not to say

2. Age Group *

○ Under 18

○ 18 - 34

○ 35 - 54

○ 55+

3. Occupation Background *

Is your occupation related to any of the following fields?

○ Computer Science / IT

○ Law / Legal Profession

○ Neither

These demographic questions were used to ensure that responses could be interpreted in the context of the user's background and familiarity with privacy and technology-related issues.

This diversity was essential to the study's objectives. Users' expectations regarding transparency and privacy are shaped by their prior experience with online platforms and their exposure to data protection practices. Including both tech-savvy users and general internet users allowed for a more comprehensive understanding of how different design strategies are perceived across user segments. This, in turn, supports the development of form designs that are effective and understandable for a wide audience, not just those familiar with legal or technical contexts [16].

4.3.3 Data Collection

The data was collected automatically through Google Forms platform over a period of several days. A total of 91 valid responses were recorded. All participants completed the survey online, evaluating five distinct design patterns for transparency in form design using a structured set of rating scales [16].

Each response included:

- Five individual ratings (one per design), using a 5-point Likert scale
- A final multiple-choice selection indicating which design the participant found most effective overall

The quantitative format of the questionnaire ensured that the data was immediately suitable for quantitative analysis. Ratings were aggregated to calculate average clarity scores for each design, and the most frequently selected "best overall" design was identified from the final preference question. These results formed the basis for determining which design approaches would be advanced into prototype development, as discussed in the following sections.

4.4 Findings

The questionnaire collected 91 responses, with demographic diversity across age, gender, and occupational backgrounds. This diversity allowed us to gather user preferences that reflect a wide range of experiences and expectations regarding online data collection transparency.

4.4.1 Participant Profile

- Gender: 52.7% of participants identified as female, 46.2% as male, and 1.1% preferred not to say (Figure 4.1).
- Age: A significant majority (83.5%) were aged 18–34, followed by 13.2% aged 35–54, and a small percentage aged under 18 or 55+ (Figure 4.2).
- Occupational Background: 46.2% of participants reported working in Computer Science/IT, 4.4% in Law/Legal professions, and the remaining 49.5% in unrelated fields (Figure 4.3).

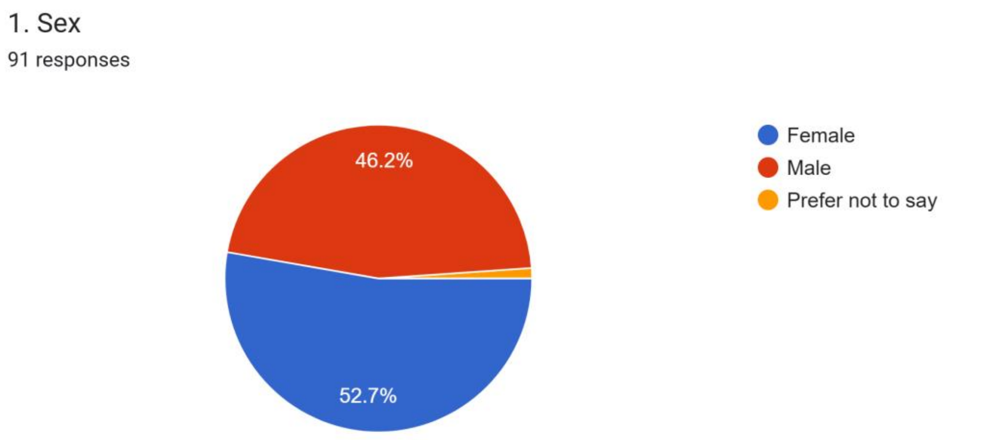


Figure 4.1

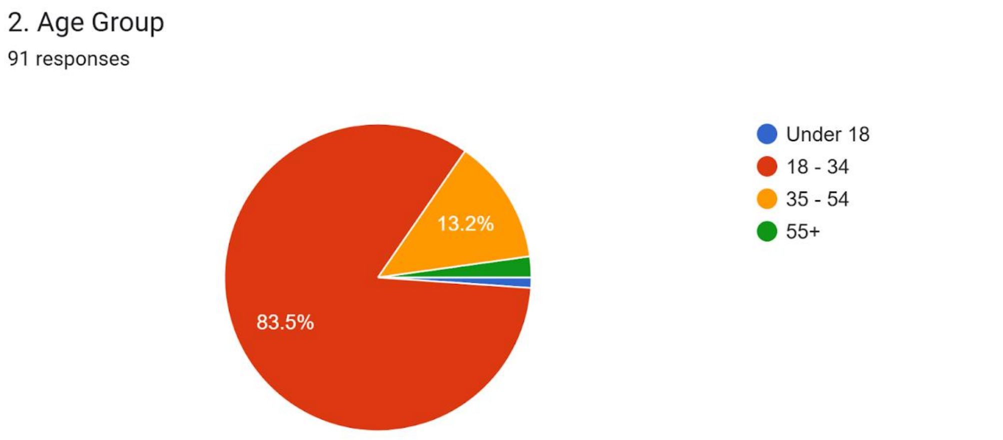


Figure 4.2

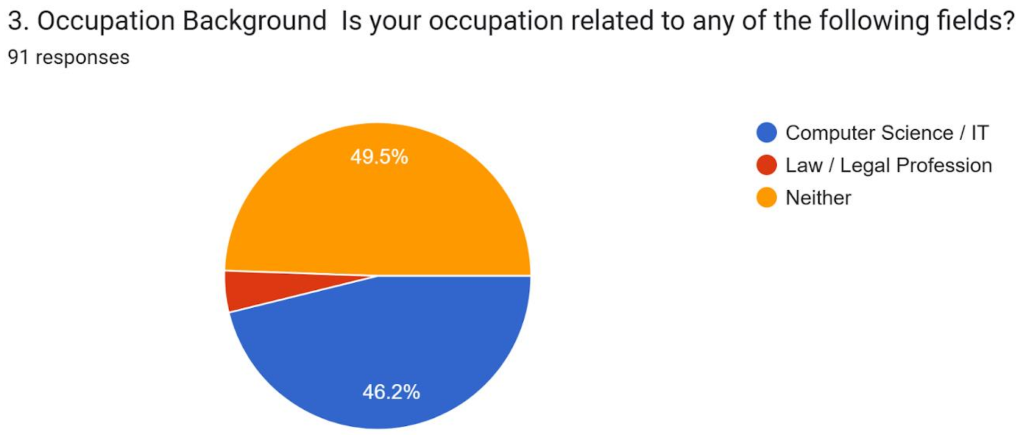


Figure 4.3

4.4.2 Design Ratings

Participants were shown five design categories representing different ways of explaining the purpose of data collection. They rated each on a 5-point scale (1 = Not clear at all, 5 = Very clear and effective):

Design Category	Average Rating
Short Explanation Next to the Field	4.44
Icon Pop-Up Messages	3.88
Pop-Up from a Clickable Link	3.68
One General Explanation for All Fields	3.64
Clickable Link to More Information	3.27

The design with the highest average rating was Short Explanation Next to the Field (4.44) (Figure 4.4), followed by Icon Pop-Up Messages (3.88) (Figure 4.5). These two formats were consistently perceived as the clearest and most user-friendly approaches for transmitting purpose information directly during form filling.

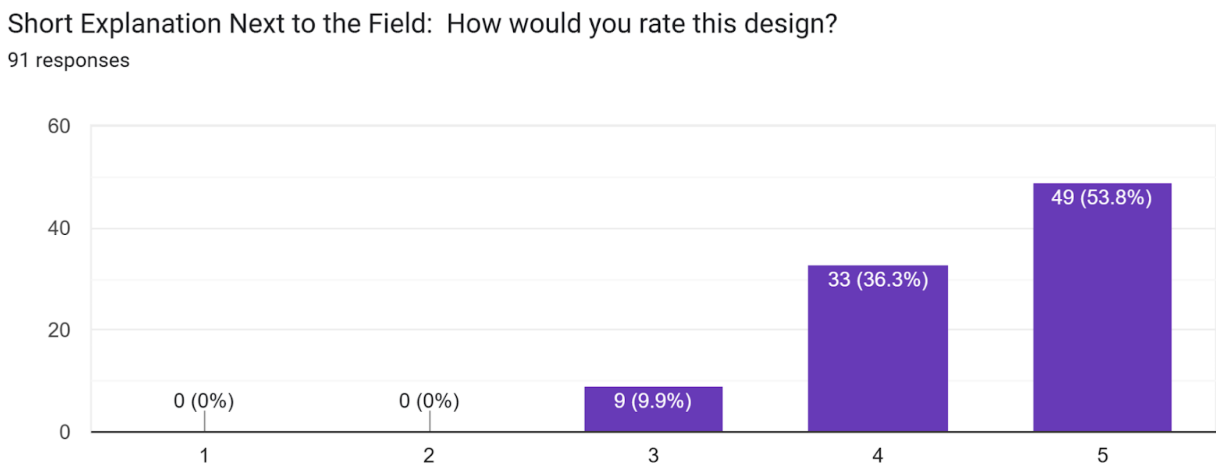


Figure 4.4

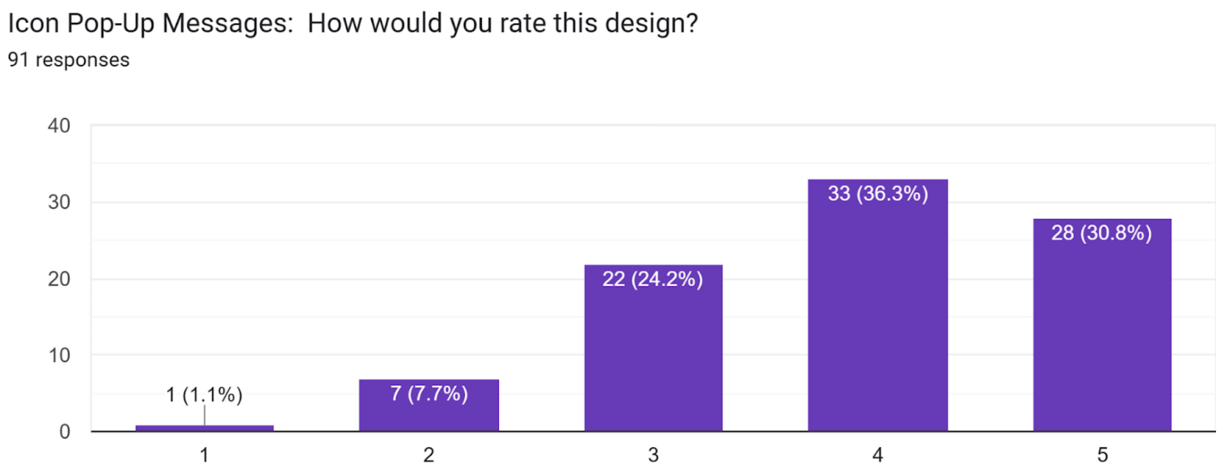


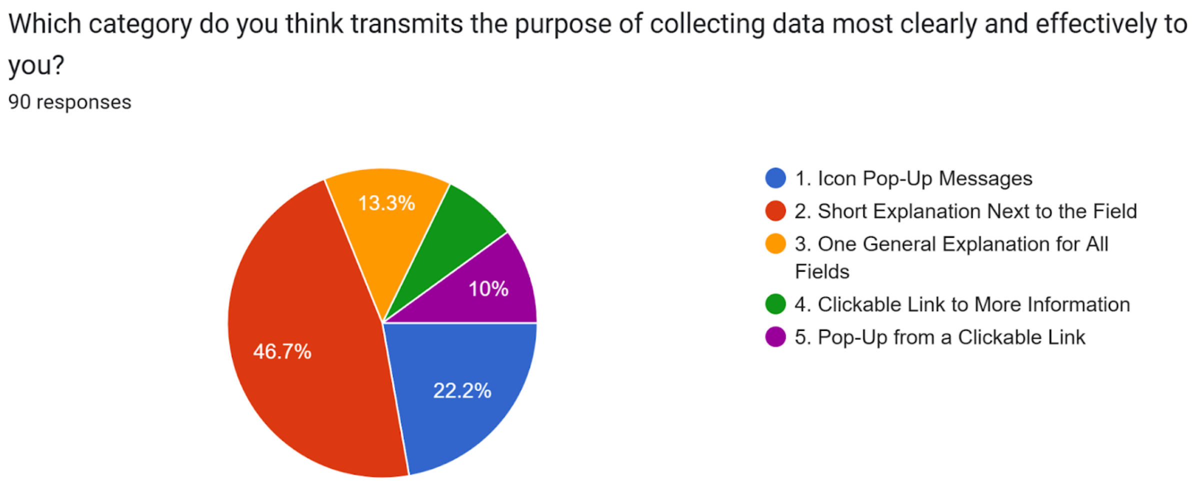
Figure 4.5

4.4.3 Preferred Overall Design

When asked to select the single most effective design, participants responded as follows: (Figure 4.6)

- Short Explanation Next to the Field: 46.7%
- Icon Pop-Up Messages: 22.2%
- One General Explanation for All Fields: 13.3%
- Pop-Up from a Clickable Link: 10%
- Clickable Link to More Information: 7.8%

These results reaffirm the importance of integrating purpose explanations directly within or next to the relevant input fields. Users preferred immediate, concise context over indirect or external information sources (such as links to other pages).



Which category do you think transmits the purpose of collecting data most clearly and effectively to you?

90 responses

Figure 4.6

4.4.4 Conclusion from Results

Based on the quantitative responses, the study identified the two most effective design strategies:

1. Short Explanation Next to the Field
2. Icon Pop-Up Messages

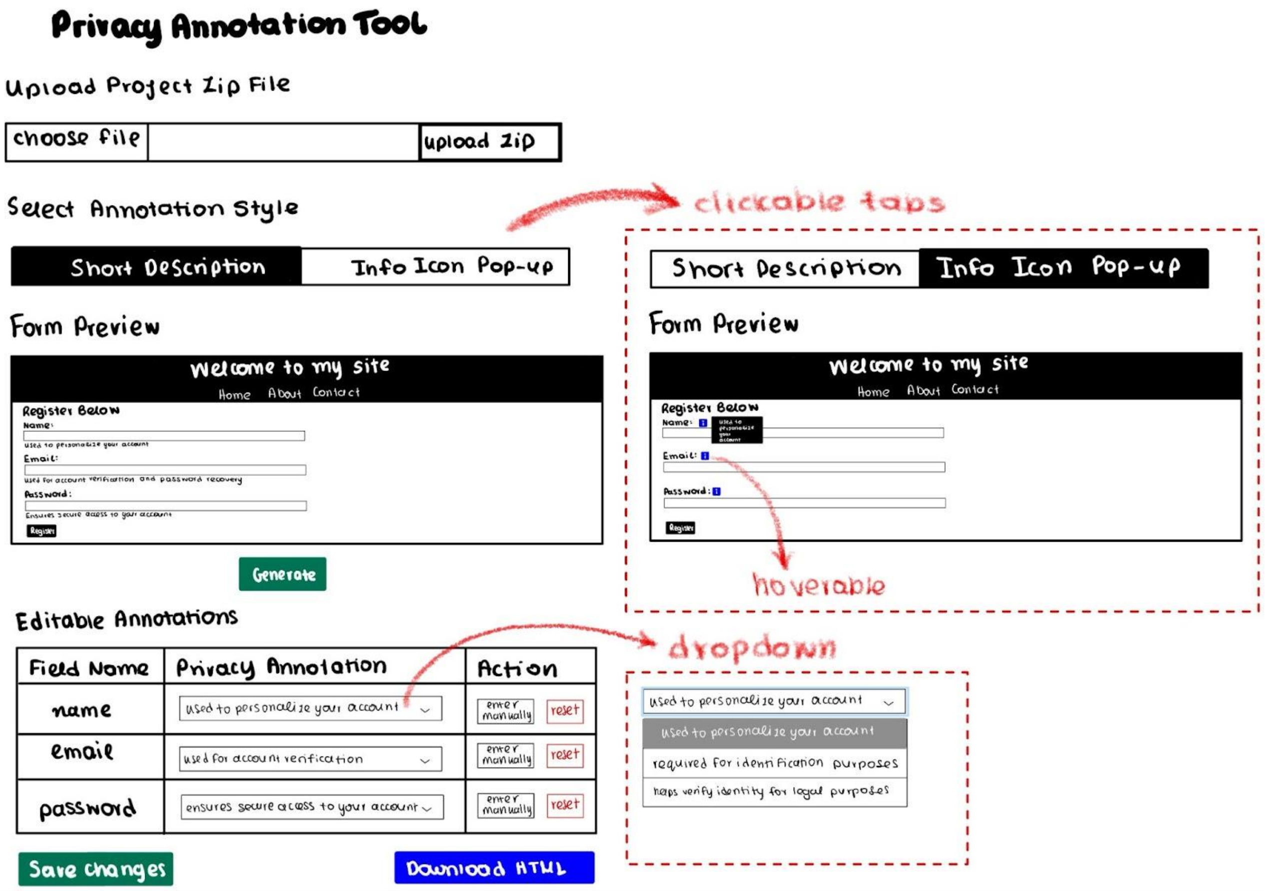
These two were selected for further development in the prototyping phase, as they balance clarity, non-intrusiveness, and practical implementation feasibility within web form design. The full set of questionnaire results, including detailed response distributions and participant breakdowns, is provided in **Appendix A**.

4.5 Prototype Development

Following the analysis of user preferences, the two most effective designs—Short Explanation Next to the Field and Icon Pop-Up Messages—were selected for prototype development. Both low- and high-fidelity prototypes were created to visualize how these strategies could be integrated into real-world form designs.

4.5.1 Low-Fidelity Prototypes

Initial sketches were created using a digital tablet to explore the layout, content placement, and interaction flow of the form. The wireframes focused on the positioning of purpose explanations near input fields, maintaining visual balance and spacing, and clearly labeling icons. These early designs served as a flexible foundation for refining ideas before moving to high-fidelity prototypes (Figure 4.7).

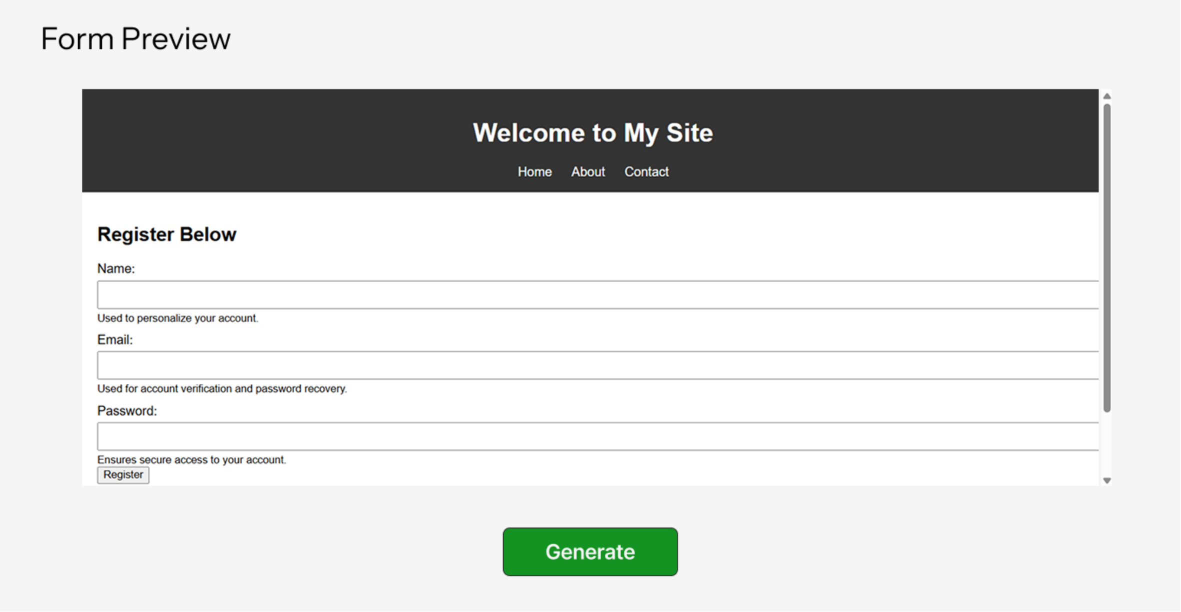


Field Name	Privacy Annotation	Action
name	used to personalise your account	enter manually · reset
email	used for account verification	enter manually · reset
password	ensures secure access to your account	enter manually · reset

Figure 4.7

4.5.2 High-Fidelity Prototypes

To bring the transparent form concepts closer to a real-world interface, high-fidelity prototypes were developed using Figma. These polished designs featured consistent visual styling in terms of color palette, typography, and iconography, ensuring a cohesive and professional appearance. Interactive behaviors were simulated to reflect realistic user interactions, such as pop-up messages triggered by hovering over or clicking on icons. Additionally, layouts were designed with responsiveness in mind, allowing the forms to adapt effectively across both desktop and mobile screen sizes. These prototypes aimed to faithfully represent how the final tool would look and function within a live web environment (Figure 4.8).



Form Preview

Welcome to My Site

Register Below

Name:

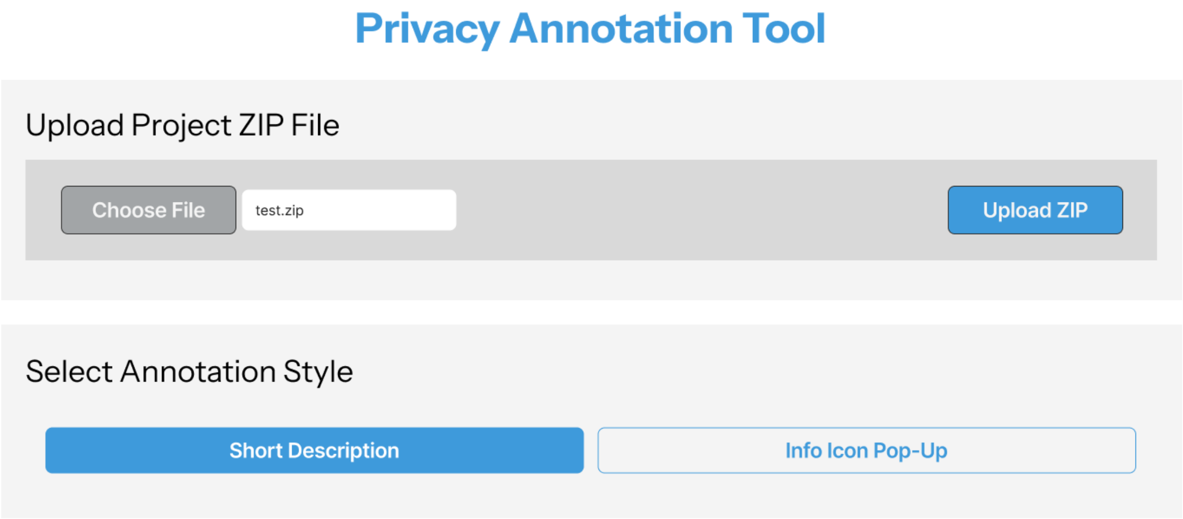
Used to personalize your account.

Email:

Used for account verification and password recovery.

Password:

Ensures secure access to your account.

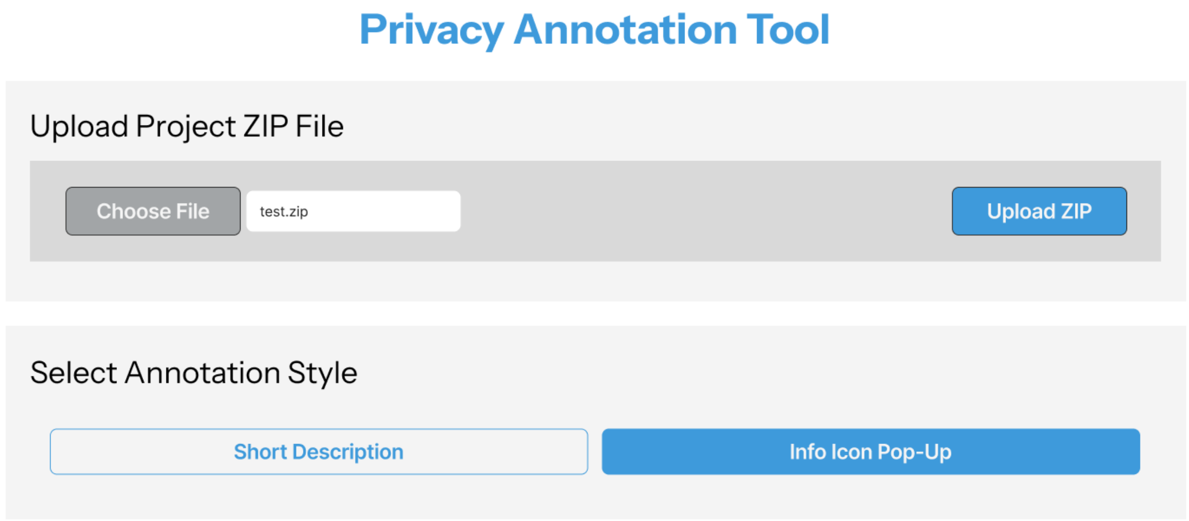


Privacy Annotation Tool

Upload Project ZIP File

test.zip

Select Annotation Style

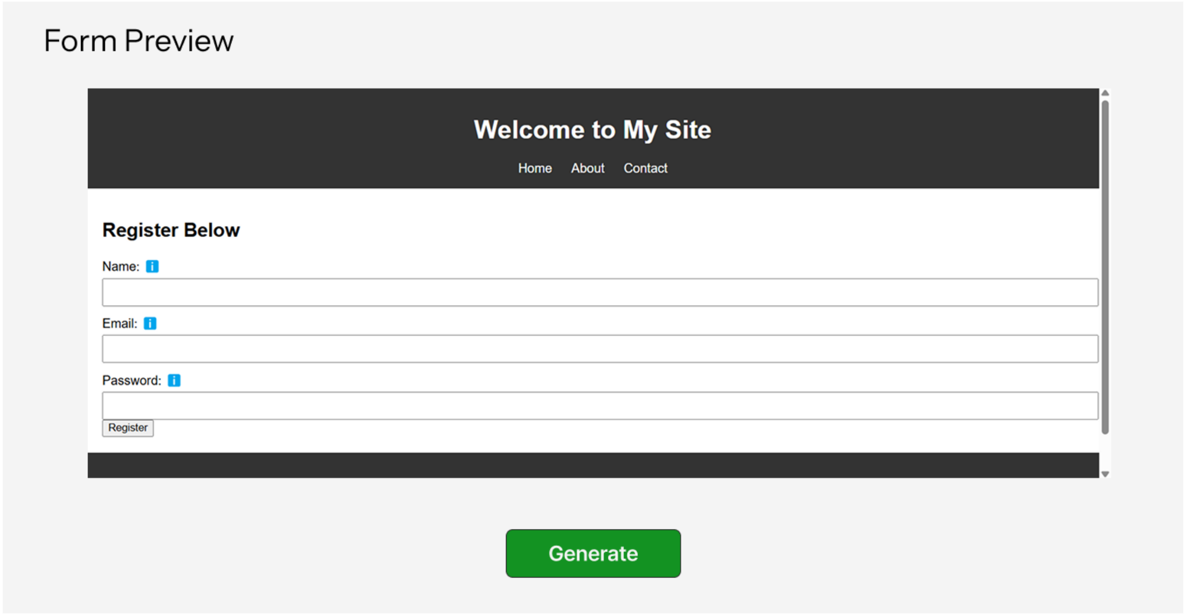


Privacy Annotation Tool

Upload Project ZIP File

test.zip

Select Annotation Style



Form Preview

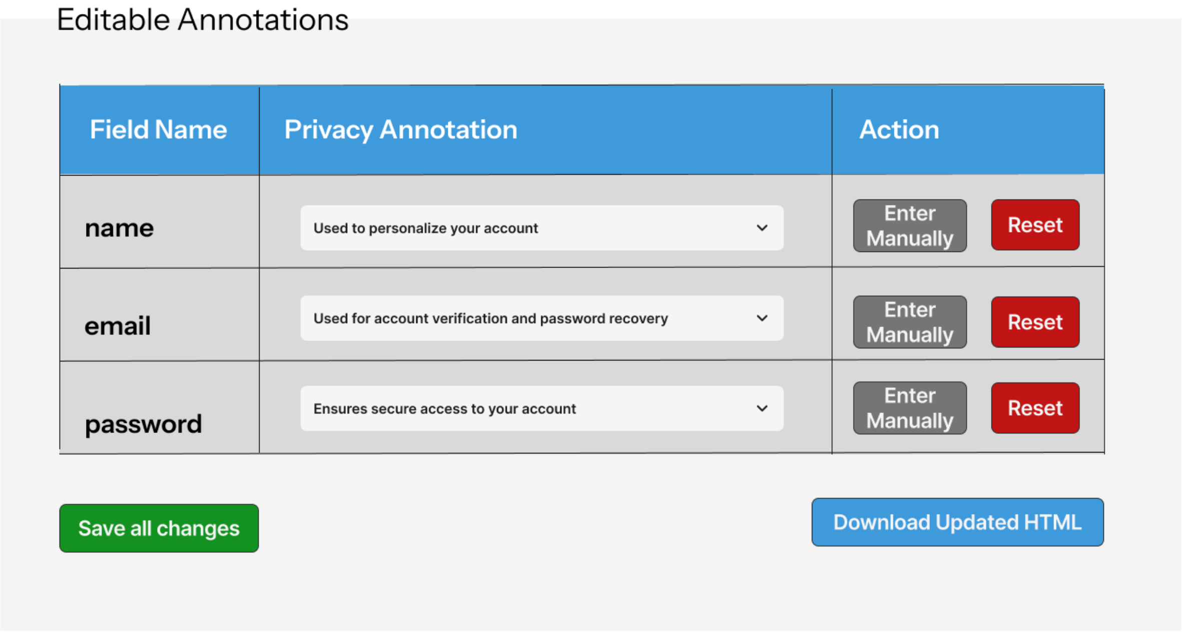
Welcome to My Site

Register Below

Name:

Email:

Password:



Editable Annotations

Field Name	Privacy Annotation	Action
name	Used to personalize your account	Enter Manually Reset
email	Used for account verification and password recovery	Enter Manually Reset
password	Ensures secure access to your account	Enter Manually Reset

Figure 4.8

4.6 Conclusion

Through a user survey, it was found that participants favored form designs that provided brief, context-specific explanations placed near data fields or presented via icons. Low and high-fidelity prototypes incorporating these elements were then created to reflect the most preferred approaches. While full evaluation of their effectiveness will follow, this exploratory phase highlights the importance of transparency in shaping user perceptions and supporting compliance with data protection regulations.

Chapter 5

5. Creating and Validating a Database of Processing Purposes Annotations

This chapter presents the process of constructing a structured database of personal data processing purposes annotation suggestions for common personal data fields in web forms. Drawing on the research and findings discussed in previous chapters, we compiled a set of three possible annotation options per field, each aiming to clarify the purpose of data collection in a transparent and user-friendly manner. To evaluate the ***clarity****,* ***appropriateness****, and* ***relevance*** of these proposed descriptions, we conducted a qualitative survey targeting two key stakeholder groups: legal experts (including law students) and technical experts (such as web developers and software engineers). Their feedback was used to assess the quality of the suggested processing purposes annotations according to these three dimensions.

5.1 Database Construction

To support transparency and informed consent in web forms, a curated database of privacy annotation suggestions was created. Each annotation consists of a short, human-readable description of the potential purpose behind the collection of a particular data field. The goal was to offer users a clear understanding of why specific personal data is requested, helping them make more informed privacy decisions. This database will constitute an important part of the tool developed in this thesis, used to annotate web forms fields with purposes.

The construction of the database was grounded in findings from privacy regulations (such as the GDPR), our UX research, and common industry practices. For each input field typically found in registration or profile forms, three potential purpose descriptions were drafted. These were aiming to reflect both legal expectations and user-centered design principles.
The database is shown below in a table (Figure 5.1).

Input Field	**Possible Purpose Descriptions**
Full name	- Used to personalize your account. - Required for identification purposes. - Helps verify identity for legal purposes.
Email Address	- Used for account verification and password recovery. - For sending notifications and updates. - Required for communication with customer support.
Phone number	- Used for two-factor authentication. - For account recovery and security notifications. - Can be used for marketing SMS and promotions.
Username	- Unique identifier for your account. - Displayed in forums or online interactions. - Used for logging into the platform.
Password	- Ensures secure access to your account. - Used for authentication and data protection. - Required to prevent unauthorized access.
Date of Birth	- Used to verify age eligibility. - Helps personalize content recommendations. - Used for birthday discounts and rewards.
Gender	- Used for demographic insights and analytics. - May be required for personalized experiences.

	- Helps customize product recommendations.
Address	- Used for shipping and delivery. - Required for billing and invoicing. - Needed for identity verification in some cases.
City	- Used to tailor location-based services. - Needed for address verification. - Helps provide region-specific offers.
State/Province	- Used for geographical analysis. - Required for accurate shipping calculations. - Needed for taxation purposes.
Postal code	- Ensures accurate delivery of physical items. - Needed for regional tax calculations. - Helps suggest nearby service providers.
Country	- Determines applicable laws and policies. - Helps customize content based on location. - Used for currency and language settings.
Profile picture	- Used to personalize your profile. - Displayed in user interactions and forums. - Helps recognize user identity in social spaces.
Security question	- Used for account recovery. - Provides additional security verification. - Ensures an extra layer of protection against hacking.
Company name	- Used for business-related account setup. - May be required for invoicing purposes. - Helps in verifying corporate affiliations.
Job title	- Used for networking and professional insights. - Helps tailor industry-specific content. - Displays role in business-related applications.
Website URL	- Displayed on your profile for others to visit. - Used for verifying business or personal sites. - Required for linking personal portfolios.

Social media links	- Used for connecting accounts and sharing content. - Displayed on profile pages for networking. - Allows integration with third-party apps.
Newsletter subscription	- Used to send promotional emails and updates. - Allows users to receive relevant content. - Helps businesses track user engagement.
Payment Information	- Required for processing transactions. - Used for billing and subscription services. - Ensures seamless automatic payments.

Figure 5.1

In total, the database includes annotations for 20 personal data fields, such as username, password, gender, address, and social media links. Each set of suggestions aimed to balance clarity, legal appropriateness, and relevance to real websites—the same criteria later used for evaluation in the study presented in the following section.

5.2 Evaluation Methodology

To assess the clarity, appropriateness, and relevance of the proposed processing purposes annotations, aiming to validate our database, a mixed method (quantitative and qualitative) survey was designed and distributed to two distinct expert groups: web developers (or software engineers) and legal experts. These participant categories were selected based on their practical and theoretical understanding of either user interface design and implementation, or privacy, consent, and data protection regulations.

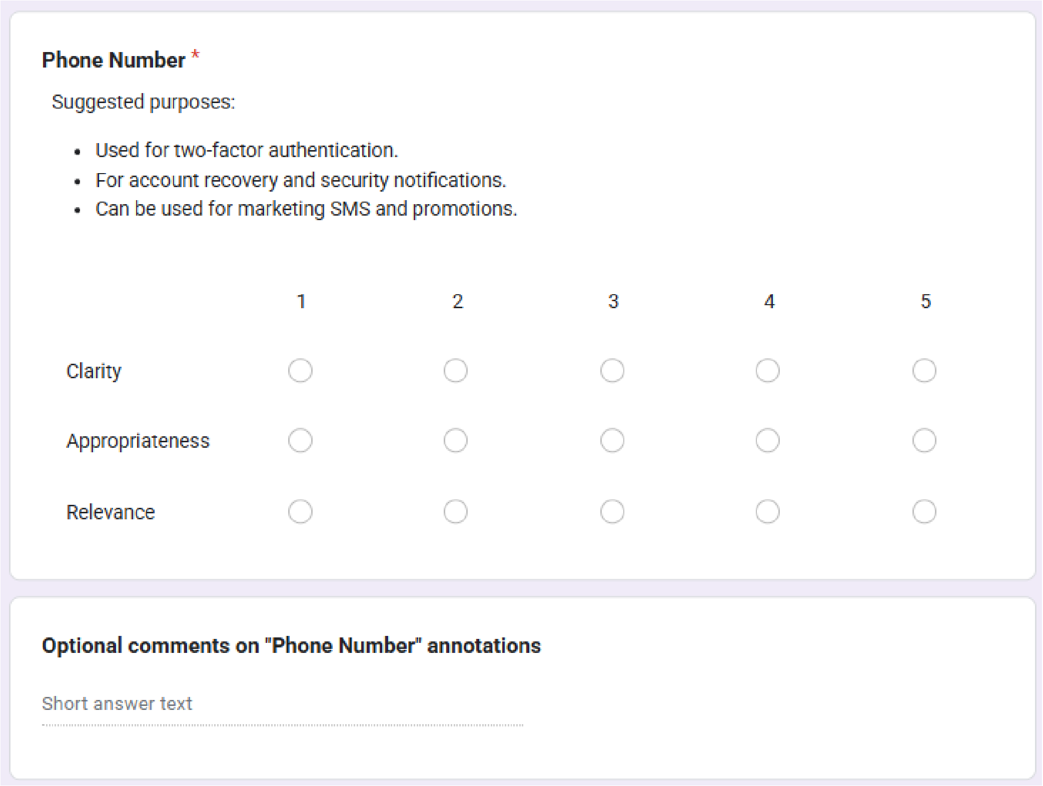
The primary objective of the survey was to validate the suggested purpose descriptions for each personal data field in a form. The questionnaire contained the 20 personal data fields, each accompanied by the three proposed purpose descriptions. Participants were asked to rate each set of descriptions based on three evaluation criteria:

- **Clarity:** How clearly are the purposes stated?
- **Appropriateness:** Do the purposes align with legal/ethical expectations for this data type?
- **Relevance:** Are the purposes directly related to the way such data are used in web platforms?

A 5-point Likert scale was used for each criterion, with the following values:

- 1 = Poor
- 2 = Fair
- 3 = Neutral
- 4 = Good
- 5 = Excellent

Figure 5.2 shows an example of how a typical question was structured in the survey. The full questionnaire is presented in Appendix B. For each field, participants were shown three proposed purpose descriptions and asked to evaluate them across the criteria of clarity, appropriateness, and relevance.



Phone Number *

Suggested purposes:

- Used for two-factor authentication.
- For account recovery and security notifications.
- Can be used for marketing SMS and promotions.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Phone Number" annotations

Short answer text

Figure 5.2 - Example survey question for the "Phone Number" field, including purpose suggestions and a 5-point evaluation scale.

Participants also had the option to provide open-ended feedback after each field, allowing for qualitative insights and suggestions for improvement.

The survey was implemented using Google Forms and began with a mandatory consent form. Participants were informed about the research objectives, their right to withdraw at any time, and the anonymous nature of their responses. Consent was explicitly requested before they could proceed.

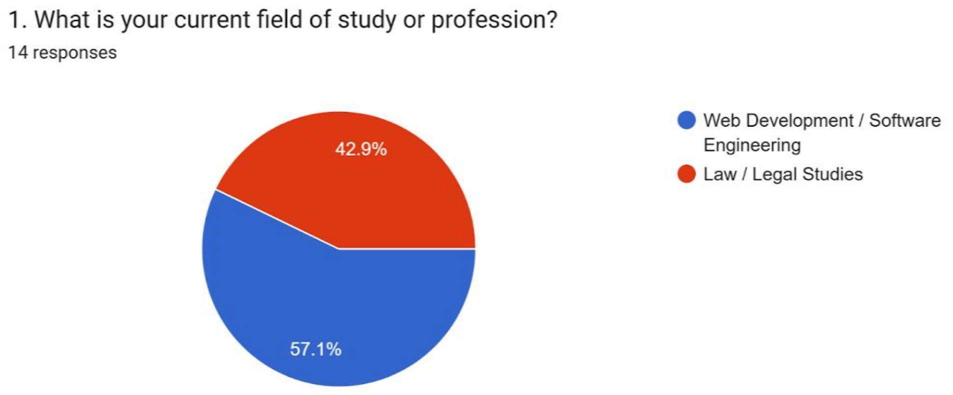
A total of 14 individuals completed the survey, representing a balanced mix of technical and legal backgrounds. Their feedback forms the basis of the analysis in the next section.

5.3 Results and Key Findings

A total of 13 participants completed the survey. These included 5 respondents from legal backgrounds (law students or professionals) and 8 from technical fields (web developers or software engineers). The participants were specifically selected to provide expert perspectives from both regulatory and implementation standpoints. We opted for quality, meaningful feedback from a lower number of experts, rather than a large number of plain quantitative responses from a diverse population.

5.3.1 Participant Profile

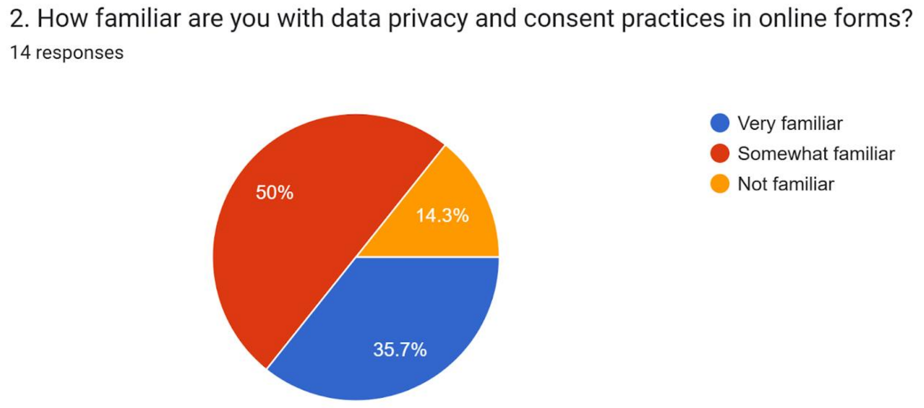
As shown in Figure 5.3, **57.1%** of respondents were from technical fields (Web Development / Software Engineering) and **42.9%** from law-related fields (Law / Legal Studies). Additionally, most participants reported at least some familiarity with data privacy and consent practices. Specifically, **35.7%** identified as "very familiar," **50%** as "somewhat familiar," and **14.3%** as "not familiar" (Figure 5.4).



1. What is your current field of study or profession?

14 responses

Figure 5.3 – Distribution of participant fields of study/profession



2. How familiar are you with data privacy and consent practices in online forms?

14 responses

Figure 5.4 – Familiarity with data privacy and consent practices

5.3.2 Quantitative Findings

Each participant rated the clarity, appropriateness, and relevance of the annotation suggestions for 20 commonly collected personal data fields using a 5-point Likert scale (1 = Poor, 5 = Excellent).

Overall, the annotations received consistently high scores in the **Clarity** and **Relevance** categories, while **Appropriateness** occasionally showed more variation - especially among legal respondents. Among all fields, **Username** received the highest overall average rating with a score of **4.69**, closely followed by **Password**, which achieved an average score of **4.64**. Both fields were considered clear, appropriate, and relevant by the vast majority of participants.

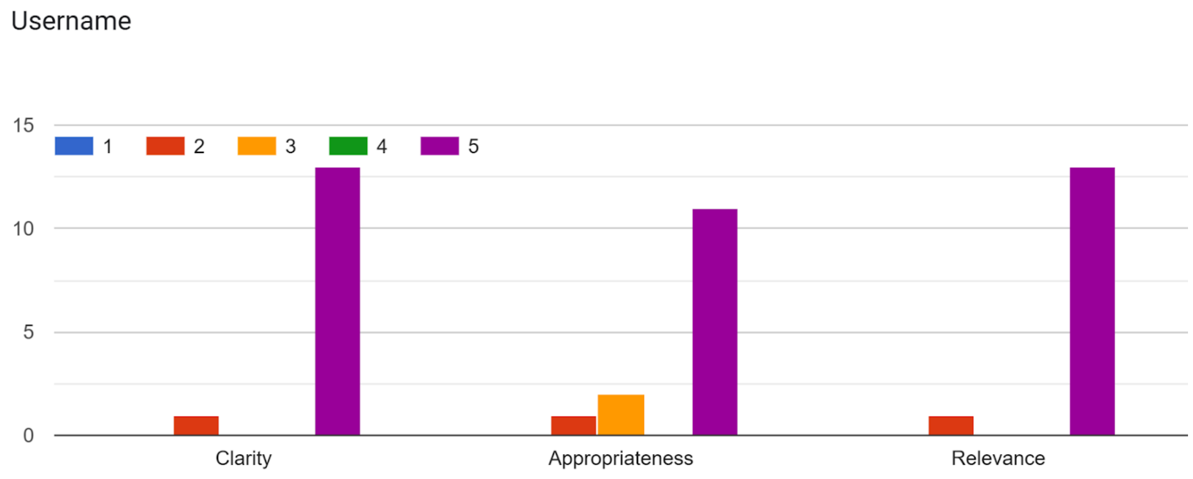


Figure 5.5 – Ratings for Username annotations

Bar chart showing participant ratings for the Username field across Clarity, Appropriateness, and Relevance. Responses are strongly concentrated in the 4–5 range, indicating high clarity and contextual fit.

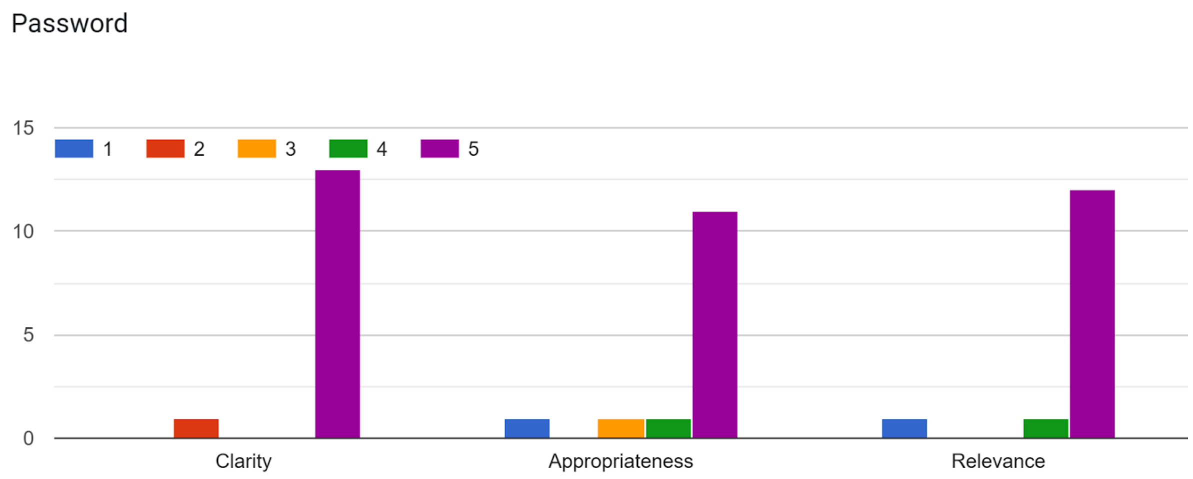


Figure 5.6 – Ratings for Password annotations

Participant feedback on the Password field also showed high ratings across all three evaluation criteria, reflecting strong agreement on the usefulness and adequacy of the suggested purposes.

These two figures demonstrate the high level of agreement among participants regarding the clarity, relevance, and appropriateness of the **Username** and **Password** annotations. Ratings were concentrated at the upper end of the scale, suggesting these descriptions were perceived as both accurate and contextually appropriate.

In contrast, the following figures highlight cases where participant evaluations were more varied - particularly in terms of appropriateness. The **Email Address** and **Phone Number** fields, shown in Figures 5.6 and 5.7, received slightly lower or more dispersed scores in that category. This variation may reflect concerns about how such data could be used beyond the stated purposes, especially in relation to marketing or third-party communication.

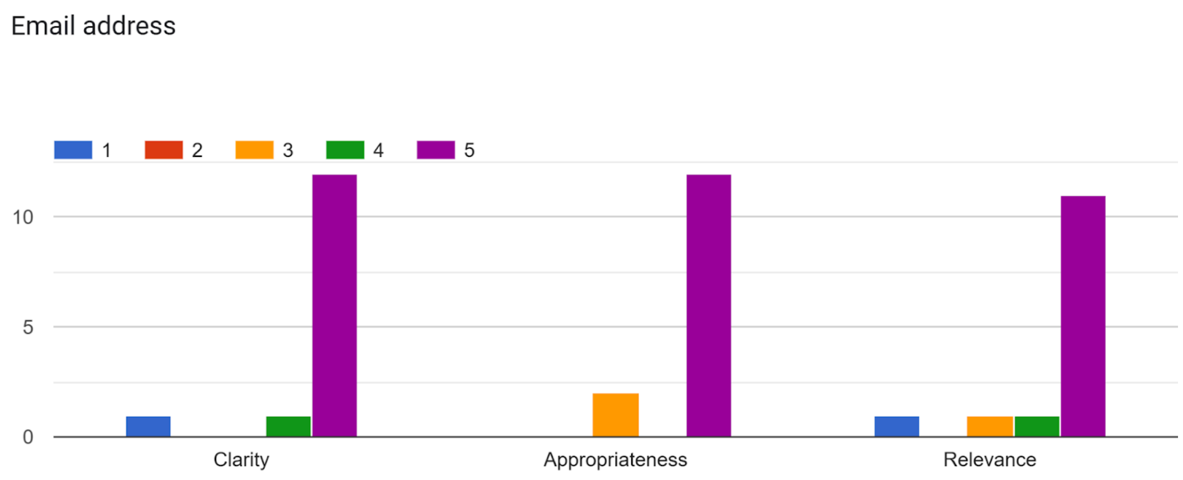


Figure 5.7 – Ratings for Email Address annotations

While Email Address received generally positive ratings for clarity and relevance, Appropriateness saw more variation, suggesting uncertainty about how email data may be used or shared.

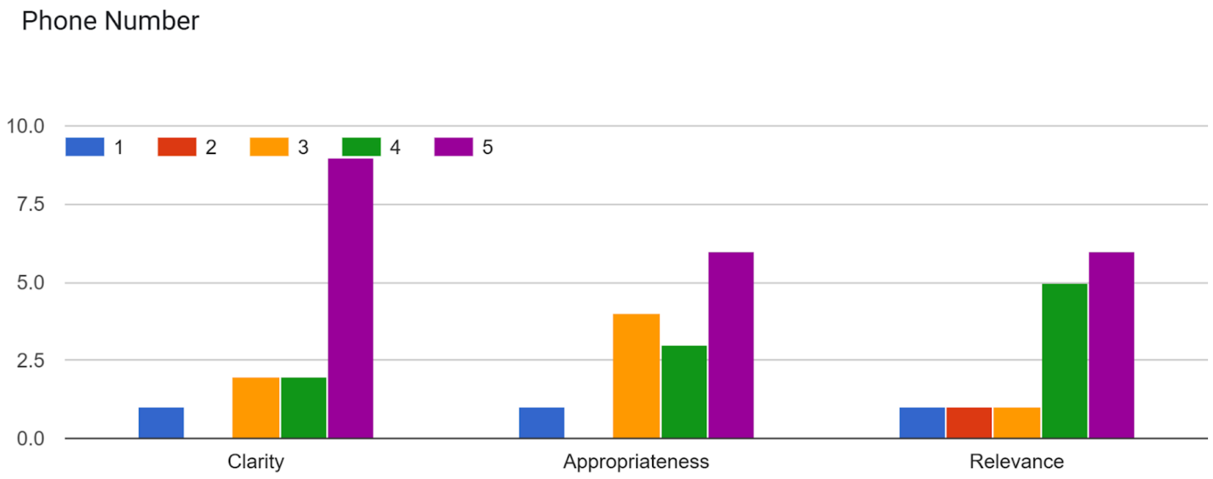


Figure 5.8 – Ratings for Phone Number annotations

The Phone Number field displayed slightly lower consistency in appropriateness ratings, potentially due to annotations referencing marketing or SMS use, which some respondents viewed as questionable or context-dependent. The full set of questionnaire responses, including ratings for all fields, is available in Appendix C.

5.3.3 Qualitative Feedback and Observed Themes

Optional comment boxes placed after each field allowed participants to provide qualitative feedback. Key observations include:

- Several respondents expressed uncertainty about the legal appropriateness of certain annotations (e.g., for phone number and email), with comments such as:
  "I am not sure about appropriateness."
- Others affirmed the usefulness of the annotations, saying:
  "Relevant for personalization and vital for identification."
  "If there is need for communication with the user it is needed."

From the final open-ended questions, several themes emerged:

- Participants appreciated the simplicity and clarity of the suggestions.
- One notable improvement suggestion was:
  "It's best to show uses of the collected data briefly on the form rather than in the privacy policy page."

This feedback suggests that while the annotations are generally well-received, contextual placement and phrasing play an important role in how users evaluate their value and trustworthiness.

5.3.4 Suggested Improvements Based on Responses

Based on the results and feedback, the following enhancements were considered for the creation of the final version of the annotation database:

Revising "appropriateness"-flagged annotations to include clearer legal grounding or more cautious wording (e.g., avoiding marketing references without consent). For instance, the annotation for **Phone Number** will be rephrased to avoid implications of unsolicited marketing, emphasizing its use for security-related communication with user consent. Similarly, the **Gender** field—which received the lowest overall scores in appropriateness and relevance—will be rephrased or marked as optional unless directly relevant to the form's purpose. For fields like **Profile Picture**, where comments indicate low perceived necessity, the description will be updated to clarify that it is used for personalization in social or community contexts only when applicable.

Additional refinements include clarifying fields such as **State/Province** and **Company Name**, where participants questioned their relevance. These will be adjusted to highlight use in region-specific services or business-related contexts. The annotation for **Social Media Links** will also be revised to reflect that integration is optional and relevant only when users choose to connect or share across platforms.

To ensure the annotations remain both legally sound and user-friendly, aligning with principles of transparency and informed consent, the final version of the database was constructed as shown in a table (Figure 5.9). This table presents the updated annotations based on the survey feedback, ensuring that each purpose description reflects both the practical needs of developers and the legal considerations of privacy experts.

Input Field	**Possible Purpose Descriptions**
Full name	- Used to personalize your account. - Required for identification purposes. - Helps verify identity for legal purposes.
Email Address	- Used for account verification and password recovery. - For sending notifications and updates. - Required for communication with customer support.
Phone number	- Used for two-factor authentication. - For account recovery and security notifications. - May be used to send important security updates or optional service notifications (with user consent).
Username	- Unique identifier for your account. - Displayed in forums or online interactions. - Used for logging into the platform.
Password	- Ensures secure access to your account. - Used for authentication and data protection. - Required to prevent unauthorized access.

Date of Birth	- Used to verify age eligibility. - Helps personalize content recommendations. - Used for birthday discounts and rewards.
Gender	- Used for demographic insights and analytics. - May be required for personalized experiences. - Helps customize product recommendations.
Address	- Used for shipping and delivery. - Required for billing and invoicing. - Needed for identity verification in some cases.
City	- Used to tailor location-based services. - Needed for address verification. - Helps provide region-specific offers.
State/Province	- Used for geographical analysis. - Required for accurate shipping calculations. - Needed for taxation purposes.
Postal code	- Ensures accurate delivery of physical items. - Needed for regional tax calculations. - Helps suggest nearby service providers.
Country	- Determines applicable laws and policies. - Helps customize content based on location. - Used for currency and language settings.
Profile picture	- Used to personalize your profile. - Displayed in user interactions and forums. - Used for profile personalization in community or social features.
Security question	- Used for account recovery. - Provides additional security verification. - Ensures an extra layer of protection against hacking.
Company name	-May be used for business-related account setup or invoicing. -Helps verify corporate affiliations for organizational access. -Supports generation of business-related documents, such as invoices or reports.

Job title	- Used for networking and professional insights. - Helps tailor industry-specific content. - Displays role in business-related applications.
Website URL	- Displayed on your profile for others to visit. - Used for verifying business or personal sites. - Required for linking personal portfolios.
Social media links	- Used for connecting accounts or sharing content when the user opts in. - May be displayed on profile pages to support social or networking features. - Allows integration with third-party apps if enabled by the user.
Newsletter subscription	- Used to send promotional emails and updates. - Allows users to receive relevant content. - Helps businesses track user engagement.
Payment Information	- Required for processing transactions. - Used for billing and subscription services. - Ensures seamless automatic payments.

Figure 5.9

5.4 Conclusion

This chapter presented the design, development, and expert validation of a structured database of processing purpose annotations for common personal data fields. The evaluation confirmed that most proposed purpose descriptions were perceived as clear, relevant, and appropriate - particularly in fields such as Username and Password. However, the feedback also revealed important areas for refinement, especially in annotations that may imply secondary uses, such as marketing or third-party involvement.

The insights gained from both legal and technical participants have informed the final version of the annotation database, ensuring that its content is both transparent and legally sound. These refinements are expected to improve user understanding and trust, aligning the annotations more closely with both legal requirements and user expectations.

Chapter 6

6. Design and Development of the Privacy Annotation Tool

6.1 Overview

This chapter presents the design and technical development of the Privacy Annotation Tool, a browser-based application created to support privacy-aware web form design. The tool enables users - especially web developers, designers, and legal experts - to add privacy-related explanations to HTML form fields, helping improve transparency and user trust. These annotations are embedded directly into the form interface using selectable styles, such as short descriptions or info icon pop-ups, allowing for smooth integration into an existing website layout.

The chapter follows a structured software engineering approach to describe the tool's development process. From early requirements analysis to final implementation, each phase was based on methodical design practices. Particular focus is given to usability, accessibility, and privacy-by-design—a design principle that encourages the inclusion of privacy features from the beginning, rather than adding them later as an afterthought.

By using modern web technologies like HTML, CSS, JavaScript, and client-side ZIP handling libraries, the Privacy Annotation Tool runs entirely in the browser. This means that user files are never uploaded to a server. Instead, all processing, annotation, and file generation happen locally, supporting the tool's privacy-focused goals.

The rest of this chapter outlines the tool’s functional and non-functional requirements, the software development methodology used (Waterfall model), the system architecture, the main implementation components, and a visual walkthrough of its interface and functionality.

6.2 Methodology

The development of the Privacy Annotation Tool followed the Waterfall software development model [11] [18], a linear and sequential approach where each phase depends on the deliverables of the previous one. This model was chosen due to its structured nature and suitability for clearly scoped academic projects.

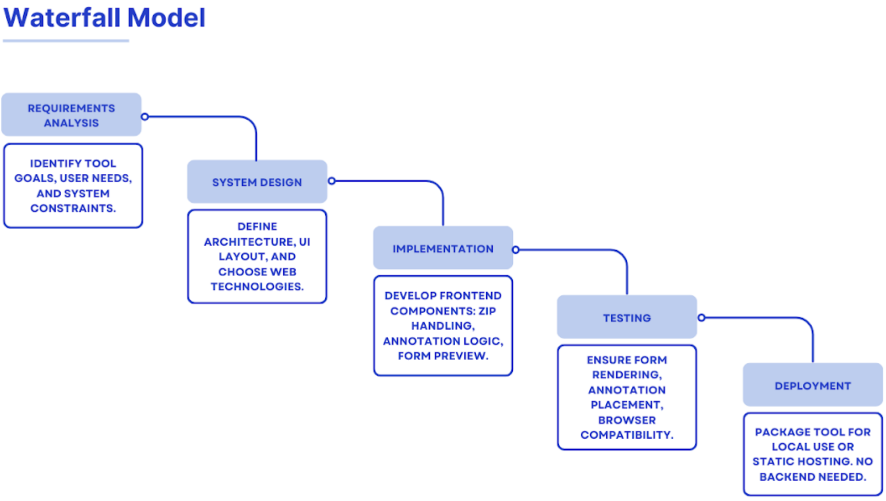

Waterfall Model
REQUIREMENTS ANALYSIS
IDENTIFY TOOL GOALS, USER NEEDS, AND SYSTEM CONSTRAINTS.
SYSTEM DESIGN
DEFINE ARCHITECTURE, UI LAYOUT, AND CHOOSE WEB TECHNOLOGIES.
IMPLEMENTATION
DEVELOP FRONTEND COMPONENTS: ZIP HANDLING, ANNOTATION LOGIC, FORM PREVIEW.
TESTING
ENSURE FORM RENDERING, ANNOTATION PLACEMENT, BROWSER COMPATIBILITY.
DEPLOYMENT
PACKAGE TOOL FOR LOCAL USE OR STATIC HOSTING. NO BACKEND NEEDED.

Figure 6.1 – Waterfall Model Diagram

The diagram above (Figure 6.1) outlines the five sequential phases that structured the development of the Privacy Annotation Tool. Each phase was completed in order, ensuring thorough planning, defined deliverables, and a well-documented development process.

6.3 Requirements Gathering

The requirements for the Privacy Annotation Tool were identified through a combination of user-centered design principles, analysis of existing form annotation practices, and technical feasibility constraints. These aspects were informed by the findings presented in **Chapter 03**, which details the background research on privacy patterns and annotation approaches, and **Chapter 05**, which presents the results of the user study and survey insights. This section outlines the core functionalities that the tool must support, as well as the non-functional attributes necessary to ensure usability, accessibility, and privacy compliance.

The requirements were gathered prior to the design and implementation phases, in accordance with the Waterfall model. These specifications served as the foundation for the system architecture and guided all development efforts.

6.3.1 Functional Requirements

The following functional requirements define the key capabilities the tool must provide:

1. *ZIP File Upload*
   Users must be able to upload a .zip archive containing a complete HTML/CSS/JavaScript project representing a website that includes forms for collecting personal data.

2. *Form Rendering*
   The tool should automatically extract the contents of the uploaded project and render the primary HTML form inside an embedded iframe, preserving the original styling and layout.

3. *Annotation Style Selection*
   Users must be able to choose between two annotation styles:
   a. Info Icon Pop-up: An icon placed next to the label that displays an explanatory tooltip.
   b. Short Description: A brief explanation shown directly beneath the input field.

4. *Annotation Generation and Injection*
   The tool should automatically detect common input fields (e.g., name, email, password) and associate them with predefined privacy annotations, which are injected into the rendered form in the chosen style.

5. *Live Form Preview*

   Changes to annotation styles or content must be reflected immediately in the form preview, allowing users to visually assess the impact of their selections in real time.

6. *Editable Annotation Panel*

   An interactive table should allow users to:

   - View the auto-detected fields.
   - Modify or enter annotations manually.
   - Reset annotations to default values.

7. *HTML Export Functionality*

   Users must be able to generate and download an updated version of the original HTML file with all privacy annotations embedded, ensuring easy integration into existing workflows

6.3.2 Non-Functional Requirements

The following non-functional requirements address the tool's performance, accessibility, and privacy-preserving characteristics:

1. *Usability and Accessibility*

   The interface must be intuitive and easy to navigate for users with varying levels of technical expertise, including those from legal or design backgrounds. Clear layout, visual consistency, and straightforward interactions were prioritized to support ease of use.

2. *Real-Time Responsiveness*

   All changes to annotation content or style must update the form preview immediately, with no need for page reloads or additional input.

3. *Cross-Browser Compatibility*

   The tool must function correctly across major web browsers (e.g., Chrome, Firefox, Edge, Safari) to ensure broad accessibility.

4. *Client-Side Processing*

   As storage of data was not one of the tool’s functional requirements, it was deemed better, all operations—including ZIP extraction, annotation injection, preview rendering, and file generation—to be handled entirely on the client side, with no server communication or data storage.

6.4 System Design

The architecture of the Privacy Annotation Tool is modular and fully client-side, meaning all operations run directly in the user's browser without needing a server. This design was influenced by the design principles, user feedback, and prototype evaluations presented in Chapter 4, where both low-fidelity and high-fidelity prototypes were created to visualize key features like annotation styles, form preview, and user workflows. These prototypes were guided by early user feedback gathered through a survey, which helped shape the tool’s layout, interaction flow, and overall user experience.

Additionally, the data collected and analyzed in Chapter 5 guided the final annotation content. This included building a structured database of personal data processing purposes and privacy annotation suggestions for common form fields. These suggestions were evaluated through a survey involving legal experts and technical professionals, ensuring that the final tool provides accurate, clear, and relevant explanations.

The system itself is made up of several interconnected components, each responsible for a specific part of the form annotation process—from ZIP file upload and HTML extraction to live form rendering, annotation injection, and downloadable HTML export. Figure 6.2 illustrates this workflow, showing how each part of the tool works together to create a seamless, privacy-preserving user experience.

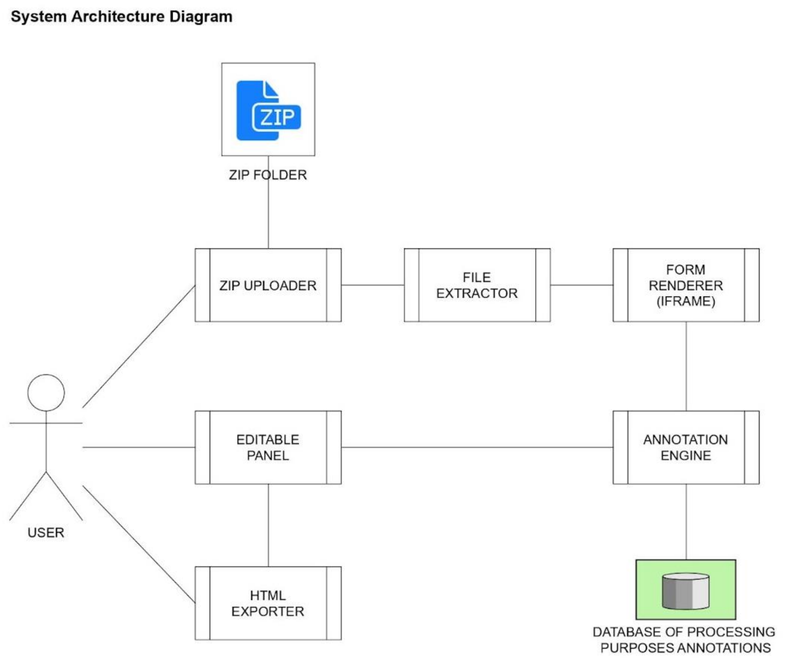


Figure 6.2 – System Architecture Diagram

The architecture shown in Figure 6.2 emphasizes the modularity and client-centric nature of the system. By isolating responsibilities into distinct components—such as extraction, rendering, annotation, and export—the tool achieves maintainability, extensibility, and a seamless user experience. This modular approach also aligns with privacy-by-design principles, ensuring that no user data ever leaves the local environment.

6.5 Implementation Technologies

The Privacy Annotation Tool was developed entirely using web technologies, with a focus on simplicity, accessibility, and full client-side functionality. This approach ensures that no server infrastructure is required, and all operations—including form rendering, annotation, and file handling—take place securely within the user's browser.

Below is an overview of the key technologies and libraries used in the implementation:

6.5.1 HTML & CSS (with Bootstrap)

The user interface of the tool is structured using standard HTML5 and styled using a combination of custom CSS and the Bootstrap 5 framework. Bootstrap was selected for its responsive design utilities, consistent components, and modern aesthetic. Custom styles were added to handle tooltips, table layouts, and annotation previews within the iframe.

6.5.2 JavaScript

Core application logic—including annotation handling, field detection, event listeners, and DOM manipulation—is implemented in vanilla JavaScript. JavaScript also facilitates interaction between the annotation engine and the iframe-rendered form, enabling real-time updates as users make changes in the UI.

6.5.3 JSZip

To handle uploaded ZIP archives, the tool uses the JSZip library, a lightweight client-side utility for reading and extracting ZIP file contents directly in the browser. Once extracted, the tool identifies and renders the main HTML file from within the archive, preserving all relative file paths and assets.

6.5.4 FileReader API & Blob API

- The **FileReader API** is used to read the binary contents of the uploaded ZIP file so that JSZip can process it.

- The **Blob API** enables the tool to generate and download a fully updated HTML file containing the injected annotations. This allows users to export a final version of their form without any server-side storage or communication.

6.5.5 Client-Side Execution

A critical design decision was to implement the entire tool as a browser-based application without any back-end component. This ensures:

- **Maximum privacy:** No user files or annotations are ever uploaded or logged.
- **Ease of deployment:** The tool can be used locally or hosted as a static website.
- **Instant feedback:** All changes are rendered live in the browser.

6.6 Tool Functionality Walkthrough

This section provides a step-by-step walkthrough of the Privacy Annotation Tool's core functionality. It serves as a visual guide, illustrating how the tool operates from the moment a project is uploaded to the final download of the annotated HTML form. Each phase of interaction is accompanied by relevant screenshots to support clarity and usability. The complete tool workflow is demonstrated by Figure 6.3.

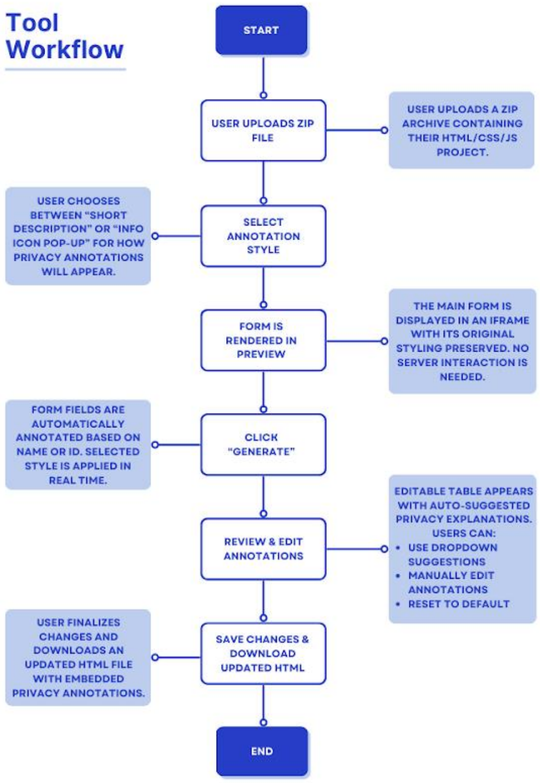

Tool Workflow
START
USER UPLOADS ZIP FILE
USER UPLOADS A ZIP ARCHIVE CONTAINING THEIR HTML/CSS/JS PROJECT.
SELECT ANNOTATION STYLE
USER CHOOSES BETWEEN "SHORT DESCRIPTION" OR "INFO ICON POP-UP" FOR HOW PRIVACY ANNOTATIONS WILL APPEAR.
FORM IS RENDERED IN PREVIEW
THE MAIN FORM IS DISPLAYED IN AN IFRAME WITH ITS ORIGINAL STYLING PRESERVED. NO SERVER INTERACTION IS NEEDED.
CLICK "GENERATE"
FORM FIELDS ARE AUTOMATICALLY ANNOTATED BASED ON NAME OR ID. SELECTED STYLE IS APPLIED IN REAL TIME.
REVIEW & EDIT ANNOTATIONS
EDITABLE TABLE APPEARS WITH AUTO-SUGGESTED PRIVACY EXPLANATIONS. USERS CAN:
• USE DROPDOWN SUGGESTIONS
• MANUALLY EDIT ANNOTATIONS
• RESET TO DEFAULT
SAVE CHANGES & DOWNLOAD UPDATED HTML
USER FINALIZES CHANGES AND DOWNLOADS AN UPDATED HTML FILE WITH EMBEDDED PRIVACY ANNOTATIONS.
END

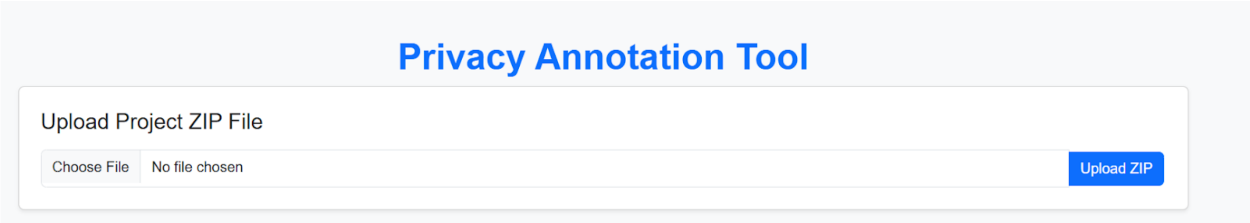
Figure 6.3 – Tool Workflow Diagram

This figure presents a high-level overview of the envisioned user journey within the Privacy Annotation Tool, from project upload to annotation and export. It was designed prior to development and reflects the planned interactive flow of the system.

6.6.1 Upload ZIP File

Users begin by uploading a .zip archive that contains a complete HTML/CSS/JS web form project. The interface includes a simple file input field accompanied by an

“Upload ZIP” button. Once the file is uploaded, the tool extracts the contents using JSZip and identifies the main HTML file to display.

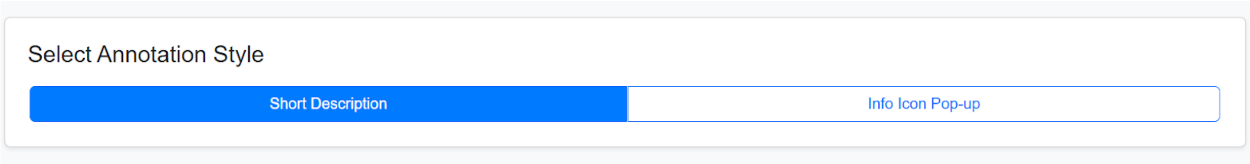


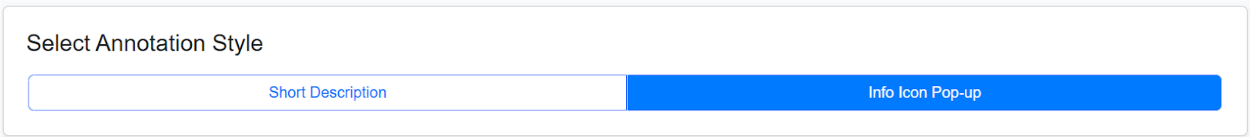
6.6.2 Annotation Style Selection

After uploading, users are prompted to select their preferred annotation style:

- Short Description: A brief explanation displayed under the input field.
- Info Icon Pop-up: An info icon next to the label that shows a tooltip on hover.

This toggle is implemented using two buttons, and the selected style is highlighted. The style selection affects how annotations are injected during rendering.



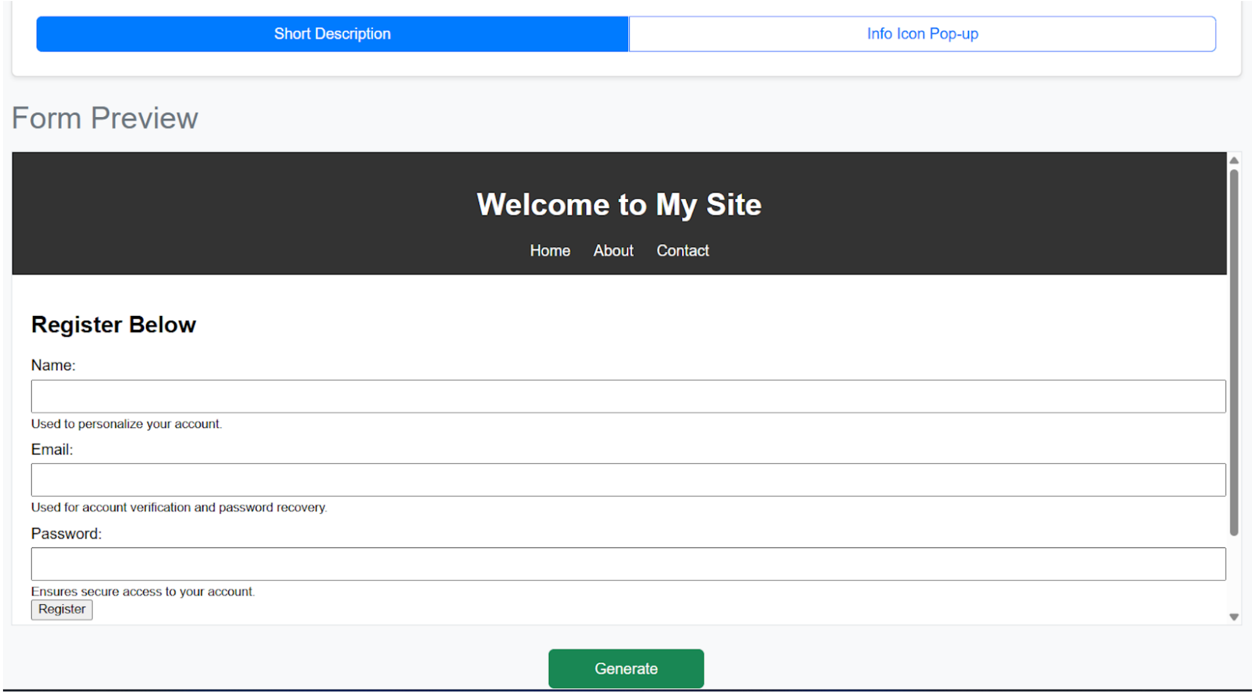


6.6.3 Form Preview and Generate

The form is then rendered live within a sandboxed iframe, preserving the original layout and functionality. The “Generate” button, located directly beneath the iframe, allows users to apply the selected annotation style to the preview.

The annotation engine automatically detects form fields (e.g., name, email, password) and injects either:

- Inline descriptions (<small>) for the short description style.
- Tooltip icons for the info pop-up style.



Form Preview

Welcome to My Site

Register Below

Name:

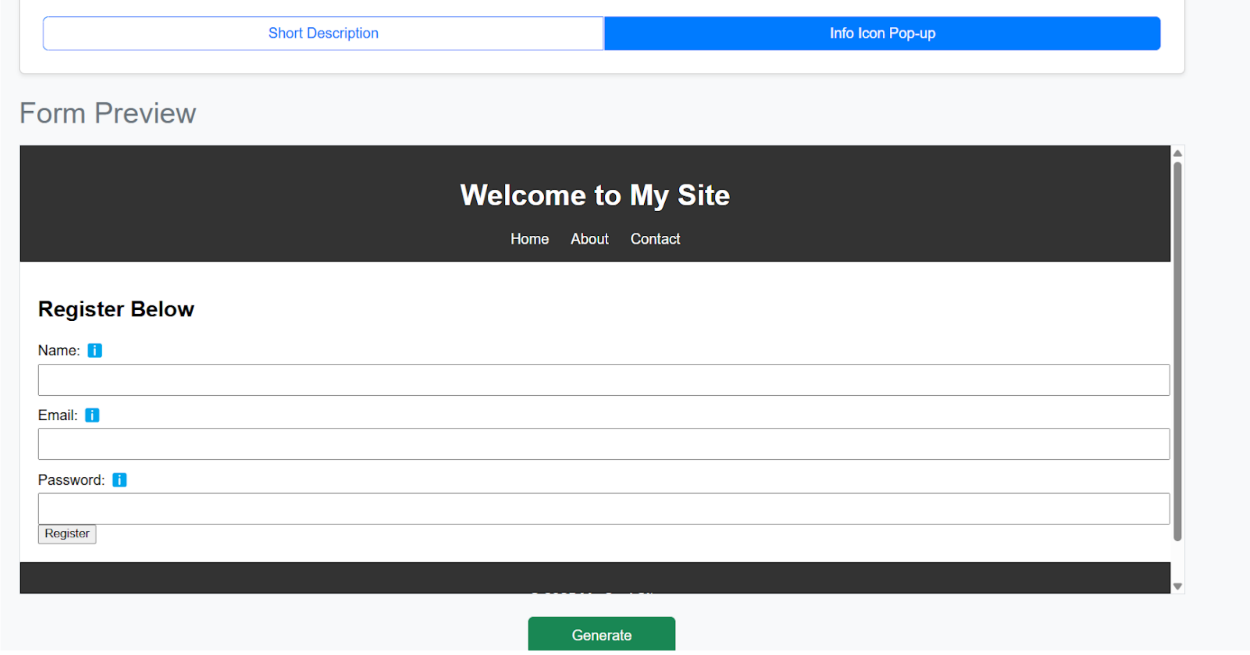
Used to personalize your account.

Email:

Used for account verification and password recovery.

Password:

Ensures secure access to your account.



Form Preview

Welcome to My Site

Register Below

Name: ℹ

Email: ℹ

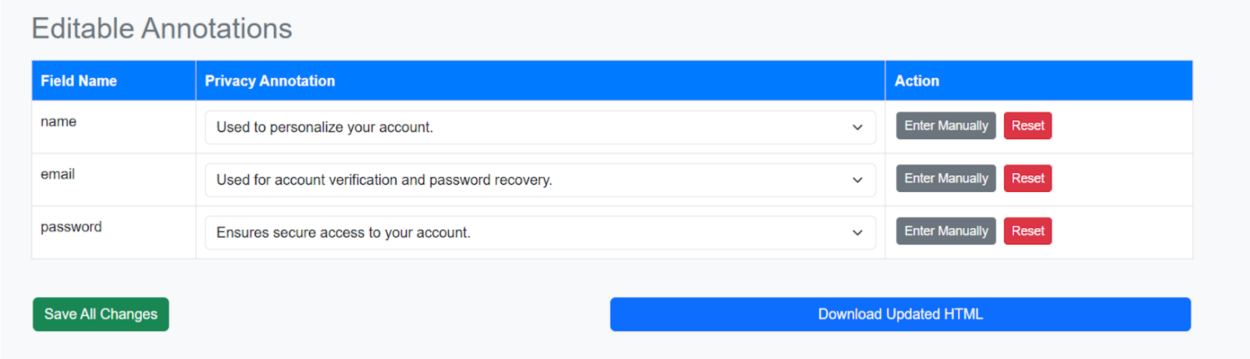
Password: ℹ

6.6.4 Editable Annotations

After pressing “Generate”, an editable annotations panel becomes visible. This table lists each detected form field along with:

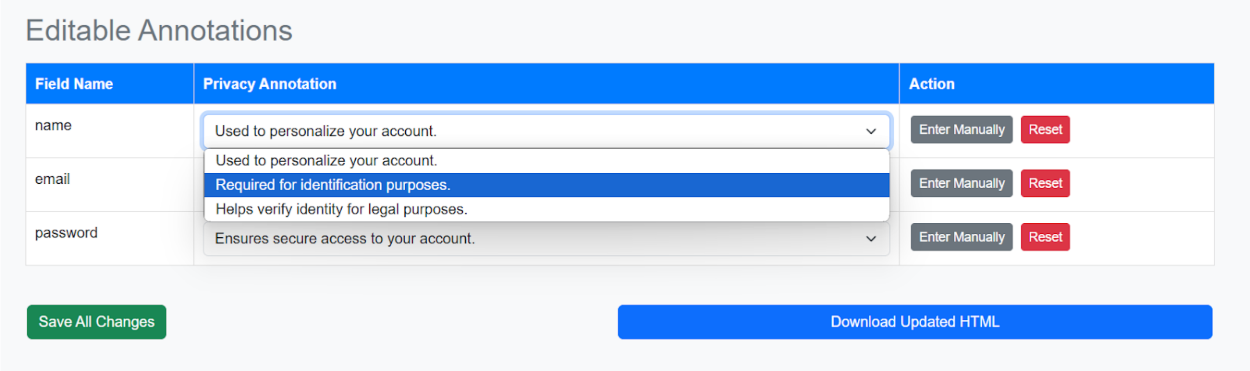
- A dropdown of predefined annotation suggestions.
- A manual input option for custom annotations.
- A Reset button to revert to default values.

This allows the user to personalize or refine the annotation content before export.



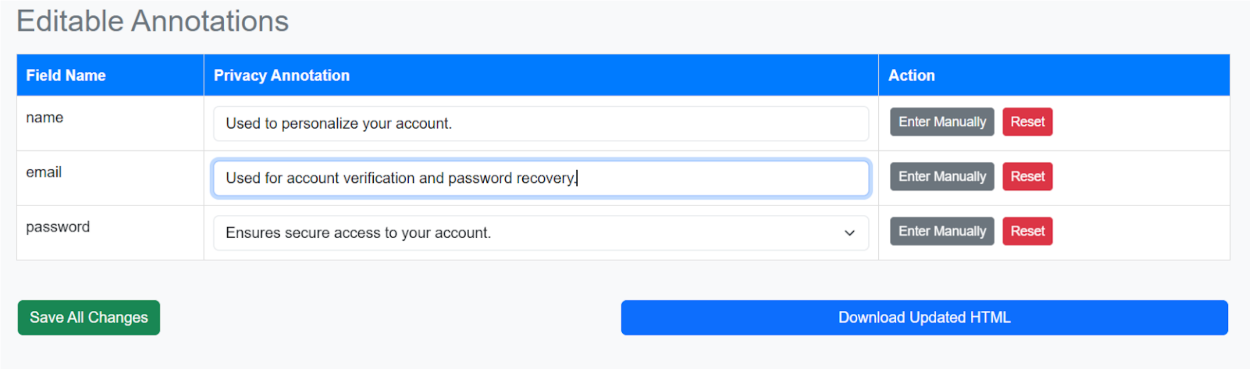
Editable Annotations

Field Name	Privacy Annotation	Action
name	Used to personalize your account.	Enter Manually Reset
email	Used for account verification and password recovery.	Enter Manually Reset
password	Ensures secure access to your account.	Enter Manually Reset



Editable Annotations

Field Name	Privacy Annotation	Action
name	Used to personalize your account. Used to personalize your account. Required for identification purposes. Helps verify identity for legal purposes.	Enter Manually Reset
email		Enter Manually Reset
password	Ensures secure access to your account.	Enter Manually Reset

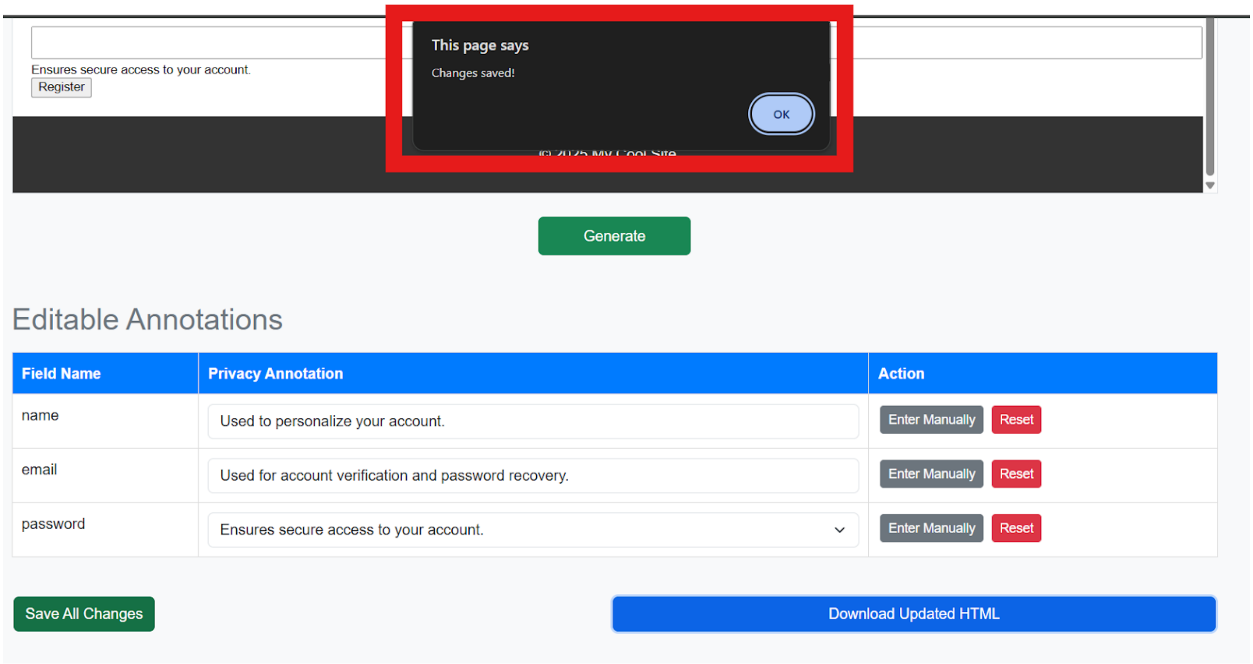


Editable Annotations

Field Name	Privacy Annotation	Action
name	Used to personalize your account.	Enter Manually Reset
email	Used for account verification and password recovery.	Enter Manually Reset
password	Ensures secure access to your account.	Enter Manually Reset

6.6.5 Save and Download

Once the annotations are customized, the user can press “Save All Changes” to store their edits, and then click “Download Updated HTML” to export a fully annotated version of the form. The updated file includes all injected annotations and is generated locally using the Blob API.



Ensures secure access to your account.

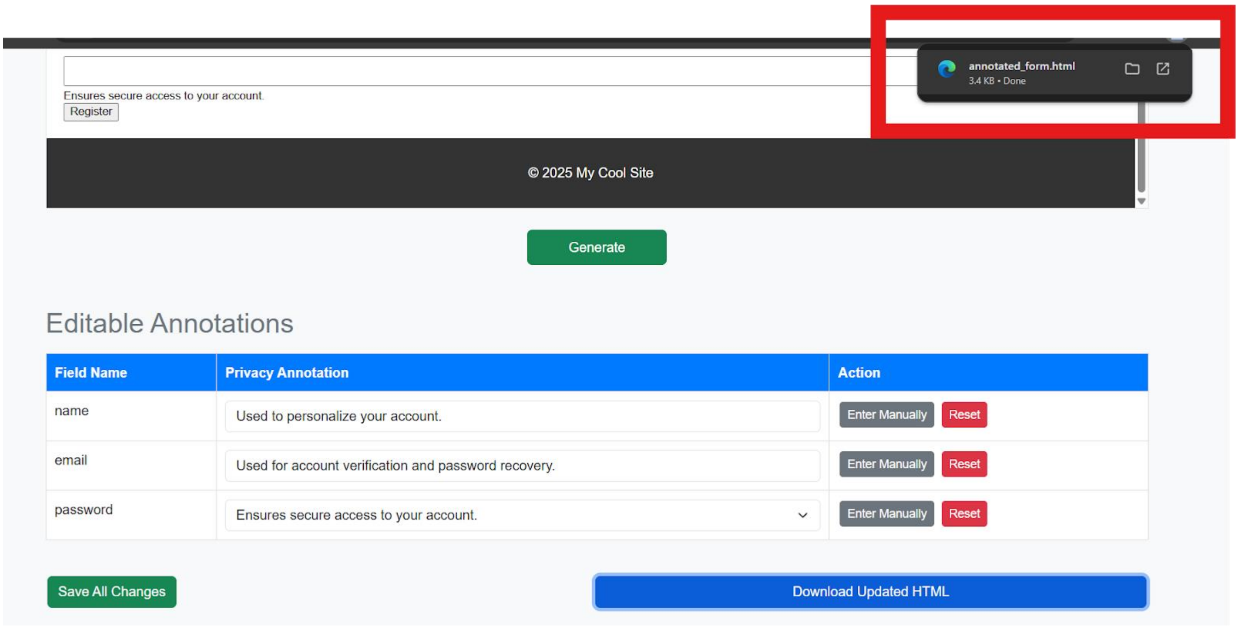
This page says

Changes saved!

© 2025 My Cool Site

Editable Annotations

Field Name	Privacy Annotation	Action
name	Used to personalize your account.	Enter Manually Reset
email	Used for account verification and password recovery.	Enter Manually Reset
password	Ensures secure access to your account.	Enter Manually Reset



Ensures secure access to your account.

annotated_form.html
3.4 KB • Done

© 2025 My Cool Site

Editable Annotations

Field Name	Privacy Annotation	Action
name	Used to personalize your account.	Enter Manually Reset
email	Used for account verification and password recovery.	Enter Manually Reset
password	Ensures secure access to your account.	Enter Manually Reset

6.7 Annotation Logic and Injection

A key component of the Privacy Annotation Tool is its ability to intelligently detect form fields and inject context-aware privacy explanations in real time. This section outlines the logic used to identify relevant fields, the style-specific annotation strategies applied, and the way these annotations are synchronized with the editable user interface.

6.7.1 Detection of Input Fields

Upon loading the form into the preview iframe, the tool scans the DOM for input elements using standard tags: <input>, <select>, and <textarea>. To associate these fields with meaningful privacy annotations, the tool attempts to match each field using:

- The name attribute (most common identifier).
- The id attribute (used when name is missing).
- Associated <label> elements via for attributes or structural proximity (i.e., labels that wrap or precede the field).

If a field is detected but does not match any entry in the predefined annotation database, the tool automatically assigns a placeholder annotation stating **"No predefined annotation available"**. This ensures that every detected field is accounted for and gives the user the opportunity to manually define a suitable description via the editable panel.

6.7.2 Style-Specific Annotation Injection

Based on the user's selected style—Short Description or Info Icon Pop-up—the tool dynamically injects the corresponding annotation elements next to each detected field.

- **Info Icon Pop-up**

  The tool creates a <span> styled as an info icon (**ℹ**), which contains a nested <span> with the tooltip text. It is inserted beside the field's label.

  ```
  <span class="tooltip">ℹ
    <span class="tooltiptext">Used for account verification and password
  recovery.</span>
  </span>
  ```

- **Short Description**

  A <small> element is inserted below the input field to show a muted, inline annotation.

  ```
  <small class="text-muted">Used for account verification and password
  recovery.</small>
  ```

Both styles are styled consistently to maintain a polished and non-intrusive visual experience.

6.7.3 Data Binding to Annotation Panel

Each detected field is automatically listed in the editable annotation panel. This enables two-way synchronization:

- Changes in the table (e.g., dropdown selection or manual input) are reflected instantly in the preview.
- Resetting or updating annotation values updates the annotation engine's state and the iframe's DOM accordingly.

This dynamic binding ensures a seamless editing experience between the form preview and the configuration table.

6.7.4 Real-Time Preview Updates

The preview iframe is fully dynamic and updates in real-time. Whenever the user:

- Changes the annotation style (e.g., switches from pop-up to short description),
- Modifies a field's annotation text, or
- Clicks "Generate" to apply changes

The iframe is refreshed with a clean copy of the form DOM. Annotations are cleared and reinjected using the most up-to-date configuration. This live regeneration ensures that the preview is always consistent with the user's selections, without requiring a page reload.

6.8 File Handling and Rendering

The Privacy Annotation Tool is designed to accept full HTML/CSS/JS projects packaged as ZIP archives and render them directly within the browser. This section outlines how uploaded files are processed, how assets are managed, and how the form is safely and accurately previewed in an iframe.

6.8.1 ZIP Extraction and Processing

When a user uploads a ZIP file, the tool uses the JSZip library alongside the FileReader API to extract its contents entirely on the client side. The ZIP archive is parsed in-memory, and the contents of each file are stored in a JavaScript object, indexed by their relative paths. This avoids any server-side processing, ensuring full privacy and compliance with the tool's privacy-by-design principles.

6.8.2 Rebuilding the File Structure

Once extracted, the tool reconstructs the project's original structure by mapping each file's relative path and content. This step is critical for preserving:

- Folder nesting (e.g., /css/style.css)
- Relative asset references in HTML (e.g., <link href="css/style.css">)
  Project integrity during rendering and annotation

This virtual reconstruction allows seamless referencing of stylesheets, scripts, and media files in the next step.

6.8.3 HTML File Detection and Iframe Rendering

The tool identifies the main HTML file—usually the first file ending in .html, such as index.html—and loads it into a sandboxed <iframe>. The loading is performed using the srcdoc attribute with a Blob-based data URL, which allows HTML to be rendered directly from memory.

This method ensures:

- Layout and styling remain faithful to the original project.
- The rendering is isolated from the tool's main interface.
- No reliance on external servers or HTTP requests.

6.8.4 Asset Injection and Resolution

To ensure the HTML form appears and behaves correctly inside the iframe, the tool injects linked resources manually:

- **CSS files** are inserted into the iframe's <head> as <style> tags.
- **JavaScript files** are added at the bottom of the <body> as <script> tags.
- **Image paths** are preserved, assuming the ZIP includes the image assets.

This guarantees that the original styling and functionality are maintained without relying on remote dependencies.

6.8.5 Limitations and Sandboxing Considerations

Rendering within an iframe has important limitations, primarily due to browser-enforced security models:

- Scripts are confined to the iframe's sandbox and cannot interact with the parent page.
- External assets or cross-origin requests (e.g., CDN resources, APIs) are blocked.
- Only safe, static rendering is supported.

These constraints, while limiting certain advanced features, enhance the privacy and security of the tool and ensure consistent behavior across browsers.

6.9 Challenges and Solutions

During the development of the Privacy Annotation Tool, several practical challenges were encountered, primarily related to DOM handling, file processing, and UI consistency. This section summarizes key hurdles and how they were addressed.

6.9.1 Annotation Placement Without Layout Disruption

Injecting annotations into a wide variety of form layouts risked breaking the visual structure, especially with tightly styled inputs. To solve this, annotations were injected using non-intrusive tags (<small> or <span>) with margin styling, ensuring they aligned naturally with the existing layout without requiring structural changes.

6.9.2 Forms Without Proper Labels

Some HTML forms lacked <label> tags or had loosely associated fields. In these cases, the tool uses fallback logic to associate annotations by checking:

- The for attribute
- Parent or sibling elements
- Field id or name attributes

This flexible strategy ensures most fields are properly annotated even in poorly structured forms.

6.9.3 Style Usability Across Scenarios

Maintaining clarity and consistency in both annotation styles (short description and pop-up) required careful attention to spacing, font size, and tooltip behavior. Custom styling was added to ensure both styles are readable, responsive, and do not interfere with the form’s original styling.

6.9.4 ZIP Structure Variability

Users may upload ZIP archives with unusual structures, such as deeply nested folders or missing index.html files. The tool handles this by:

- Searching all extracted files for any .html file
- Using the first valid file as the main form
- Displaying error messages when no form is detected

6.9.5 Preserving Functionality After Annotation

To avoid interfering with form behavior, the tool injects annotations as passive elements only—without altering form controls or JavaScript logic. This ensures that the form remains functional after annotations are applied and can be used immediately after download.

6.10 Summary

This chapter presented the design and development of the Privacy Annotation Tool, a browser-based application built to support the integration of privacy explanations into HTML forms. Following a structured software engineering approach—guided by the Waterfall model - the chapter detailed the tool's functional and non-functional requirements, architectural design, core technologies, and interactive workflow.

Key components such as ZIP file handling, form rendering in a secure iframe, annotation injection logic, and dynamic editing via an annotation table were described in depth. Screenshots and diagrams supported a step-by-step walkthrough of the tool’s functionality, while technical sections explained the underlying logic behind field detection, asset injection, and privacy-safe rendering.

Challenges encountered during development - such as maintaining layout integrity, handling incomplete form markup, and ensuring annotation usability—were addressed with practical solutions that prioritize user experience and security.

The chapter concludes the system-building portion of the dissertation. In the next chapter, the tool will be evaluated in terms of usability, effectiveness, and its potential to support privacy-aware web development through qualitative and/or user-centered validation.

The complete source code of the Privacy Annotation Tool, including HTML, CSS, JavaScript files, and demonstration projects, is publicly available on Google Drive for reference and reproducibility purposes[8].

[8] Google Drive folder: https://drive.google.com/drive/folders/1a8IJE55X6lNl0Vr6JxOllNBLaht2rSse?usp=sharing

Chapter 7

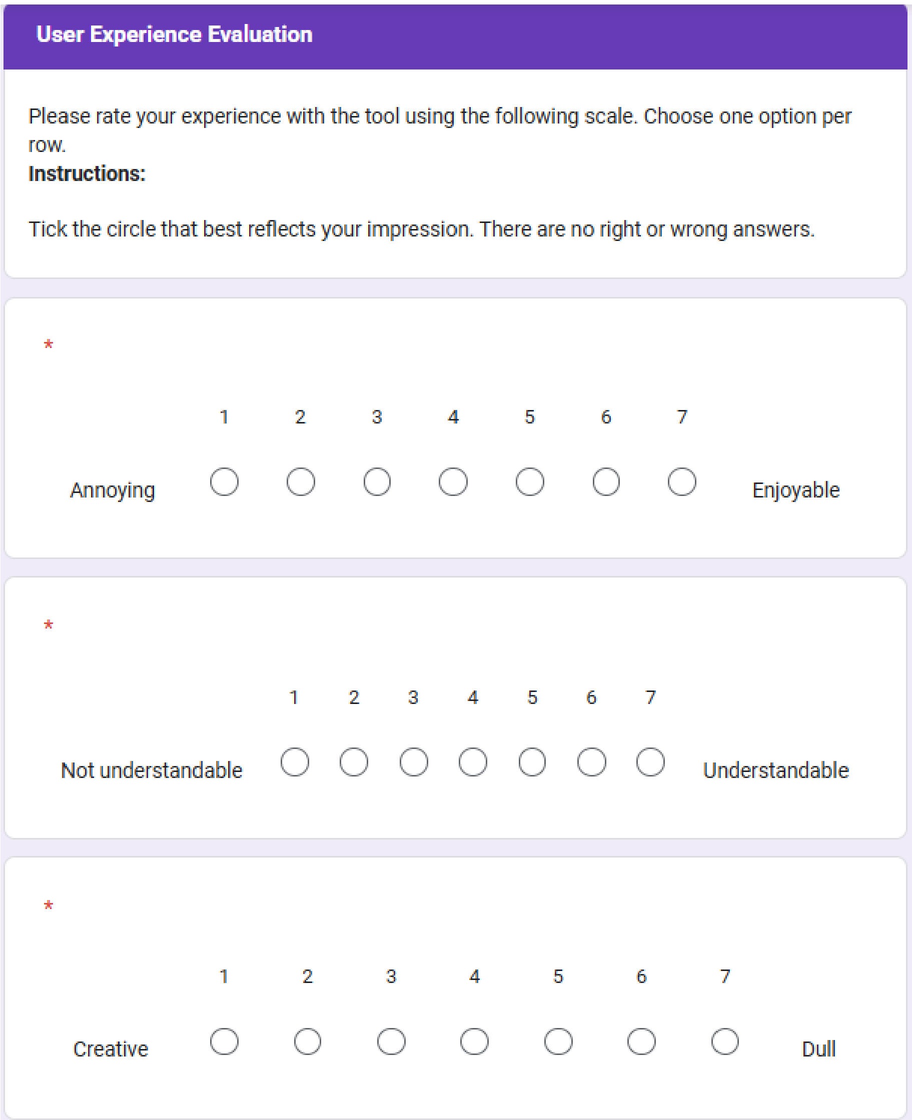
7. Evaluation of the Privacy Annotation Tool

7.1 Introduction

This chapter presents the evaluation of the Privacy Annotation Tool developed as part of this research. The evaluation was conducted using a structured questionnaire based on the User Experience Questionnaire (UEQ), a widely accepted instrument for measuring the perceived user experience of interactive systems. The UEQ is designed to capture immediate user impressions of a product based on six key dimensions: Attractiveness, Perspicuity, Efficiency, Dependability, Stimulation, and Novelty [20].

7.2 Methodology

The evaluation process involved 40 participants who interacted with the Privacy Annotation Tool and subsequently completed an online questionnaire. The questionnaire was designed based on the standardized UEQ format, which includes 26 pairs of contrasting attributes rated on a 7-point Likert scale. Participants were instructed to make spontaneous judgments to capture their immediate impressions, as recommended by the UEQ guidelines. An example is presented below (Figure 7.1). The full questionnaire is included in Appendix D for reference.



User Experience Evaluation

Please rate your experience with the tool using the following scale. Choose one option per row.
Instructions:

Tick the circle that best reflects your impression. There are no right or wrong answers.

*

	1	2	3	4	5	6	7	
Annoying	○	○	○	○	○	○	○	Enjoyable

*

	1	2	3	4	5	6	7	
Not understandable	○	○	○	○	○	○	○	Understandable

*

	1	2	3	4	5	6	7	
Creative	○	○	○	○	○	○	○	Dull

Figure 7.1 - Example of the survey questionnaire

To respond to the questionnaire, participants were asked to watch a brief demo video of the Privacy Annotation Tool, which provided a detailed overview of its features and usage.[9]

7.3 Results

The responses were collected and analyzed to assess the overall user experience of the Privacy Annotation Tool. The UEQ responses were categorized into the following key dimensions [20]:

[9] Privacy Annotation Tool Demo Video. Available at: https://www.youtube.com/watch?v=beJNjk7xjfs (accessed May 2025).

1. **Attractiveness:** Overall impression of the tool, reflecting user enjoyment and appeal.

2. **Perspicuity:** Ease of learning and understanding the tool's functionality.

3. **Efficiency:** User perception of task completion speed and performance.

4. **Dependability:** Trust in the tool's functionality and reliability.

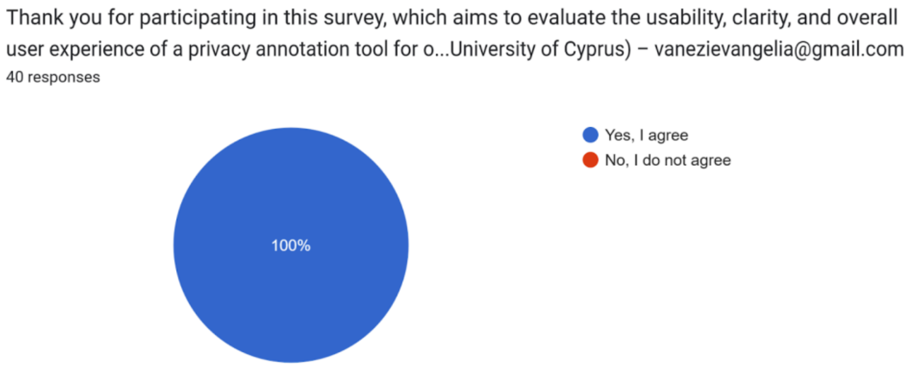
5. **Stimulation:** User engagement and motivation when using the tool.

6. **Novelty:** Perception of the tool's innovation and uniqueness.

7.4 Quantitative Analysis of Survey Responses

The quantitative analysis of the survey responses revealed the following insights:

- **Participant Agreement:** All 40 participants agreed to participate in the survey, confirming their understanding of the survey's purpose and voluntary nature (Figure 7.2).



Thank you for participating in this survey, which aims to evaluate the usability, clarity, and overall user experience of a privacy annotation tool for o...University of Cyprus) – vanezievangelia@gmail.com

40 responses

Figure 7.2

- **Familiarity with GDPR:** 42.5% of participants reported being somewhat familiar with GDPR, while 12.5% indicated being very familiar (Figure 7.3).

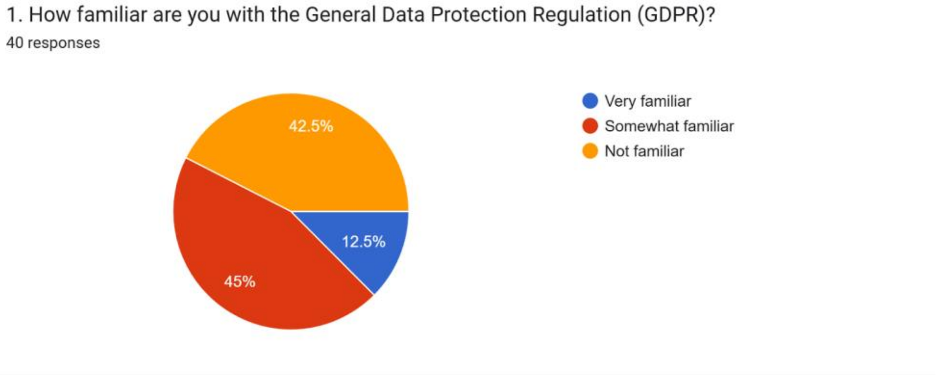


Figure 7.3

- **Interest in Web UIs**: 53.5% of participants reported being somewhat interested in developing usable web user interfaces (UIs), while 37.2% indicated being very interested (Figure 7.4).

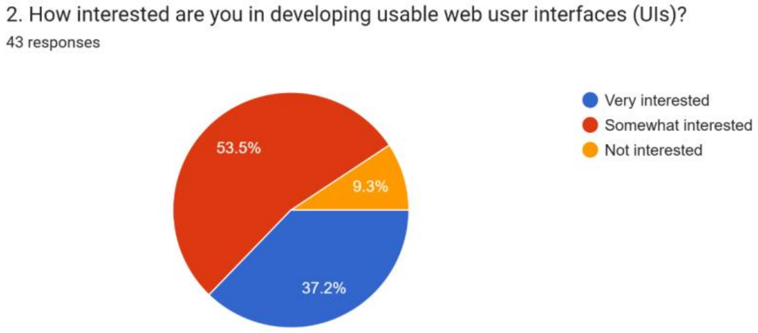


Figure 7.4

- **Interest in GDPR-compliant UIs**: 46.5% of participants reported being very interested in developing GDPR-compliant and privacy-friendly web user interfaces, while 39.5% were somewhat interested (Figure 7.5).

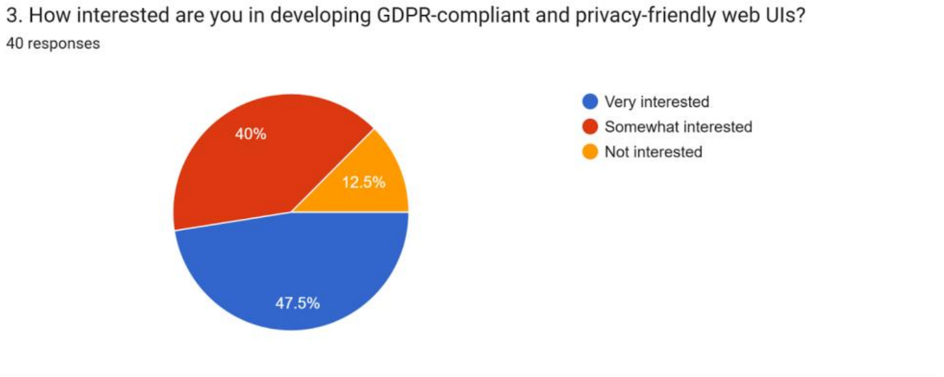


Figure 7.5

- **User Experience Scores:** Most participants rated the tool positively across key dimensions, with high scores for aspects like ease of use, efficiency, and overall satisfaction (Figures 7.5 to 7.10).

The mean values for all 26 item pairs from the questionnaire are shown in Figure 7.4. This chart reflects the direct user responses to each individual attribute pair (e.g., “annoying/enjoyable”, “efficient/inefficient”), with values transformed onto a scale from -3 (most negative) to +3 (most positive).

Overall, the highest ratings were recorded for:

- not understandable/understandable (2.3)
- bad/good (2.3)
- unfriendly/friendly (2.3)
- inefficient/efficient (2.3)
- cluttered/organized (2.3)

These scores suggest that users experienced the tool as friendly, efficient, well-structured, and helpful during interaction.

The lowest scores were observed for:

- dull/creative (1.1)
- conservative/innovative (1.1)

which may reflect room for improvement in the tool’s perceived novelty and creative design.

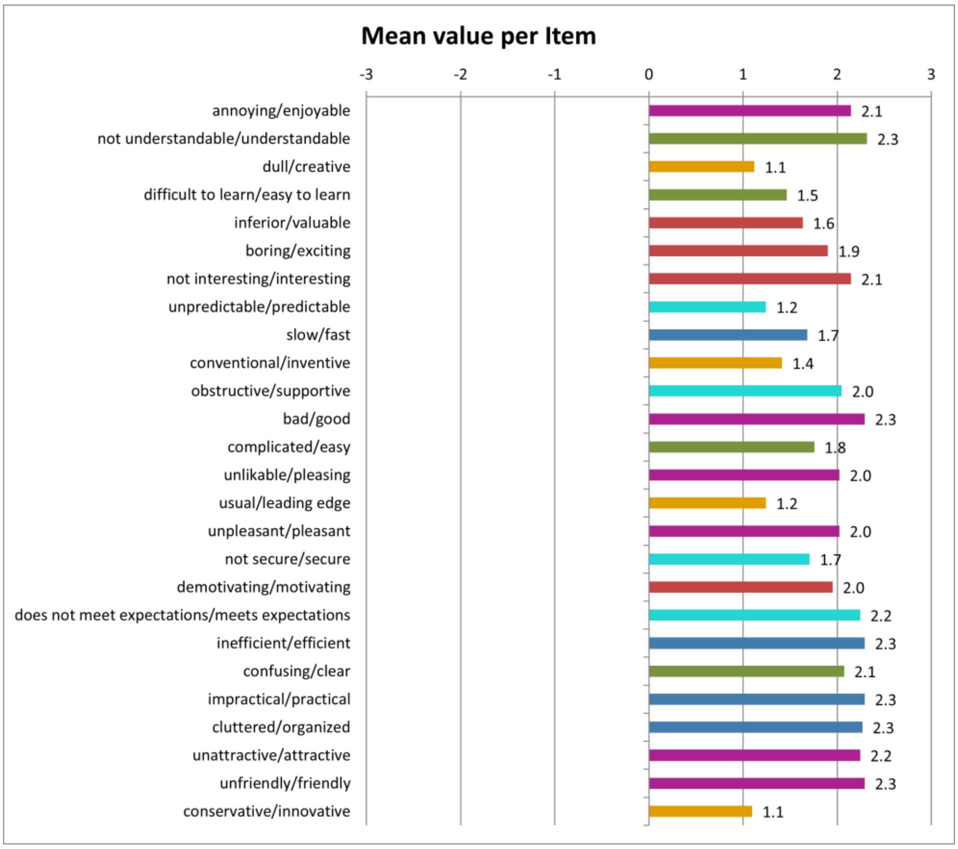


Figure 7.6 - Mean value per item

The 26 UEQ items were also grouped into six standardized categories to allow higher-level analysis: Attractiveness, Perspicuity, Efficiency, Dependability, Stimulation, and Novelty.

These group-level scores were visualized using benchmark-based interpretation in Figure 7.7.

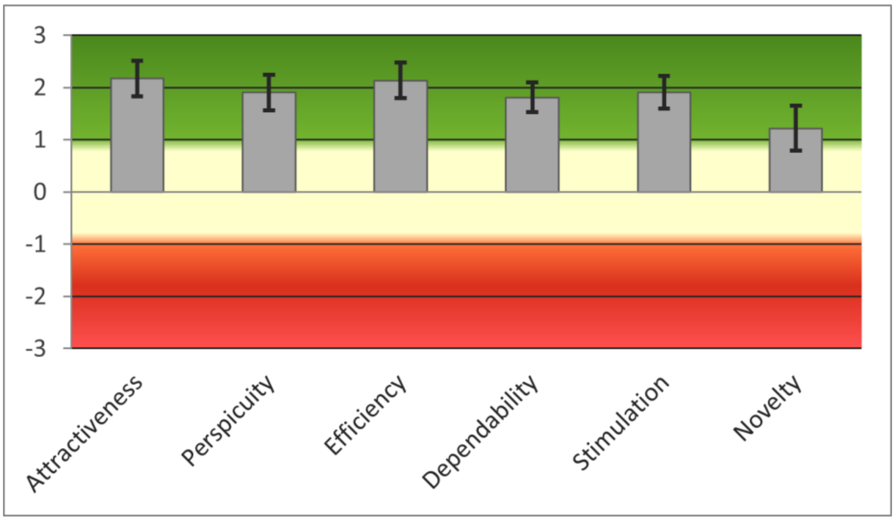


Figure 7.7 - UEQ scales overview

According to the UEQ benchmark framework:

- **Attractiveness (2.1)**, **Efficiency (2.3)**, and **Perspicuity (2.0)** were rated as **Excellent**, placing them in the top 10% of all benchmarked tools.
- **Stimulation (2.0)** and **Dependability (1.7)** were considered **Good**, suggesting above-average perceived quality.
- **Novelty (1.1)** was rated as **Above Average**, meaning users saw the tool as somewhat innovative, though there's potential for a more striking or creative design.

These results reflect a generally positive perception of the Privacy Annotation Tool across most dimensions.

Following this benchmark-based overview**,** the two most positively rated individual dimensions were **Pleasing** and **Efficient**, reflecting strong impressions of both the tool's appeal and its practical utility. These results are presented in the following figures:

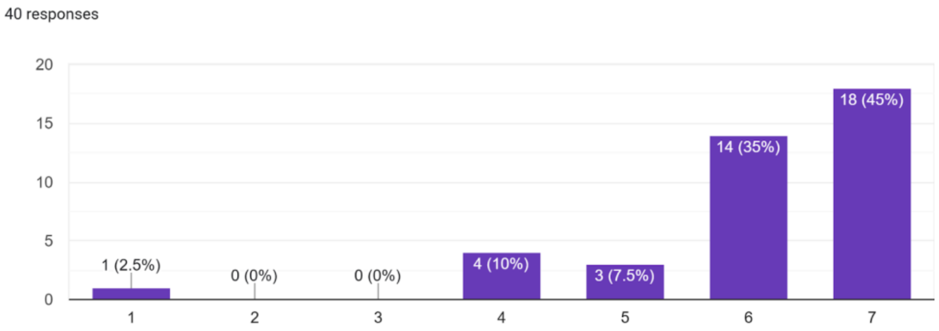


Figure 7.8 - User perceptions of the tool as pleasing, reflecting high satisfaction with the design and overall user experience.

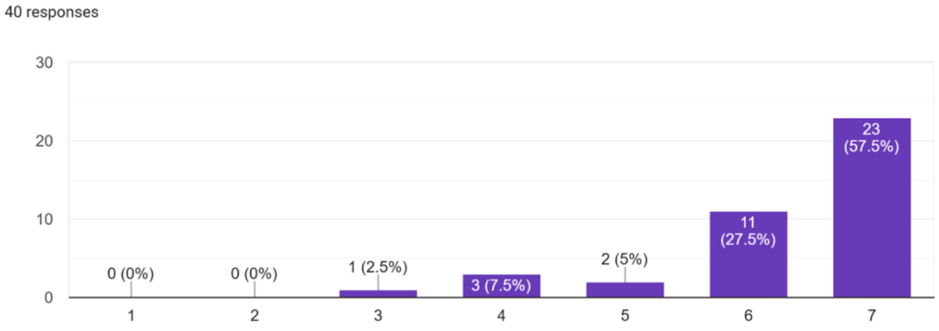


Figure 7.9 - User perceptions of the tool as efficient, indicating a strong positive impression of the tool's speed and effectiveness in supporting privacy annotations.

These high ratings suggest that the tool successfully meets user expectations for both usability and overall appeal, reinforcing its effectiveness in enhancing privacy transparency in online forms.

7.4.1 GDPR Familiarity Correlation

To explore whether GDPR knowledge affects how users perceive the tool, we grouped the UEQ answers by participants' self-reported familiarity with GDPR. As shown in Figure 7.10, responses were positive overall across all groups, but users who were more familiar with

GDPR tended to be slightly more critical in areas like clarity, helpfulness, and perceived security. This may reflect their higher expectations when it comes to privacy-compliant design and offers useful insight for future improvements.

On the other hand, participants with less familiarity showed more positive reactions in several areas, indicating a stronger perceived benefit from the tool. Considering that only 12.5% of the sample identified as very familiar with GDPR, these findings underline the practical value of the tool for the majority of users, who are less experienced and thus more in need of such support.

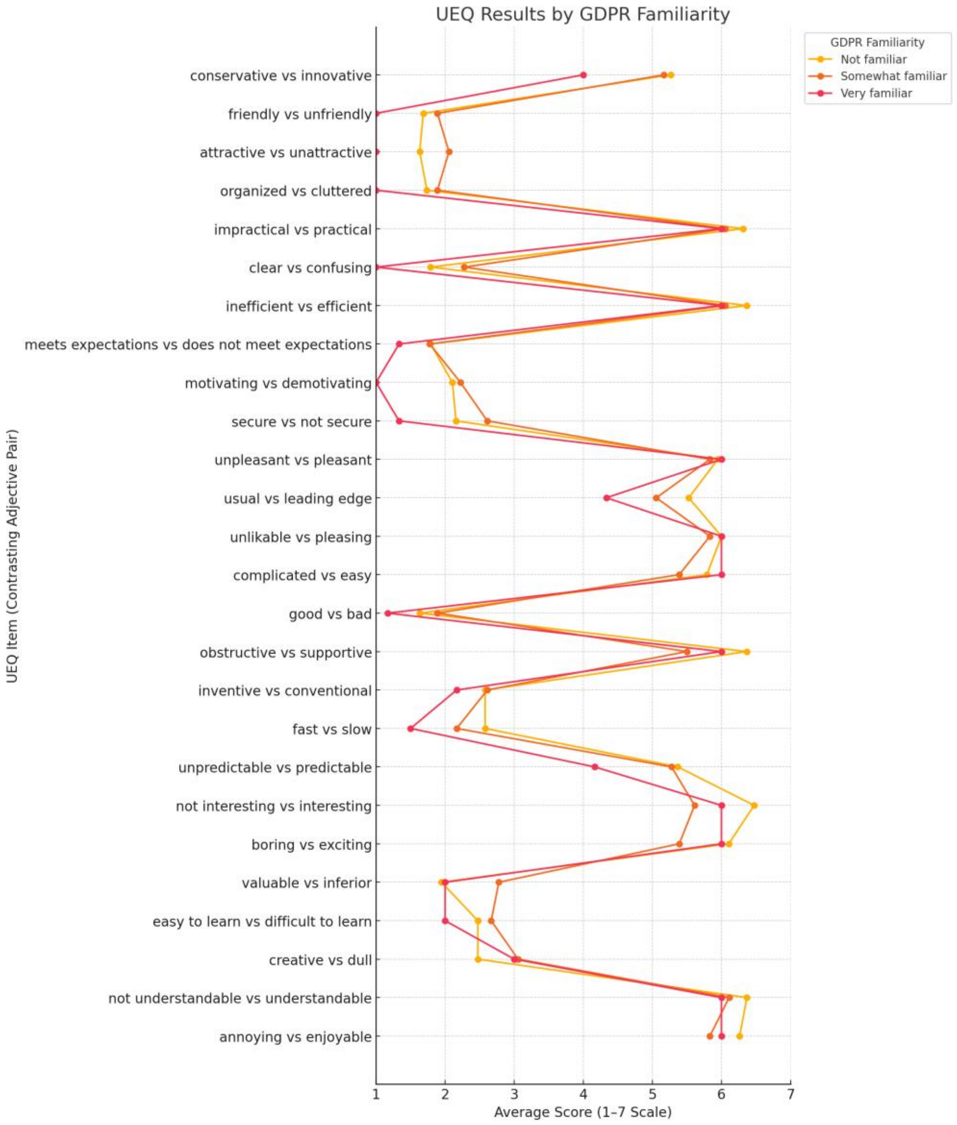


Figure 7.10 - Differentiation of UEQ scores based on GDPR familiarity

The plot shows how user experience ratings (across 26 UEQ item pairs) vary depending on the participants' familiarity with GDPR.

7.4.2 Web UI Interest Correlation

To investigate whether participants' interest in developing usable web interfaces influenced their perception of the tool, we grouped the UEQ responses based on their answers to Question 2. As shown in Figure 7.11, participants who reported being *very interested* in UI design consistently rated the tool more positively across almost all dimensions.

These users appeared to appreciate the tool’s usability, clarity, and innovation more than other groups. In contrast, participants with *some* or *low interest* in UI design provided slightly lower scores in several categories, especially related to stimulation, practicality, and novelty. This means that users who are very interested in creating web interfaces pay more attention to things like design and quality, while those who are less interested might not notice or care as much about these details.

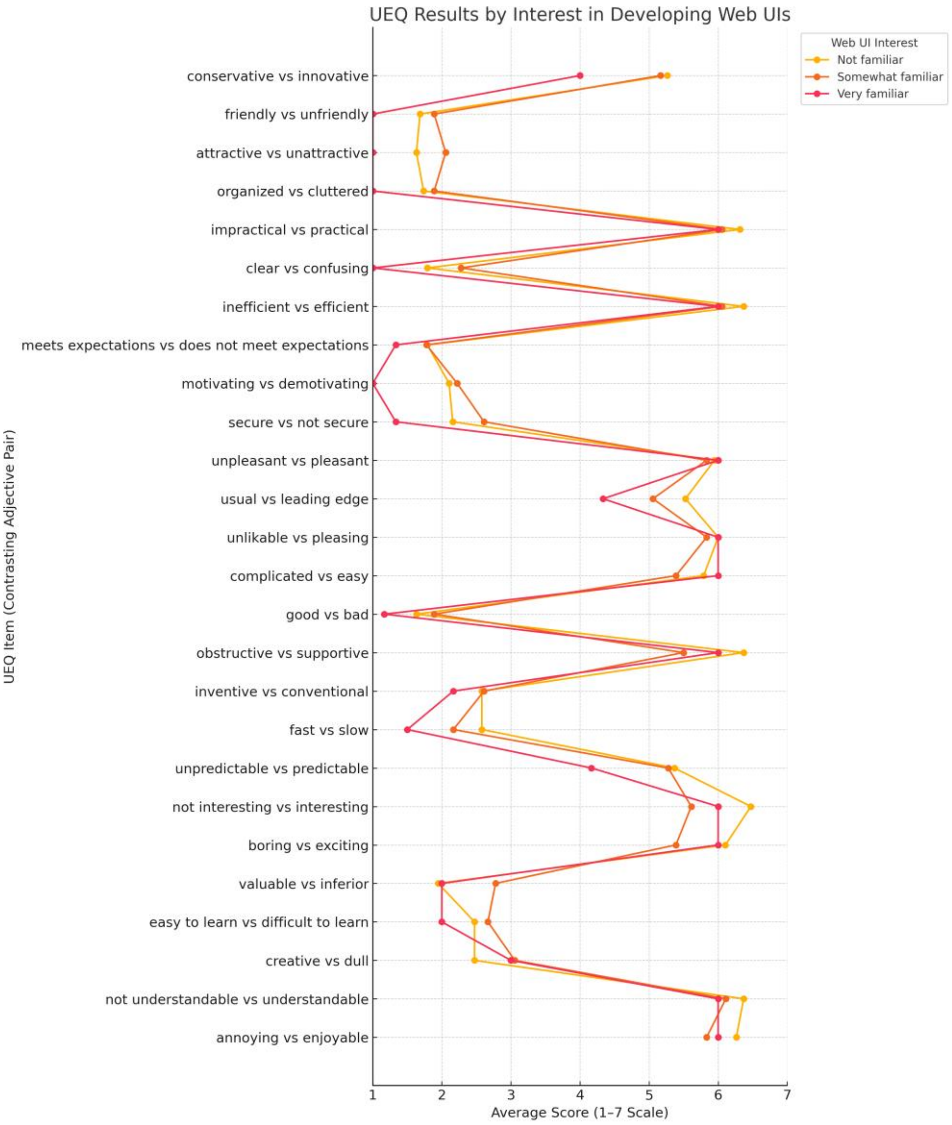


Figure 7.11 - Differentiation of UEQ scores based on Web UI interest The chart illustrates how participants' user experience ratings differ depending on their interest in developing usable web interfaces.

7.4.3 GDPR-Compliant UI Interest Correlation

We also examined whether participants' interest in developing GDPR-compliant and privacy-friendly UIs affected their evaluation of the tool. UEQ responses were grouped according to answers to Question 3. As shown in Figure 7.12, those who were *very interested* in privacy-focused design gave the highest ratings in areas such as *supportiveness*, *security*, and *pleasantness*.

Interestingly, participants with *lower interest* in privacy-compliant interfaces gave slightly lower scores in clarity, helpfulness, and innovation. These differences suggest that the tool resonates more with users already motivated to design for privacy, potentially because it aligns closely with their goals and expectations.

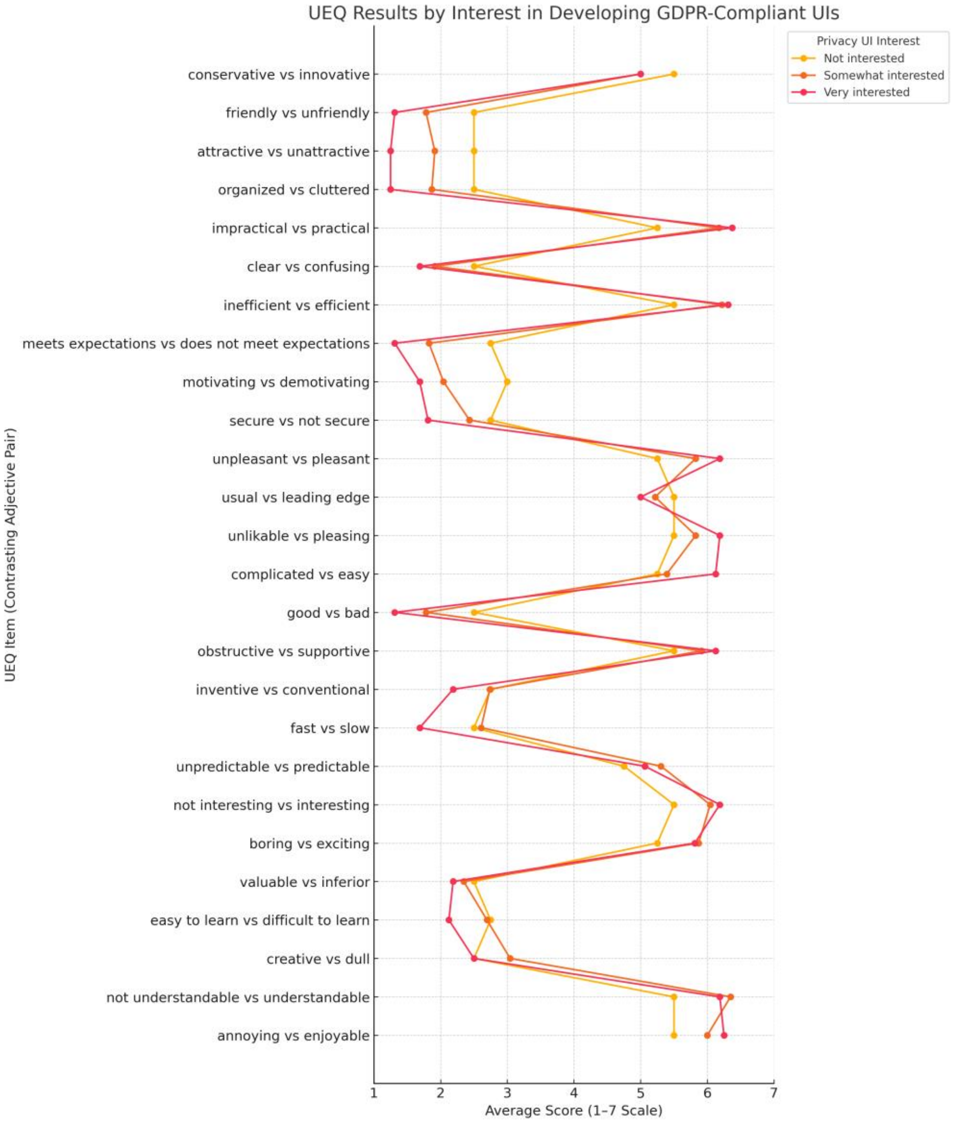


Figure 7.12 - Differentiation of UEQ scores based on privacy-compliant UI interest This chart displays how user experience ratings vary with participants' motivation to design GDPR-compliant and privacy-friendly web interfaces.

7.4.4 Overlap Between GDPR Familiarity and Web UI Interest

To explore why the UEQ correlation plots for GDPR familiarity (Question 1) and interest in developing web UIs (Question 2) were nearly identical, we examined the relationship between these two participant attributes.

A cross-tabulation analysis (Figure 7.13) revealed a clear overlap between the groups. All participants who were *very familiar* with the GDPR also reported being *very interested* in developing usable web interfaces. Similarly, most of those who were *somewhat familiar* with GDPR expressed either *some* or *high interest* in UI development.

This finding explains the similarity in patterns observed across the previous correlation charts. It suggests that participants who are more privacy-aware also tend to care more about usability and interface design. These dual interests likely shaped their evaluations of the Privacy Annotation Tool, particularly in areas like clarity, innovation, and security.

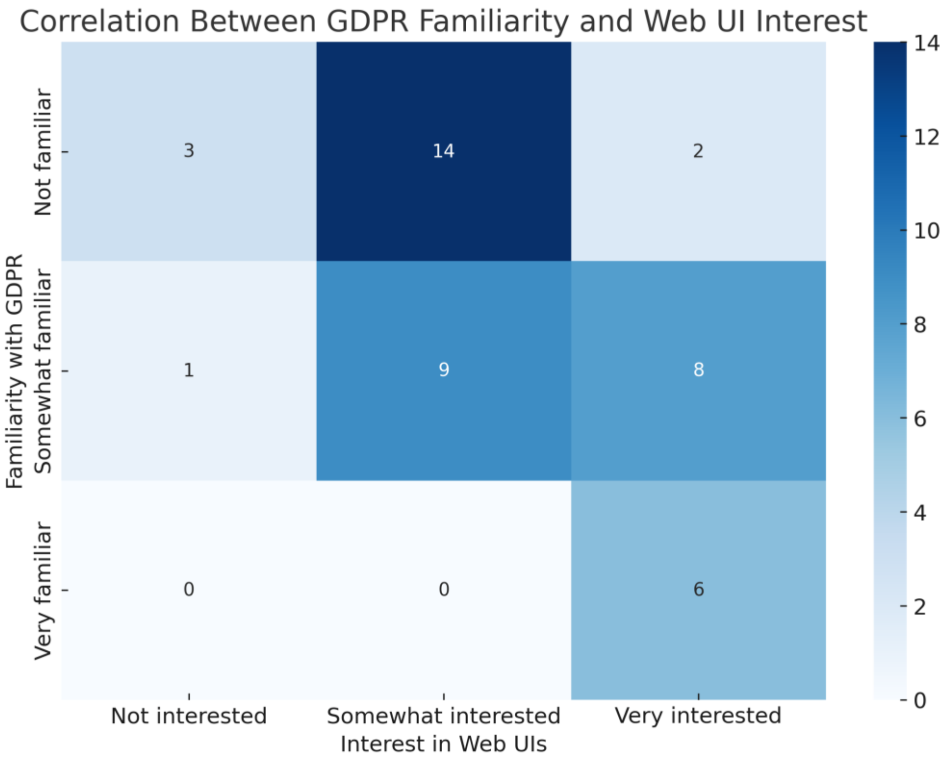


Figure 7.13 - Cross-tabulation of GDPR Familiarity vs Web UI Interest A heatmap showing the frequency distribution of participants across GDPR familiarity and web UI interest levels.

The complete set of evaluation results, including all user feedback metrics, is provided in Appendix E.

7.5 Discussion

The evaluation results indicate that the Privacy Annotation Tool received positive feedback across most dimensions, reflecting its effectiveness in enhancing privacy transparency for web forms. The results suggest that users find the tool to be clear, efficient, and innovative, aligning well with the research objectives.

Chapter 8

8. Conclusion

8.1 Final Remarks

This thesis explored the problem of GDPR-compliant transparency and usability in personal data collection on web forms and proposed a practical, research-driven solution: a browser-based Privacy Annotation Tool. The work included a broad investigation into how major online platforms communicate data collection purposes, revealing widespread gaps in field-level transparency. It also presented a user-centered design process to prototype and evaluate more transparent form designs, resulting in two preferred annotation styles.

Beyond interface design, the thesis introduced a structured database of processing purpose annotations, validated through feedback from both legal and technical experts. This database became the backbone of the tool, which was built to automatically detect form fields and allow users to apply, edit, and download HTML forms annotated with processing purposes in an accessible way. The tool was developed entirely for the browser with privacy-by-design principles and evaluated through a user experience survey, showing strong usability and clarity.

Altogether, this project combined legal compliance, usability heuristics, front-end engineering, and user feedback to offer a practical contribution to privacy-aware web development. It highlights that transparency is not only a legal requirement but a design challenge that can be addressed through thoughtful tools and research-informed solutions.

8.2 Future Work

There are many ways the tool can be improved in the future. One idea is to add smart suggestions that help developers choose the right annotation based on the field’s name and purpose. It would also be helpful to support more languages so that people around the world can use the tool. Making the tool more accessible—for example, easier to use with screen readers—should also be a priority. Another useful feature would be allowing developers and legal experts to work on the same form together, at the same time. The tool could also be connected to website-building platforms or development tools to make it easier to use during design. Testing the results of the tool with real users could help us understand if the annotations actually help people feel informed and safe. Finally, the tool could be extended to check if annotations match privacy laws like GDPR or CCPA, giving developers more confidence in their work.

Bibliography

[1] H. Bailly, A. Papanna, and R. Brennan, *Prototyping an End-User User Interface for the Solid Application Interoperability Specification under GDPR*, Dublin City University & University College Dublin, 2022. [Online]. Available: https://github.com/HBailly/solid-auth-ui/

[2] W. Brunotte, L. Chazette, L. Köhler, and K. Schneider, "What About My Privacy? Helping Users Understand Online Privacy Policies," *Proceedings of the International Conference on Software and System Processes (ICSSP)*, 2022, pp. 56–65. [Online]. Available: https://dl.acm.org/doi/10.1145/3529320.3529327

[3] W. Brunotte, A. Specht, L. Chazette, and K. Schneider, "Privacy Explanations – A Means to End-User Trust," *arXiv preprint arXiv:2210.09706*, 2022. [Online]. Available: https://arxiv.org/abs/2210.09706

[4] A. Cavoukian, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2009. [Online]. Available: https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf

[5] European Parliament and Council of the European Union, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Official Journal of the European Union, L119, pp. 1–88, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[6] M. Friedewald, "Making GDPR Usable: A Model to Support Usability Evaluations of Privacy," *arXiv preprint arXiv:1908.03503*, 2019. [Online]. Available: https://arxiv.org/abs/1908.03503

[7] Global Privacy Assembly, "Education and Public Awareness," [Online]. Available: https://globalprivacyassembly.org/news-events/gpa-awards/education-public-awareness/

[8] H. Harkous, K. Fawaz, R. Lebret, F. Schaub, K. G. Shin, and K. Aberer, "Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning," *Proceedings of the 27th USENIX Security Symposium*, 2018, pp. 531–548. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-harkous.pdf

[9] H. Harkous, K. Fawaz, K. G. Shin, and K. Aberer, "PriBots: Conversational Privacy with Chatbots," *Workshop on the Future of Privacy Notices and Indicators, 12th Symposium on Usable Privacy and Security (SOUPS)*, 2016. [Online]. Available: https://www.usenix.org/system/files/conference/soups2016/wfpn16-paper-harkous.pdf

[10] J. Nielsen, *Ten Usability Heuristics for User Interface Design*, Nielsen Norman Group, 1995. [Online]. Available: https://www.nngroup.com/articles/ten-usability-heuristics/

[11] S. L. Pfleeger and J. M. Atlee, *Software Engineering: Theory and Practice*, 3rd ed., Prentice Hall, US, 2006. [Online]. Available: https://www.pearson.com/store/p/software-engineering-theory-and-practice/P100000021383

[12] ProfileTree, "How to Design GDPR-Compliant Web Forms," ProfileTree, 2021. [Online]. Available: https://profiletree.com/how-to-design-gdpr-compliant-web-forms/

[13] J. Reidenberg, T. B. Russell, A. Callen, N. C. Norton, and S. B. Willis, “Privacy Harms and the Effectiveness of the Notice and Choice Framework,” *Berkeley Technology Law Journal*, vol. 30, no. 1, pp. 39–88, 2015. [Online]. Available: https://btlj.org/data/articles2015/vol30/30_1/0039-0088_Reidenberg_et_al_WebPdf.pdf

[14] A. L. Salgado, "Six Usable Privacy Heuristics," *Proceedings of the XXII Brazilian Symposium on Human Factors in Computing Systems (IHC)*, 2022. [Online]. Available: https://dl.acm.org/doi/10.1145/3638067.3638111

[15] F. Schaub, R. Balebako, and L. F. Cranor, "Designing Effective Privacy Notices and Controls," *IEEE Internet Computing*, vol. 21, no. 3, 2017, pp. 70–77. [Online]. Available: https://doi.org/10.1109/MIC.2017.75

[16] D. Spiekermann and F. Schaub, "Trustworthy Transparency by Design," *arXiv preprint arXiv:2103.10769*, 2021. [Online]. Available: https://arxiv.org/abs/2103.10769

[17] A. Vanezi, A. Kallenou, and G. A. Papadopoulos, "Saving the Day for Users in Web Platforms: A Chatbot-based Solution for Privacy," *10th International Conference on Behavioral and Social Computing (BESC)*, IEEE, 2023. [Online]. Available: https://www.cs.ucy.ac.cy/~george/files/BESC23.pdf

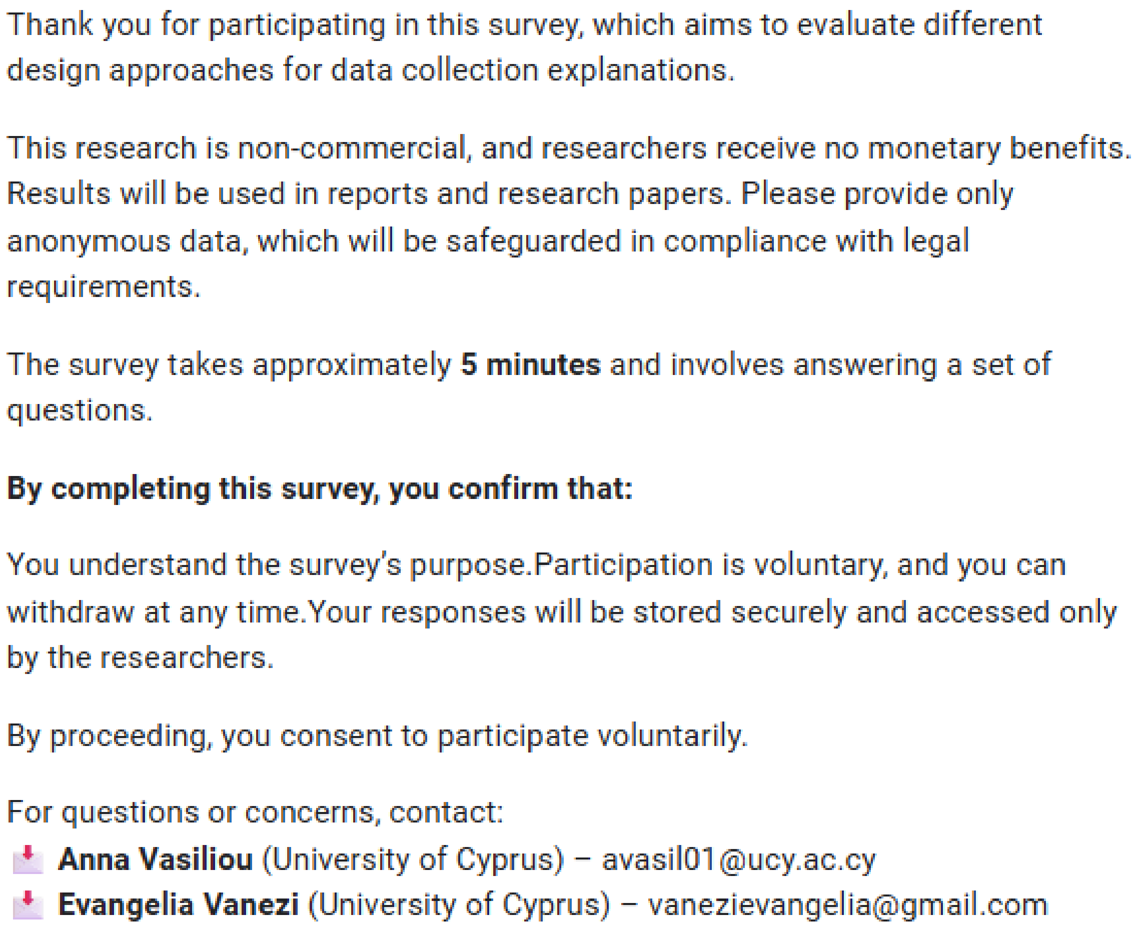
[18] W. W. Royce, "Managing the Development of Large Software Systems," *Proceedings of IEEE WESCON*, 1970. [Online]. Available: https://www.praxisframework.org/files/royce1970.pdf

[19] UserTesting, "UX Best Practices for GDPR Compliance," UserTesting, 2020. [Online]. Available: https://www.usertesting.com/blog/ux-best-practices-gdpr-compliance

[20] M. Schrepp, A. Hinderks, and J. Thomaschewski, "User Experience Questionnaire (UEQ) – An Instrument for Measuring Product Quality from the User's Perspective," 2017. Available online at UEQ-Online, accessed May 2025.

Appendix A

This appendix presents the full set of results from the questionnaire discussed in Chapter 04, which aimed to evaluate user preferences regarding different privacy annotation styles and placement strategies. The survey was conducted during the early design phase to inform the development of prototypes, helping to identify the most usable and effective annotation approaches from a user perspective.



Thank you for participating in this survey, which aims to evaluate different design approaches for data collection explanations.

This research is non-commercial, and researchers receive no monetary benefits. Results will be used in reports and research papers. Please provide only anonymous data, which will be safeguarded in compliance with legal requirements.

The survey takes approximately **5 minutes** and involves answering a set of questions.

By completing this survey, you confirm that:

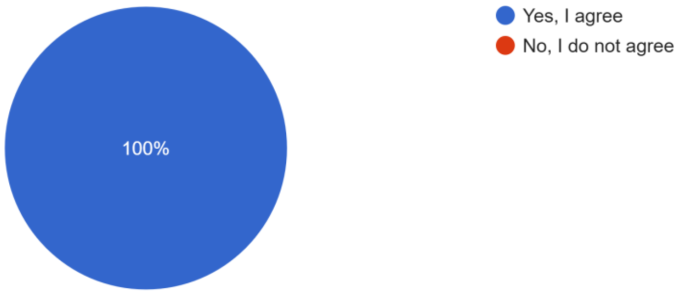
You understand the survey's purpose.Participation is voluntary, and you can withdraw at any time.Your responses will be stored securely and accessed only by the researchers.

By proceeding, you consent to participate voluntarily.

For questions or concerns, contact:
📩 **Anna Vasiliou** (University of Cyprus) – avasil01@ucy.ac.cy
📩 **Evangelia Vanezi** (University of Cyprus) – vanezievangelia@gmail.com

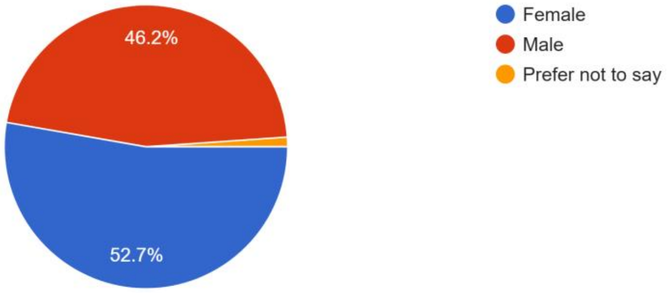
Thank you for participating in this survey, which aims to evaluate different design approaches for data collection explanations. This research is no...(University of Cyprus) – vanezievangelia@gmail.com

90 responses



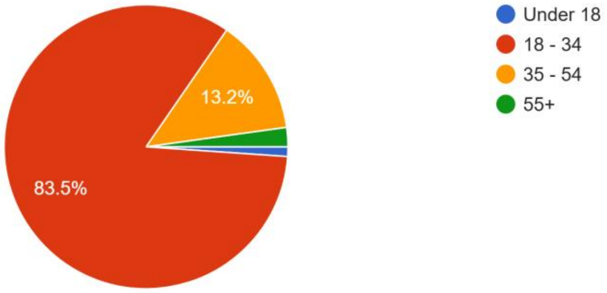
1. Sex

91 responses



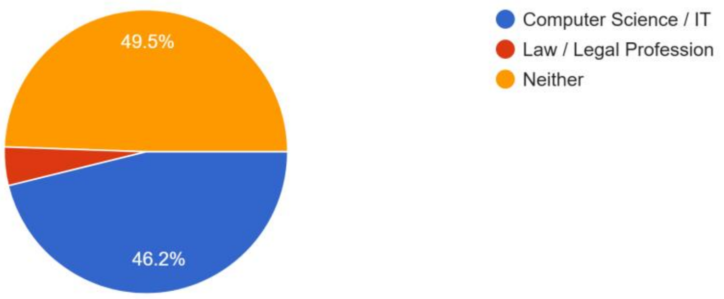
2. Age Group

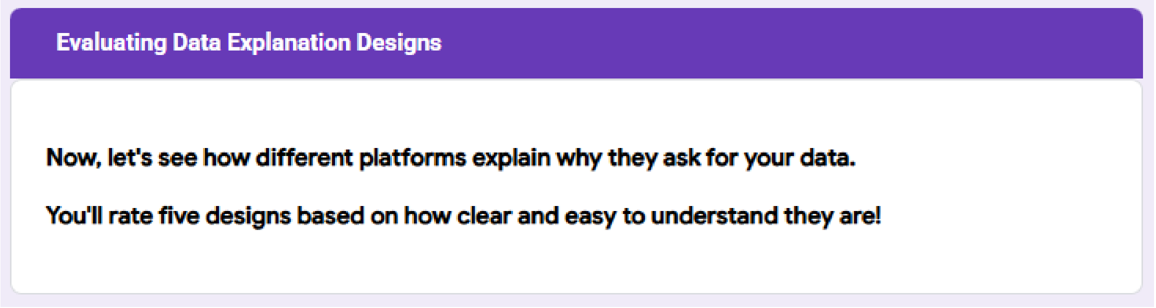
91 responses



3. Occupation Background Is your occupation related to any of the following fields?

91 responses





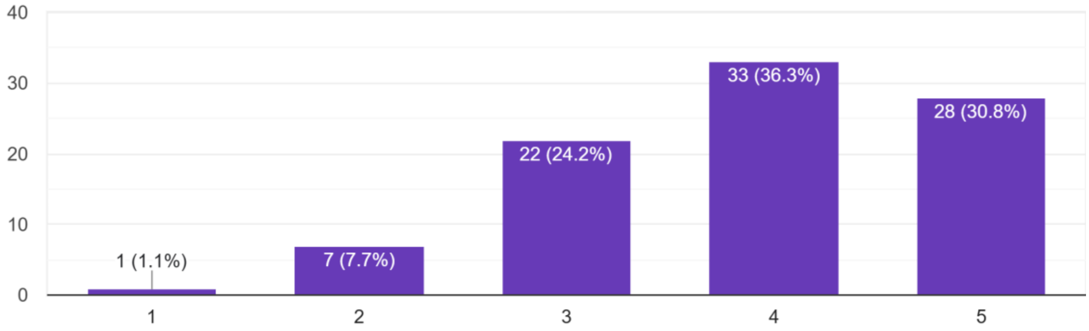
Evaluating Data Explanation Designs

Now, let's see how different platforms explain why they ask for your data.

You'll rate five designs based on how clear and easy to understand they are!

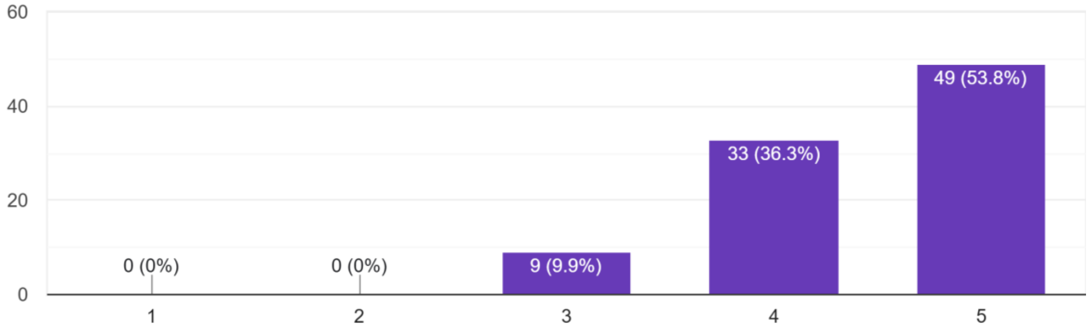
Icon Pop-Up Messages: How would you rate this design?

91 responses



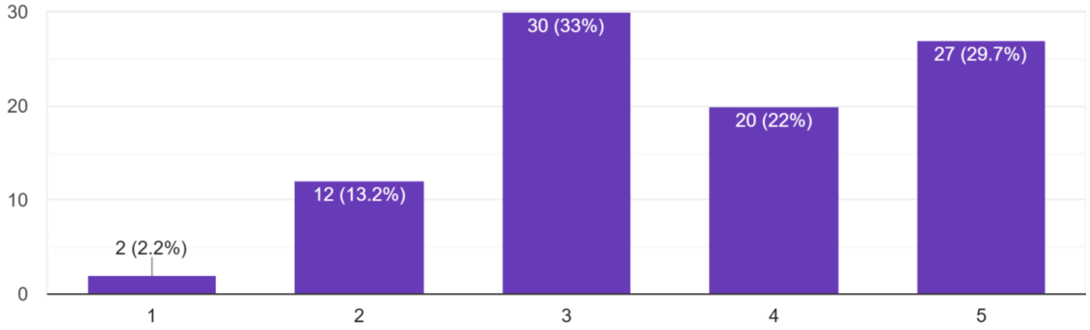
Short Explanation Next to the Field: How would you rate this design?

91 responses



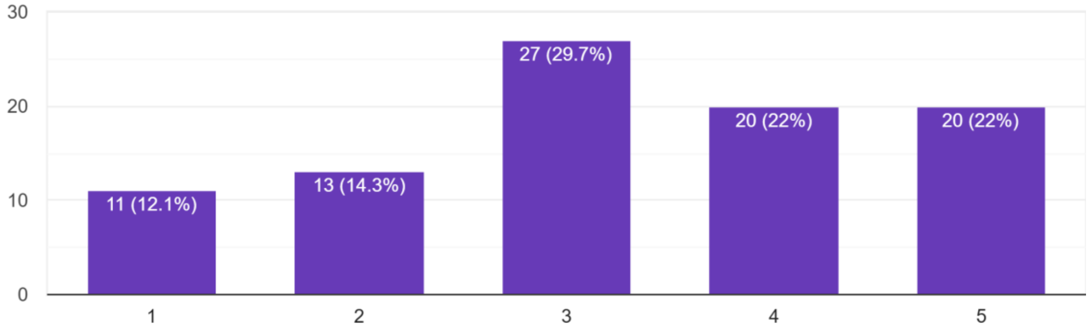
One General Explanation for All Fields: How would you rate this design?

91 responses



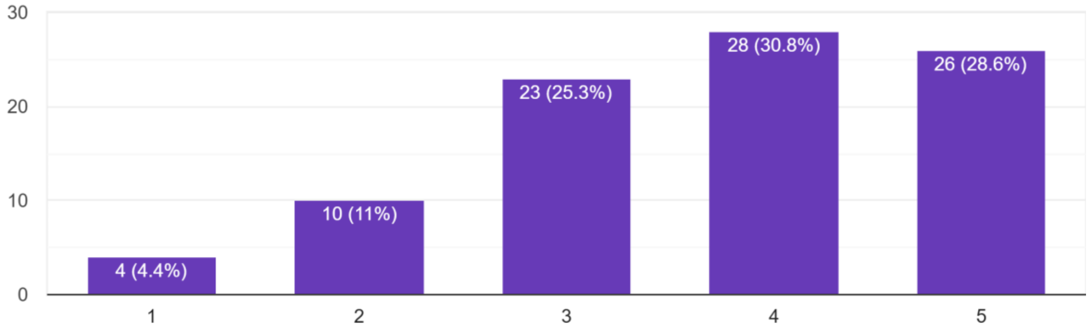
Clickable Link to More Information: How would you rate this design?

91 responses



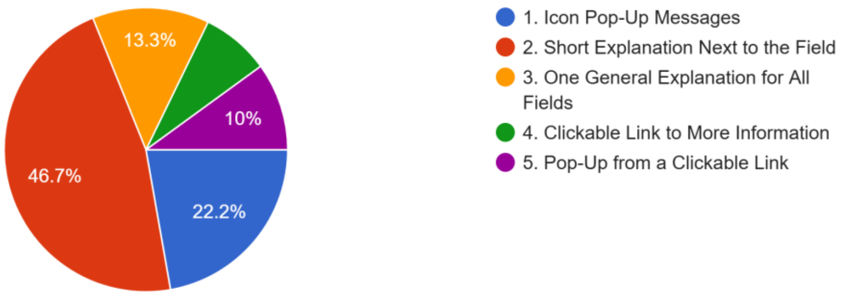
Pop-Up from a Clickable Link: How would you rate this design?

91 responses



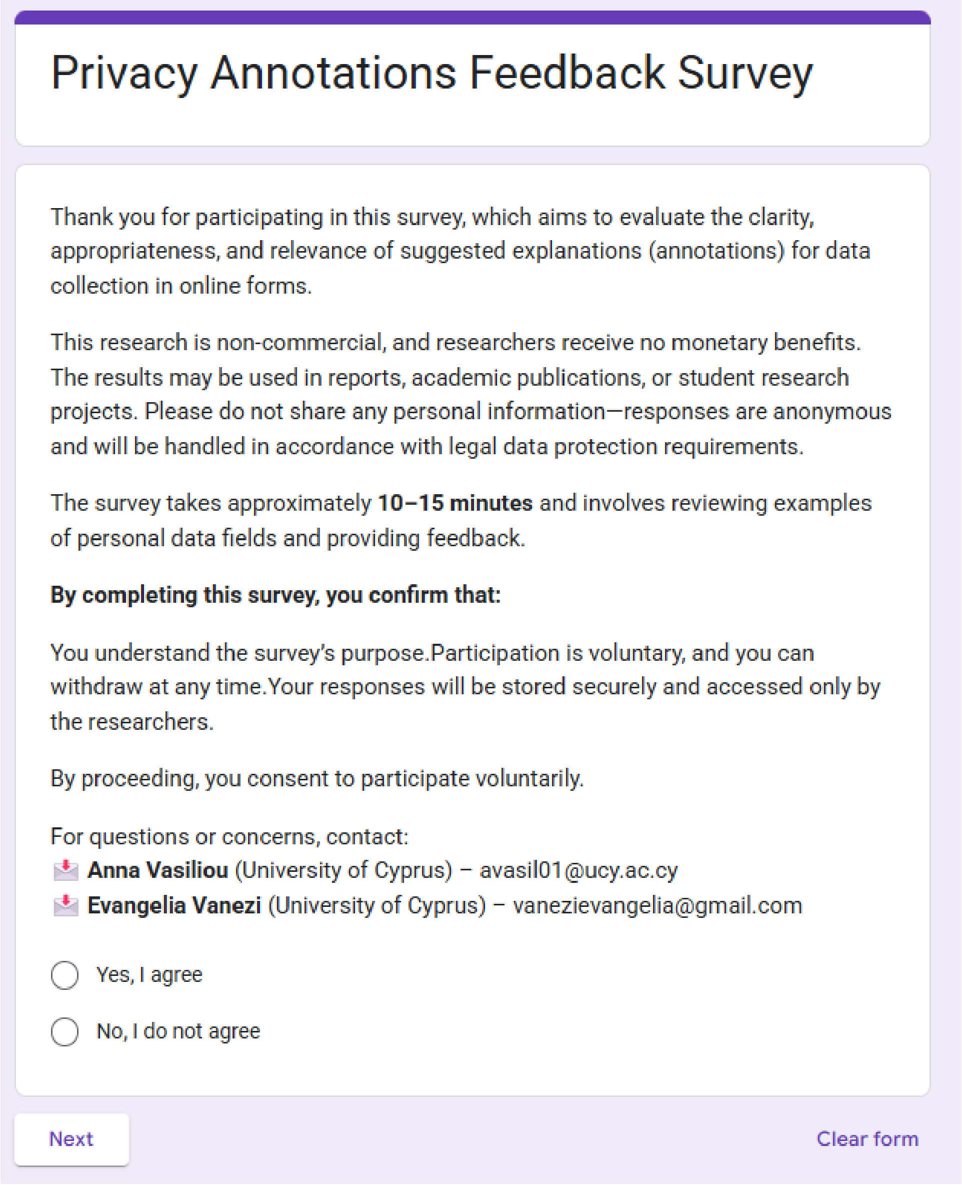
Which category do you think transmits the purpose of collecting data most clearly and effectively to you?

90 responses



Appendix B

This appendix includes the full questionnaire used in **Chapter 05** to evaluate the clarity, appropriateness, and relevance of suggested privacy annotation descriptions. The survey was distributed to legal and technical experts as part of the assessment of the annotation database, providing essential feedback for the final version presented in this thesis.



Privacy Annotations Feedback Survey

Thank you for participating in this survey, which aims to evaluate the clarity, appropriateness, and relevance of suggested explanations (annotations) for data collection in online forms.

This research is non-commercial, and researchers receive no monetary benefits. The results may be used in reports, academic publications, or student research projects. Please do not share any personal information—responses are anonymous and will be handled in accordance with legal data protection requirements.

The survey takes approximately **10–15 minutes** and involves reviewing examples of personal data fields and providing feedback.

By completing this survey, you confirm that:

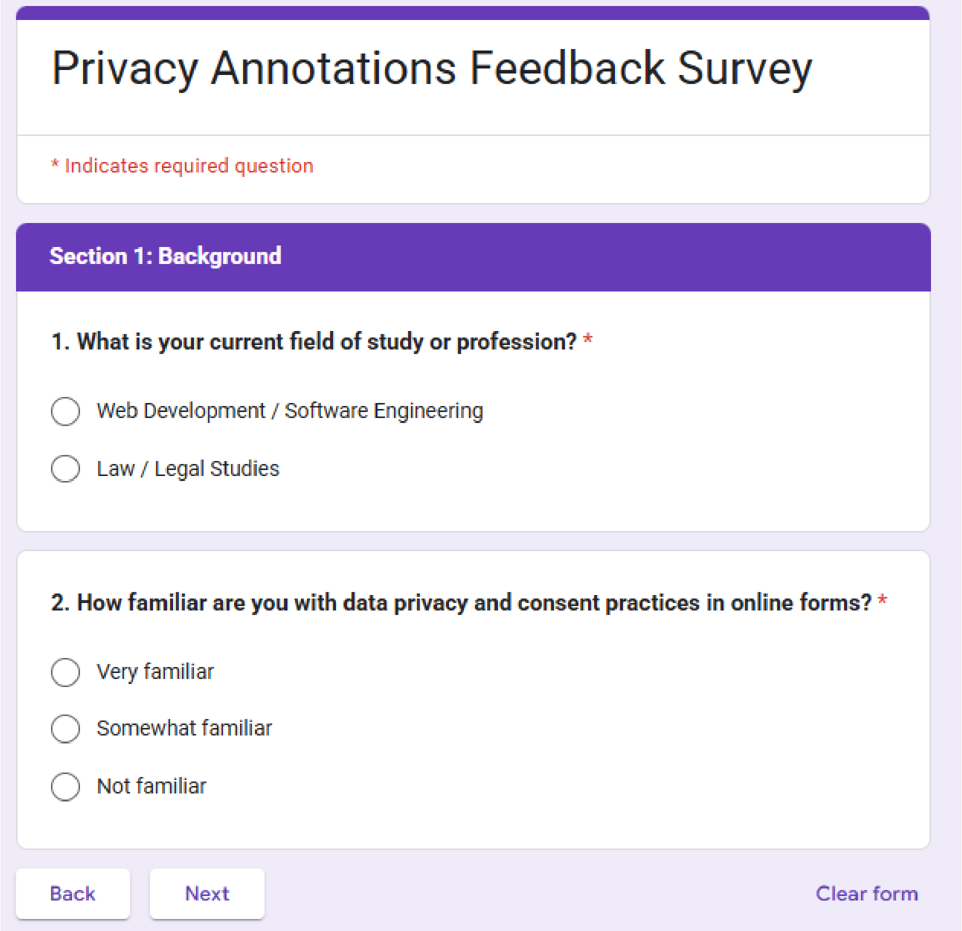
You understand the survey's purpose.Participation is voluntary, and you can withdraw at any time.Your responses will be stored securely and accessed only by the researchers.

By proceeding, you consent to participate voluntarily.

For questions or concerns, contact:
📩 **Anna Vasiliou** (University of Cyprus) – avasil01@ucy.ac.cy
📩 **Evangelia Vanezi** (University of Cyprus) – vanezievangelia@gmail.com

○ Yes, I agree

○ No, I do not agree



Privacy Annotations Feedback Survey

* Indicates required question

Section 1: Background

1. What is your current field of study or profession? *

○ Web Development / Software Engineering

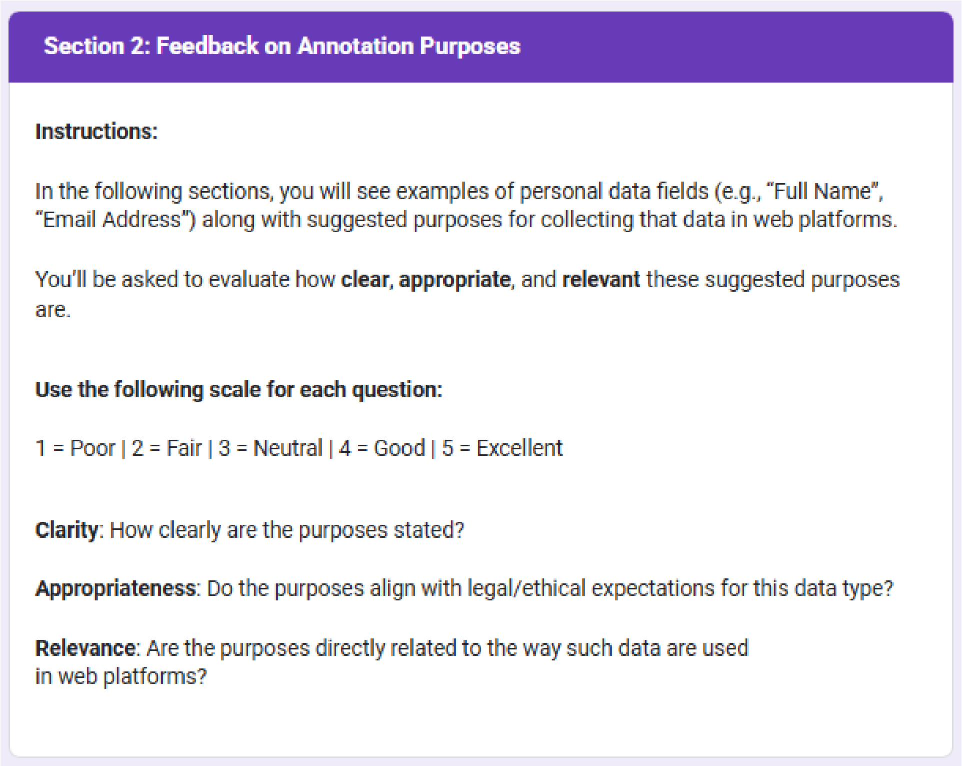
○ Law / Legal Studies

2. How familiar are you with data privacy and consent practices in online forms? *

○ Very familiar

○ Somewhat familiar

○ Not familiar



Section 2: Feedback on Annotation Purposes

Instructions:

In the following sections, you will see examples of personal data fields (e.g., “Full Name”, “Email Address”) along with suggested purposes for collecting that data in web platforms.

You’ll be asked to evaluate how **clear**, **appropriate**, and **relevant** these suggested purposes are.

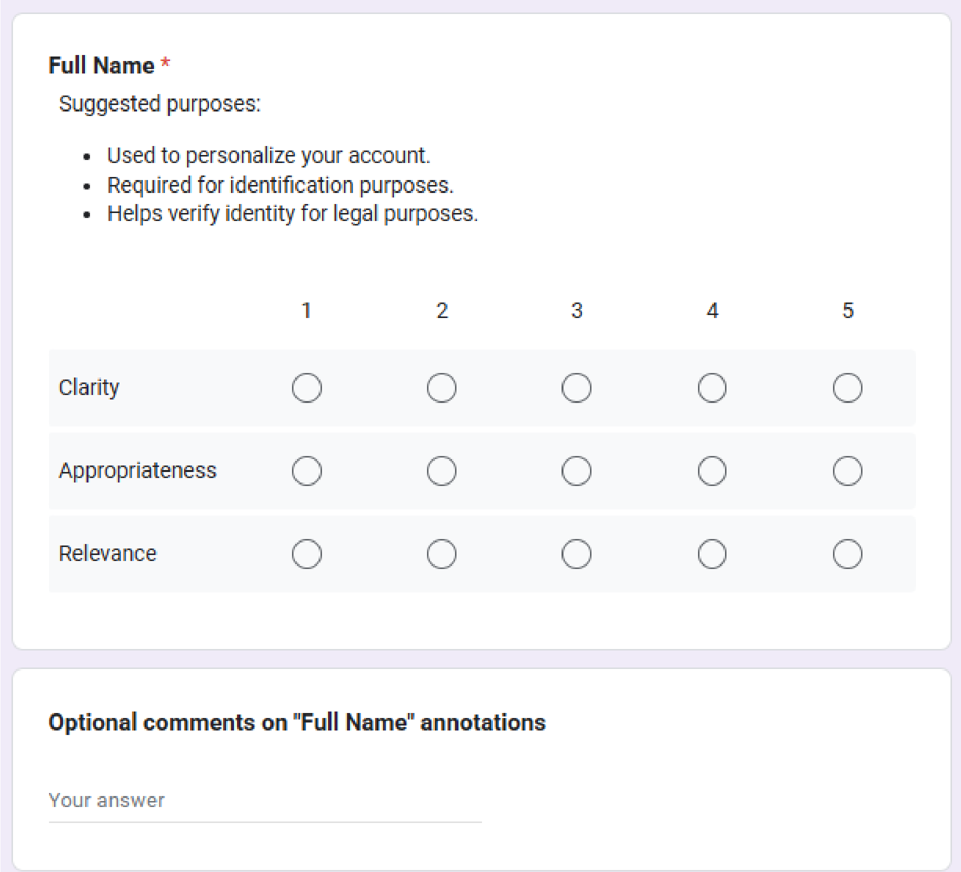
Use the following scale for each question:

1 = Poor | 2 = Fair | 3 = Neutral | 4 = Good | 5 = Excellent

Clarity: How clearly are the purposes stated?

Appropriateness: Do the purposes align with legal/ethical expectations for this data type?

Relevance: Are the purposes directly related to the way such data are used in web platforms?



Full Name *

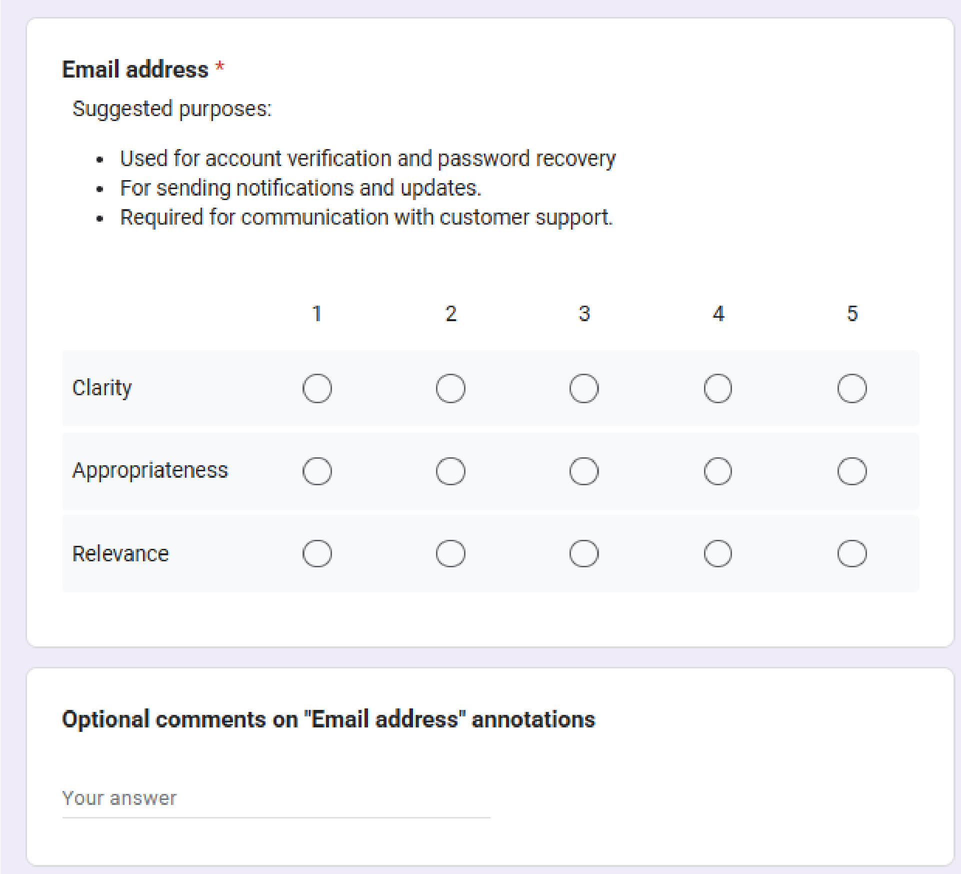
Suggested purposes:

- Used to personalize your account.
- Required for identification purposes.
- Helps verify identity for legal purposes.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Full Name" annotations

Your answer



Email address *

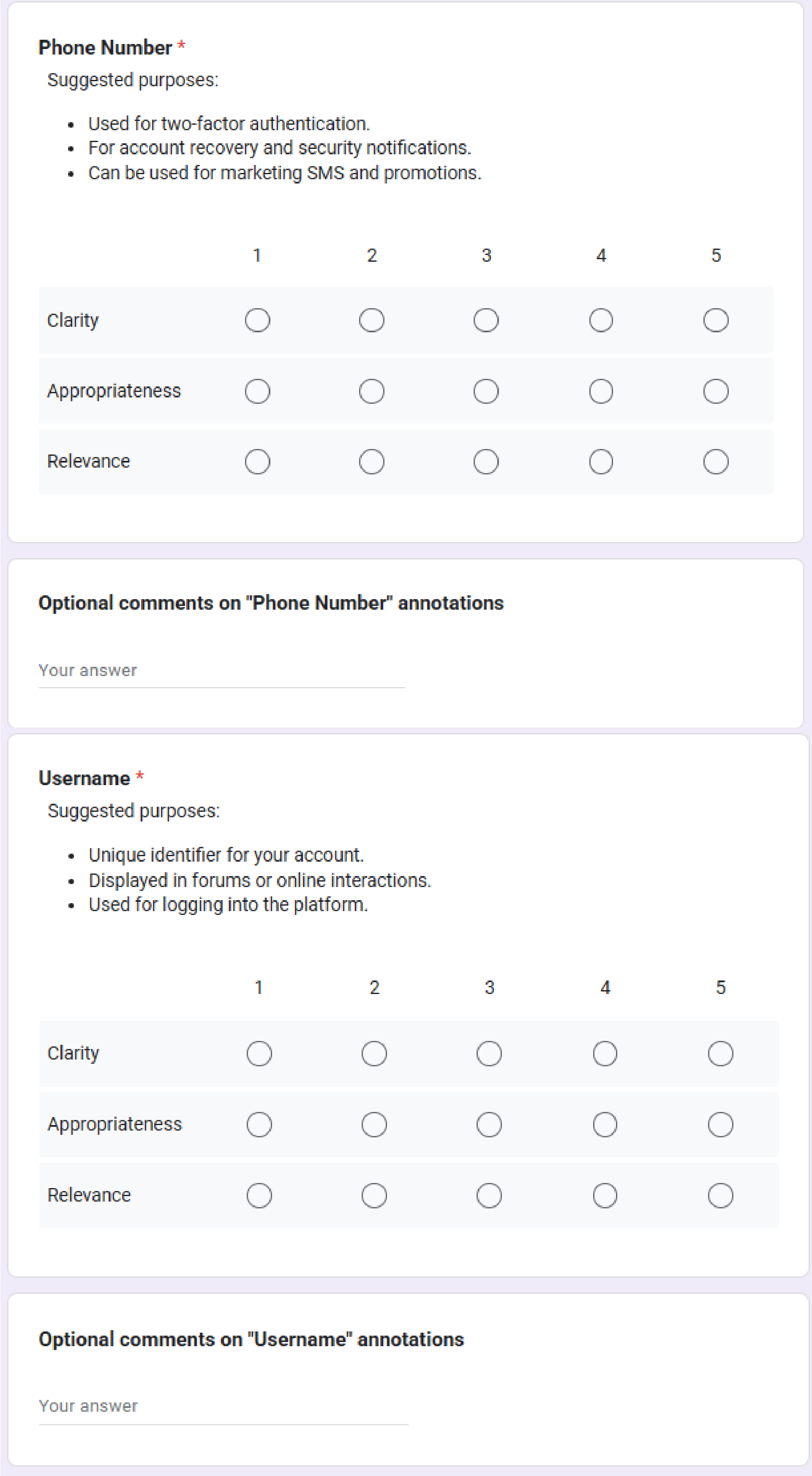
Suggested purposes:

- Used for account verification and password recovery
- For sending notifications and updates.
- Required for communication with customer support.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Email address" annotations

Your answer



Phone Number *

Suggested purposes:

- Used for two-factor authentication.
- For account recovery and security notifications.
- Can be used for marketing SMS and promotions.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Phone Number" annotations

Your answer

Username *

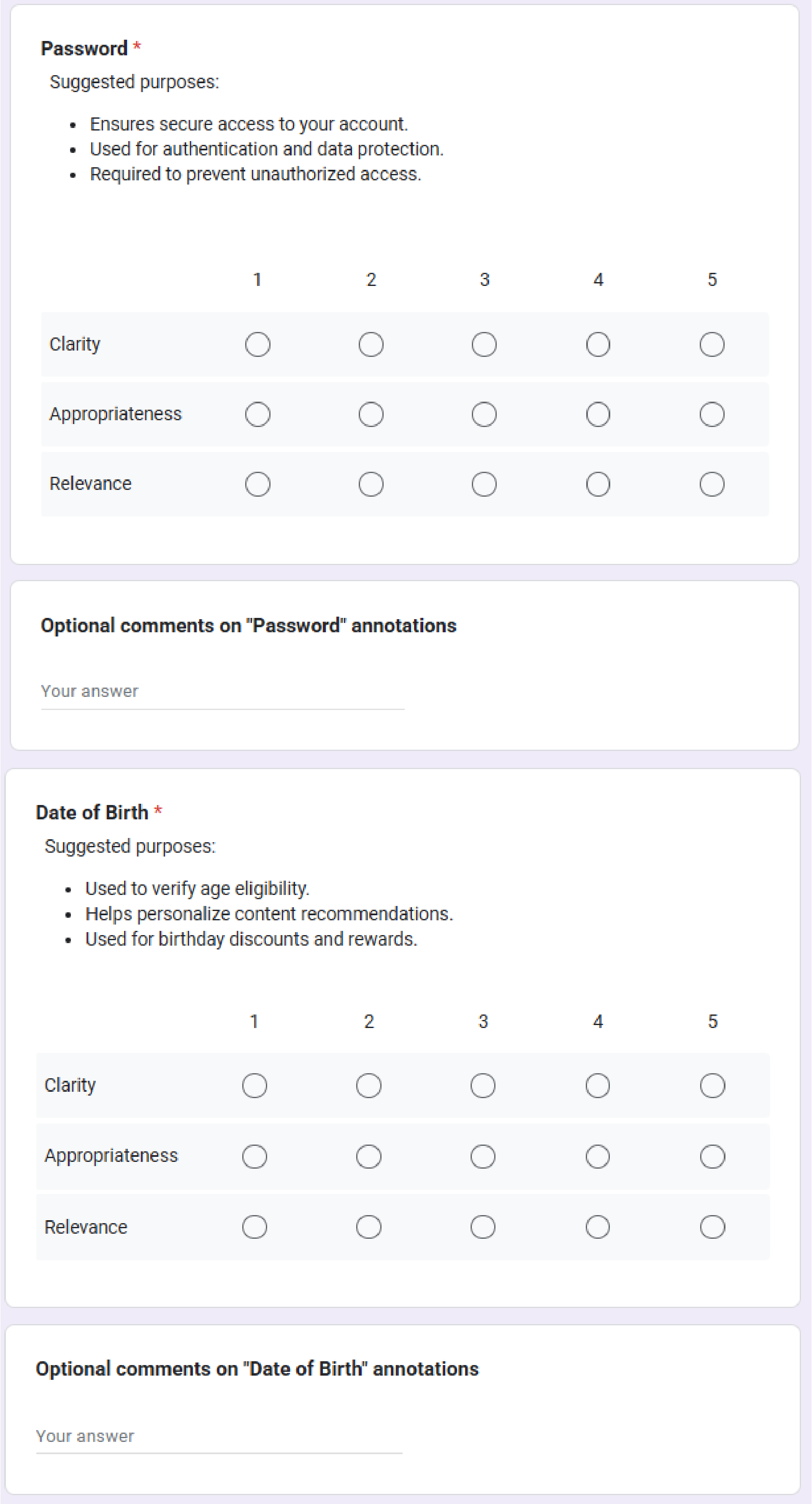
Suggested purposes:

- Unique identifier for your account.
- Displayed in forums or online interactions.
- Used for logging into the platform.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Username" annotations

Your answer



Password *

Suggested purposes:

- Ensures secure access to your account.
- Used for authentication and data protection.
- Required to prevent unauthorized access.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Password" annotations

Your answer

Date of Birth *

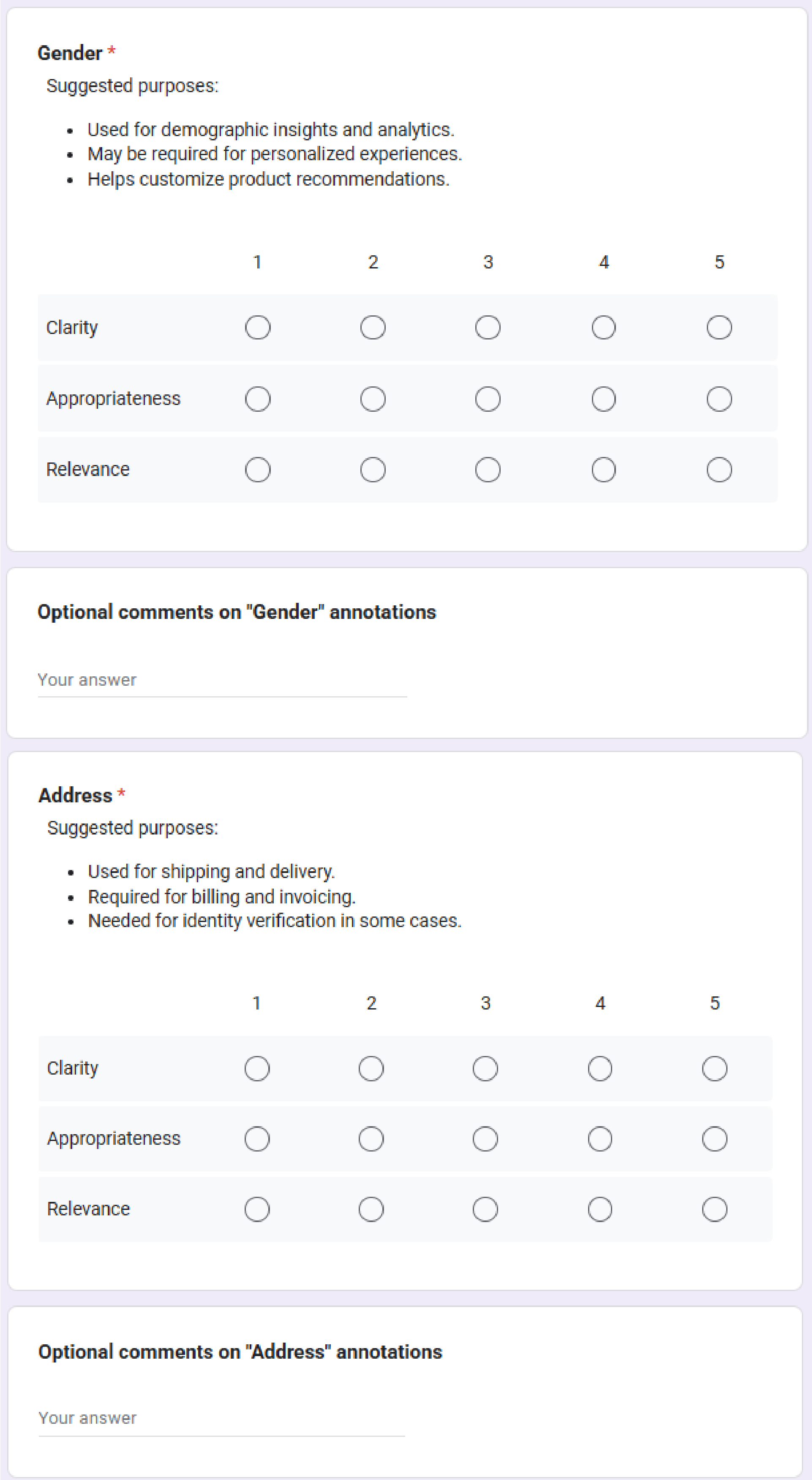
Suggested purposes:

- Used to verify age eligibility.
- Helps personalize content recommendations.
- Used for birthday discounts and rewards.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Date of Birth" annotations

Your answer



Gender *

Suggested purposes:

- Used for demographic insights and analytics.
- May be required for personalized experiences.
- Helps customize product recommendations.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Gender" annotations

Your answer

Address *

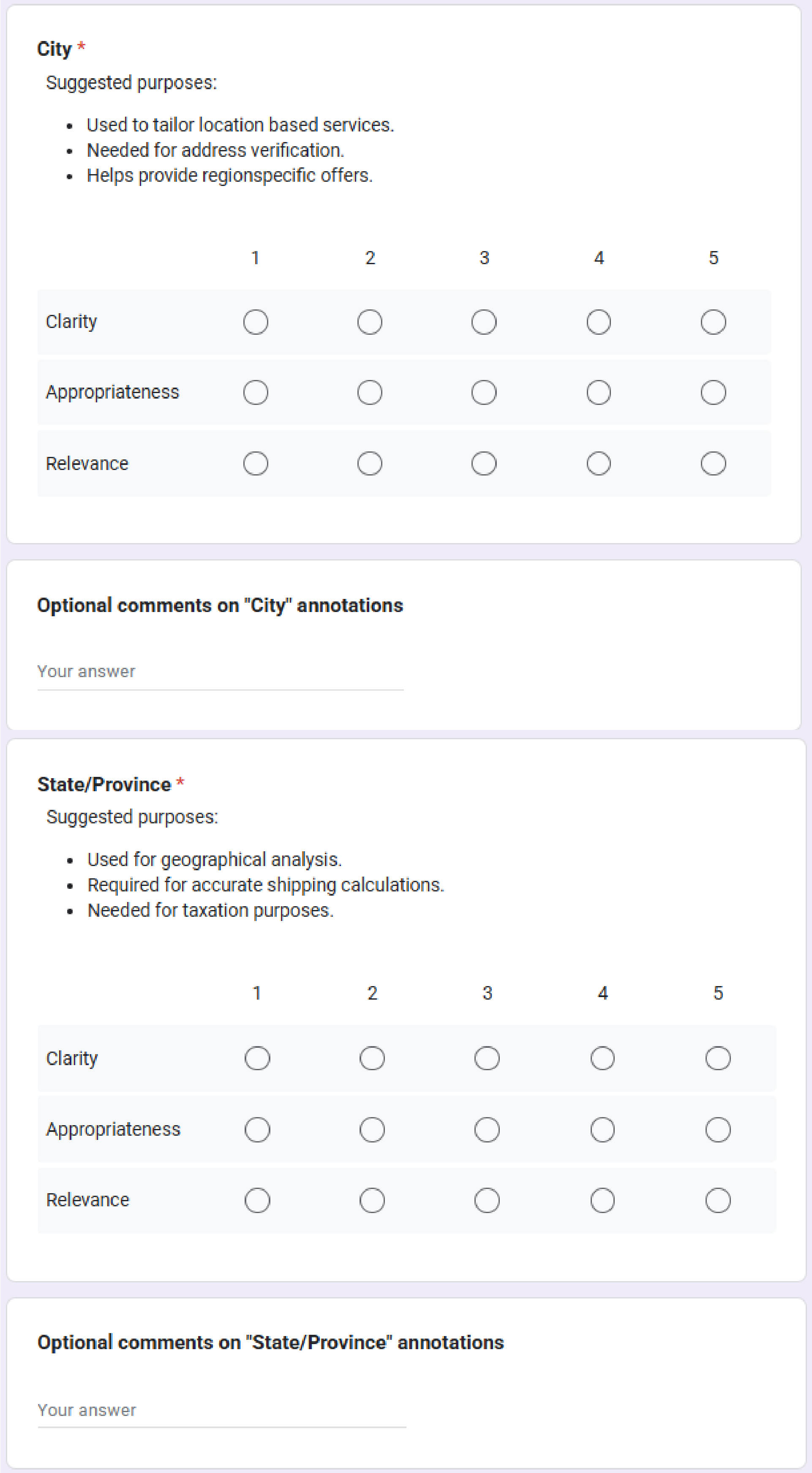
Suggested purposes:

- Used for shipping and delivery.
- Required for billing and invoicing.
- Needed for identity verification in some cases.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Address" annotations

Your answer



City *

Suggested purposes:

- Used to tailor location based services.
- Needed for address verification.
- Helps provide regionspecific offers.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "City" annotations

Your answer

State/Province *

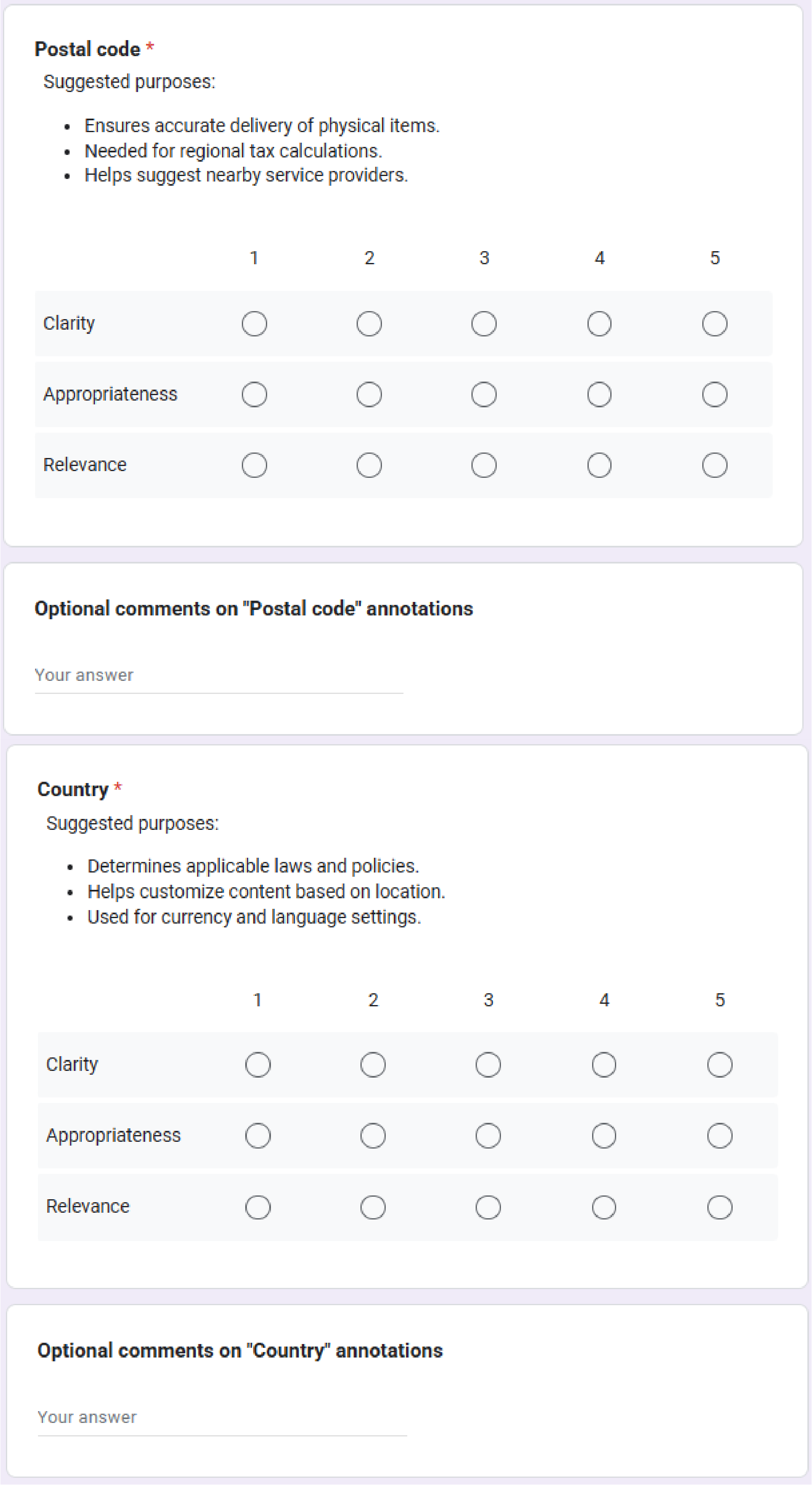
Suggested purposes:

- Used for geographical analysis.
- Required for accurate shipping calculations.
- Needed for taxation purposes.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "State/Province" annotations

Your answer



Postal code *

Suggested purposes:

- Ensures accurate delivery of physical items.
- Needed for regional tax calculations.
- Helps suggest nearby service providers.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Postal code" annotations

Your answer

Country *

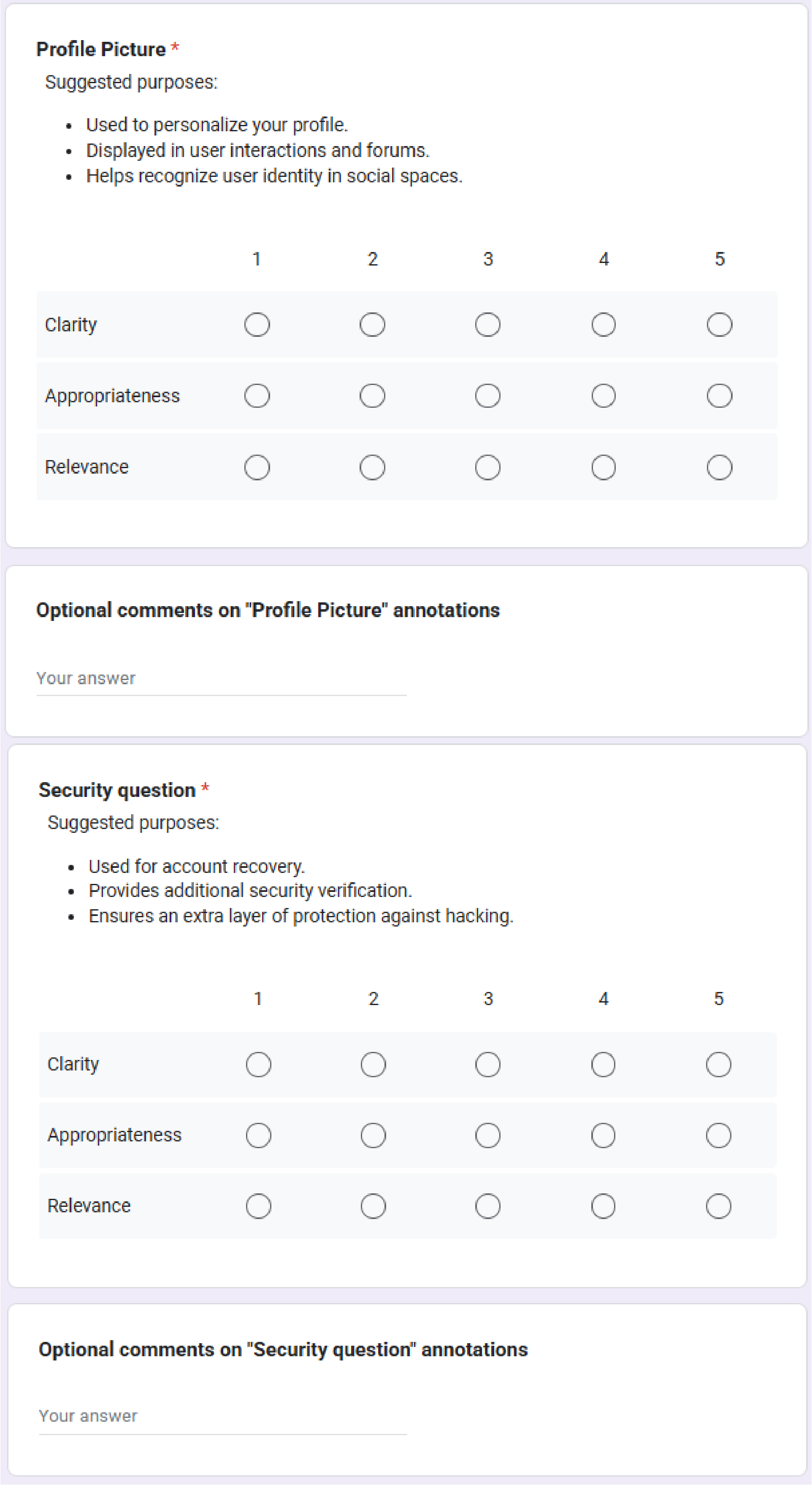
Suggested purposes:

- Determines applicable laws and policies.
- Helps customize content based on location.
- Used for currency and language settings.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Country" annotations

Your answer



Profile Picture *

Suggested purposes:

- Used to personalize your profile.
- Displayed in user interactions and forums.
- Helps recognize user identity in social spaces.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Profile Picture" annotations

Your answer

Security question *

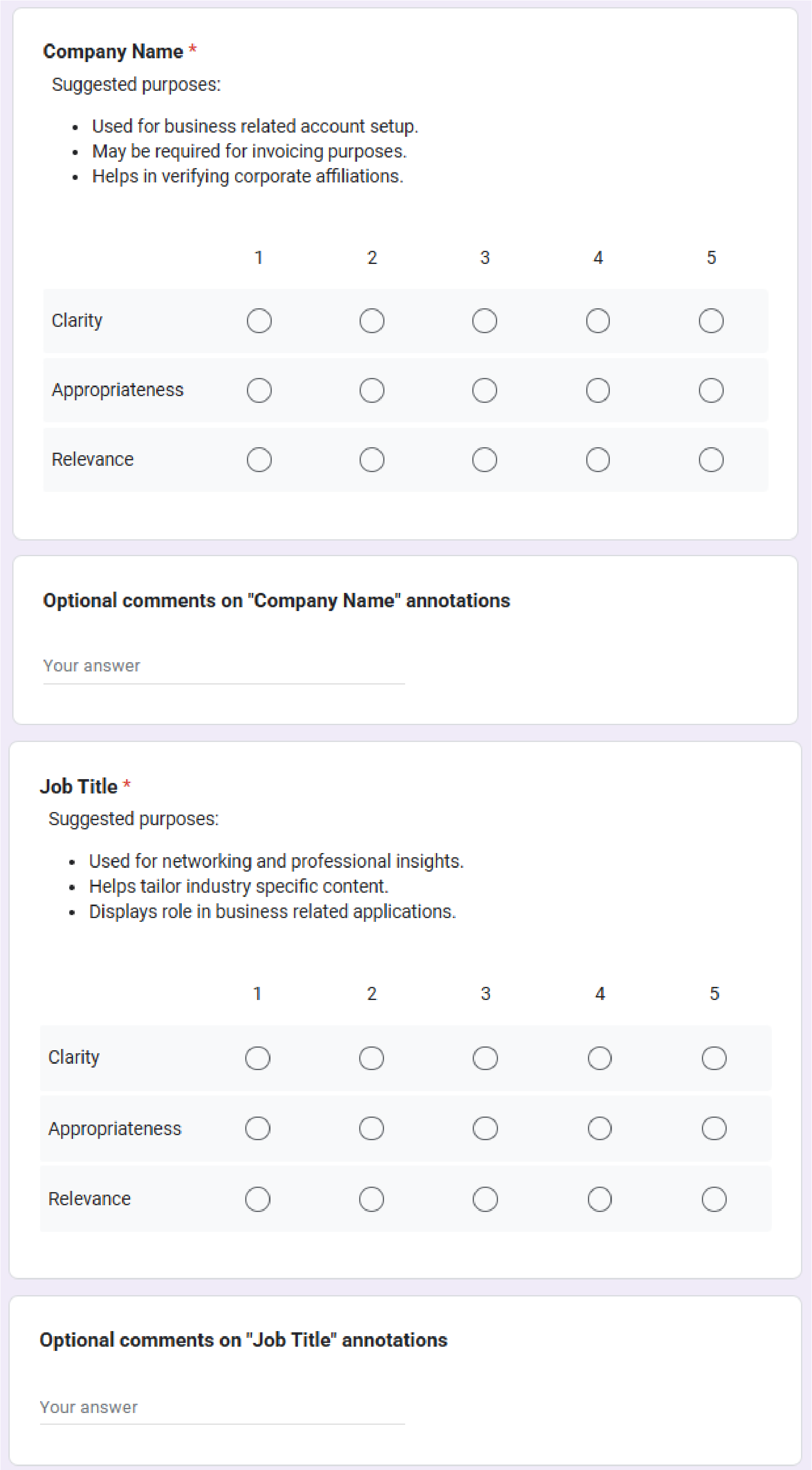
Suggested purposes:

- Used for account recovery.
- Provides additional security verification.
- Ensures an extra layer of protection against hacking.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Security question" annotations

Your answer



Company Name *

Suggested purposes:

- Used for business related account setup.
- May be required for invoicing purposes.
- Helps in verifying corporate affiliations.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Company Name" annotations

Your answer

Job Title *

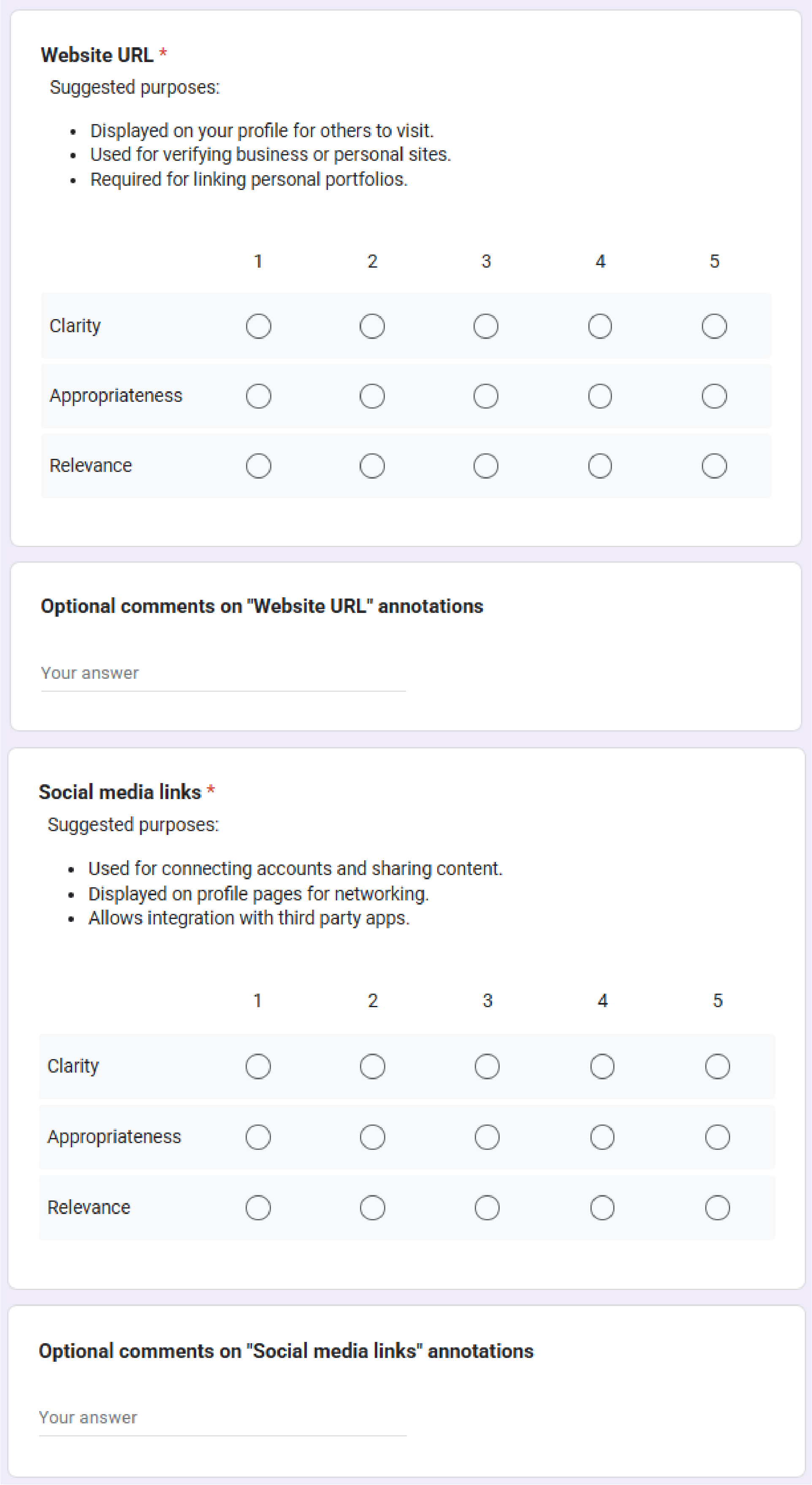
Suggested purposes:

- Used for networking and professional insights.
- Helps tailor industry specific content.
- Displays role in business related applications.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Job Title" annotations

Your answer



Website URL *

Suggested purposes:

- Displayed on your profile for others to visit.
- Used for verifying business or personal sites.
- Required for linking personal portfolios.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Website URL" annotations

Your answer

Social media links *

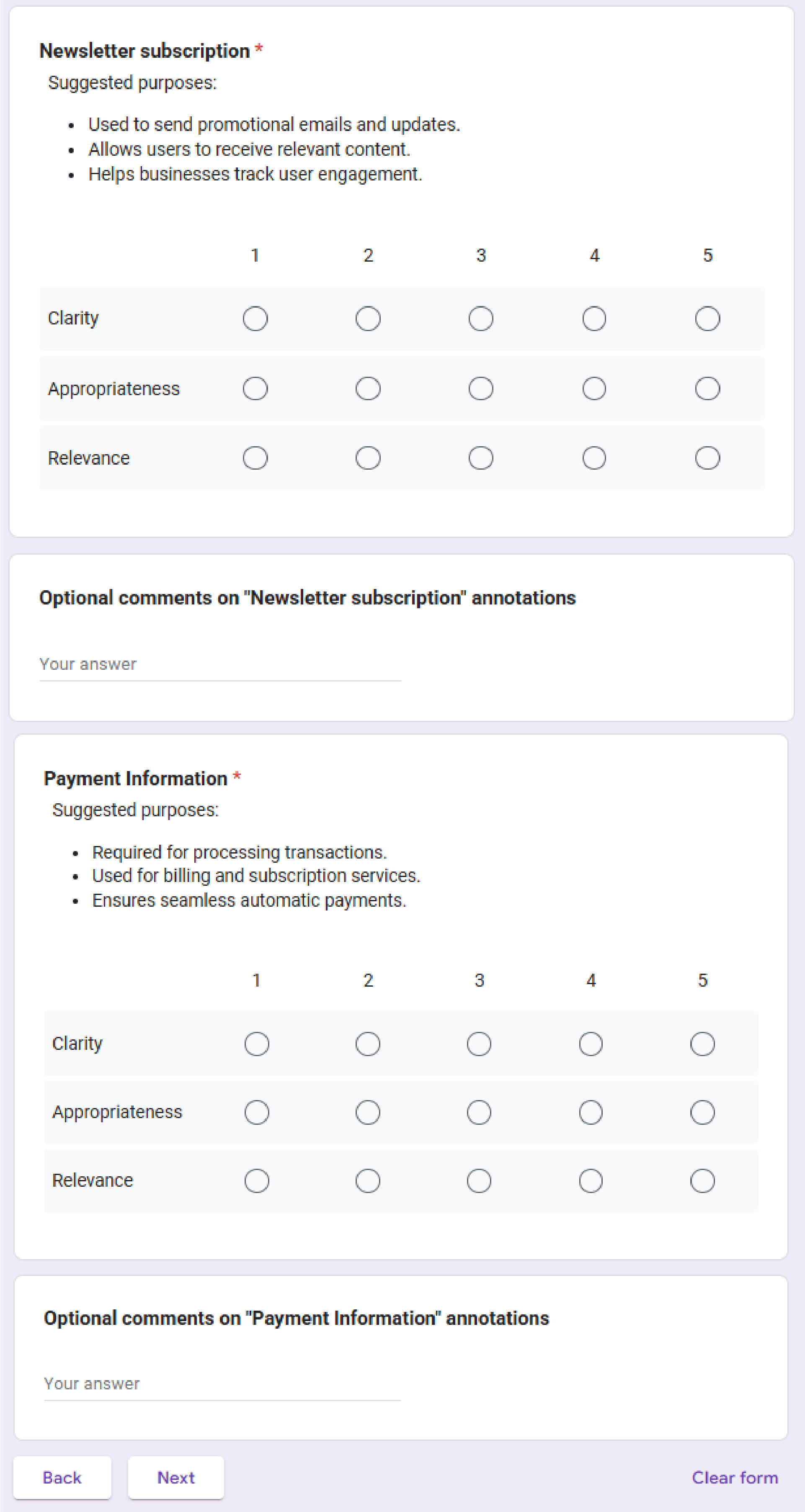
Suggested purposes:

- Used for connecting accounts and sharing content.
- Displayed on profile pages for networking.
- Allows integration with third party apps.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Social media links" annotations

Your answer



Newsletter subscription *

Suggested purposes:

- Used to send promotional emails and updates.
- Allows users to receive relevant content.
- Helps businesses track user engagement.

	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Newsletter subscription" annotations

Your answer

Payment Information *

Suggested purposes:

- Required for processing transactions.
- Used for billing and subscription services.
- Ensures seamless automatic payments.

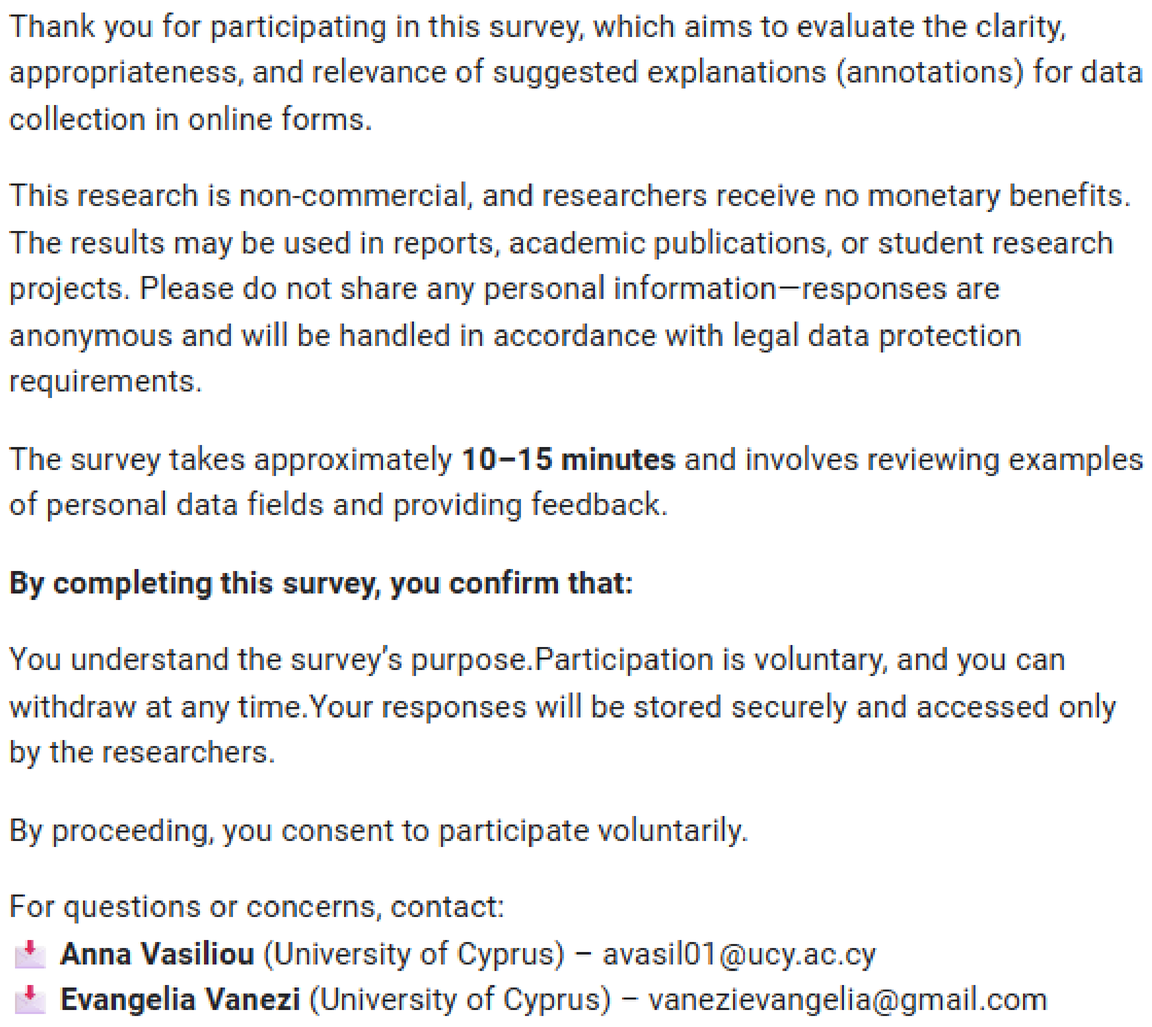
	1	2	3	4	5
Clarity	○	○	○	○	○
Appropriateness	○	○	○	○	○
Relevance	○	○	○	○	○

Optional comments on "Payment Information" annotations

Your answer

Appendix C

This appendix contains the detailed results of the annotation evaluation questionnaire presented in **Chapter 05**. It includes participant ratings for clarity, appropriateness, and relevance across multiple form field annotations. These results supported the refinement of the annotation database and informed the final selection of annotation descriptions integrated into the tool.



Thank you for participating in this survey, which aims to evaluate the clarity, appropriateness, and relevance of suggested explanations (annotations) for data collection in online forms.

This research is non-commercial, and researchers receive no monetary benefits. The results may be used in reports, academic publications, or student research projects. Please do not share any personal information—responses are anonymous and will be handled in accordance with legal data protection requirements.

The survey takes approximately **10–15 minutes** and involves reviewing examples of personal data fields and providing feedback.

By completing this survey, you confirm that:

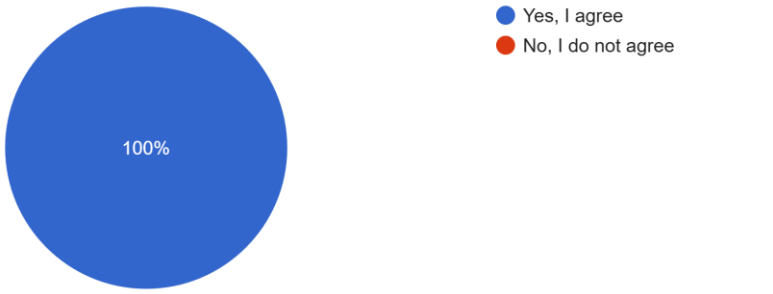
You understand the survey's purpose.Participation is voluntary, and you can withdraw at any time.Your responses will be stored securely and accessed only by the researchers.

By proceeding, you consent to participate voluntarily.

For questions or concerns, contact:
📥 **Anna Vasiliou** (University of Cyprus) – avasil01@ucy.ac.cy
📥 **Evangelia Vanezi** (University of Cyprus) – vanezievangelia@gmail.com

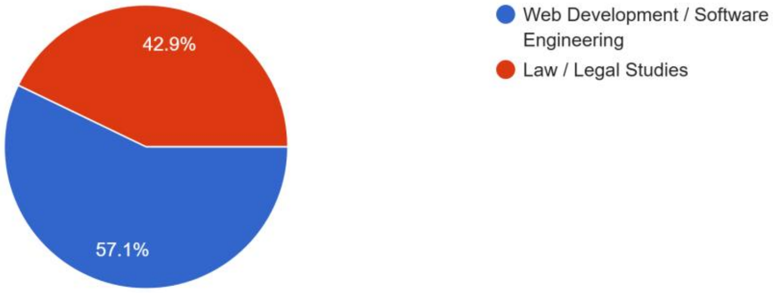
Thank you for participating in this survey, which aims to evaluate the clarity, appropriateness, and relevance of suggested explanations (annotations)...niversity of Cyprus) – vanezievangelia@gmail.com

14 responses



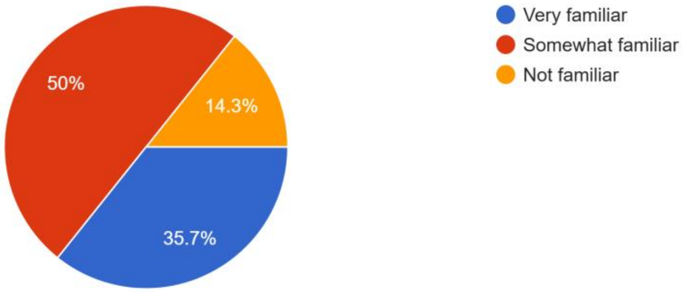
1. What is your current field of study or profession?

14 responses

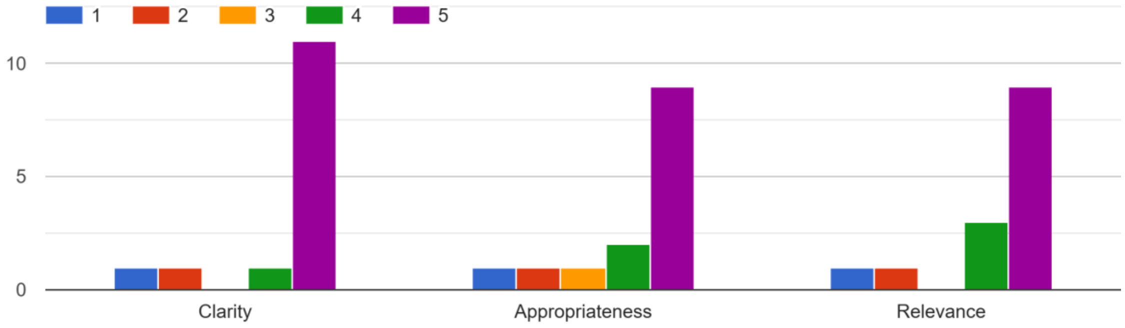


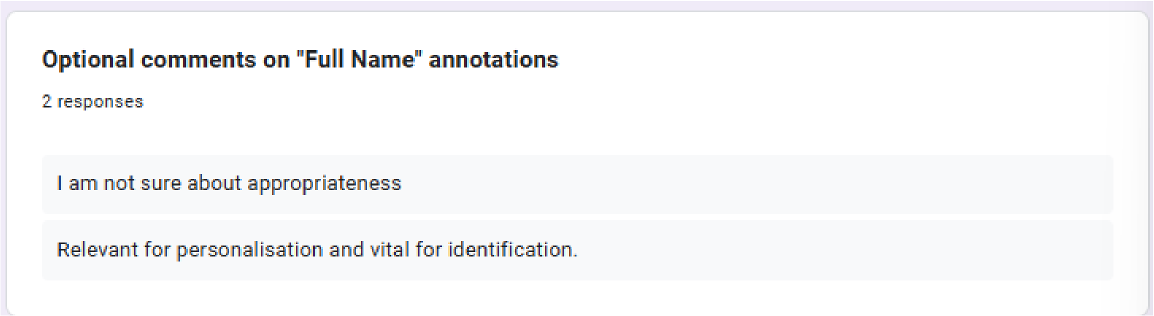
2. How familiar are you with data privacy and consent practices in online forms?

14 responses



Full Name





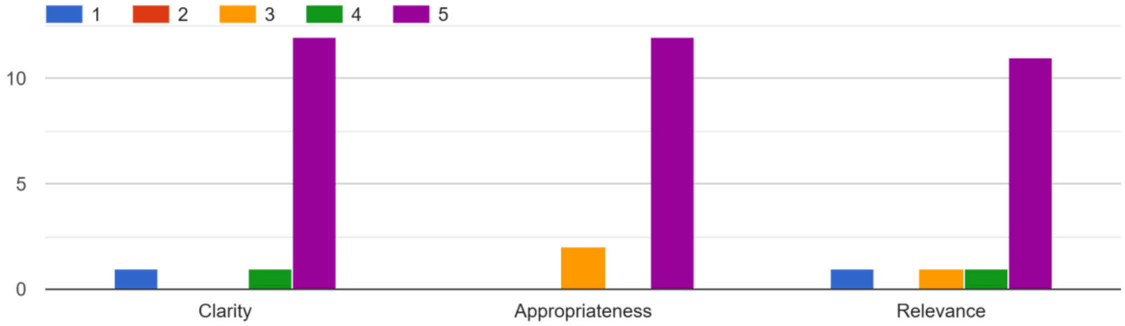
Optional comments on "Full Name" annotations

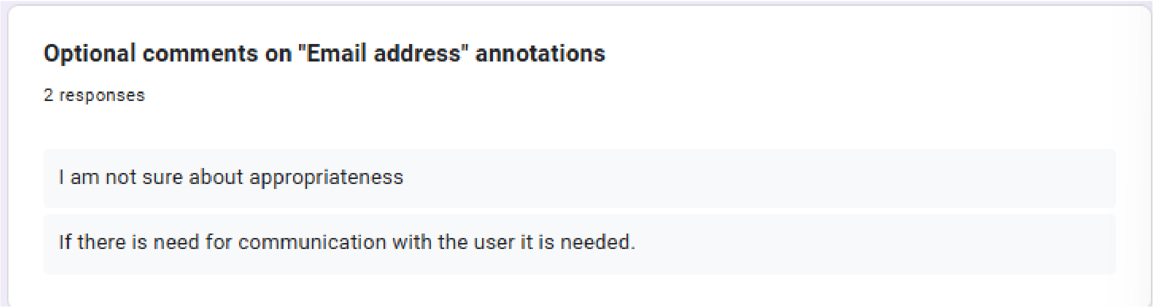
2 responses

I am not sure about appropriateness

Relevant for personalisation and vital for identification.

Email address





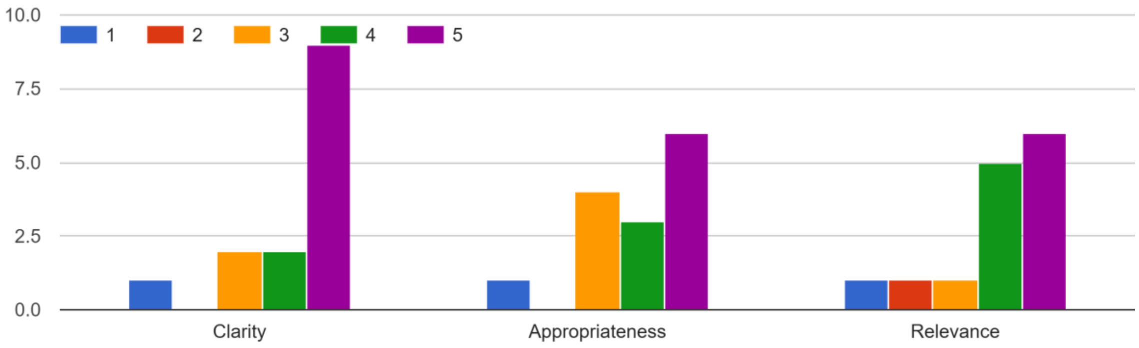
Optional comments on "Email address" annotations

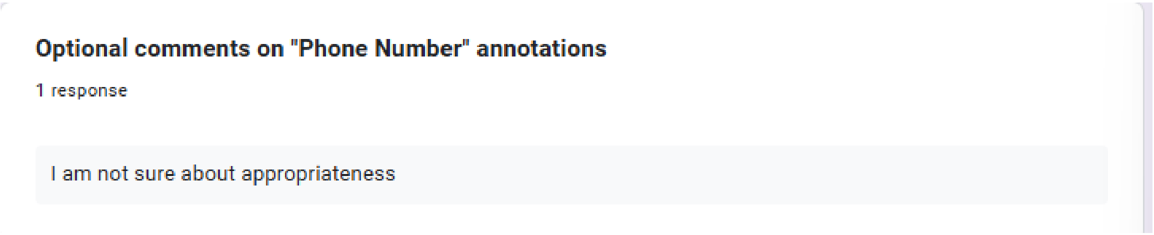
2 responses

I am not sure about appropriateness

If there is need for communication with the user it is needed.

Phone Number



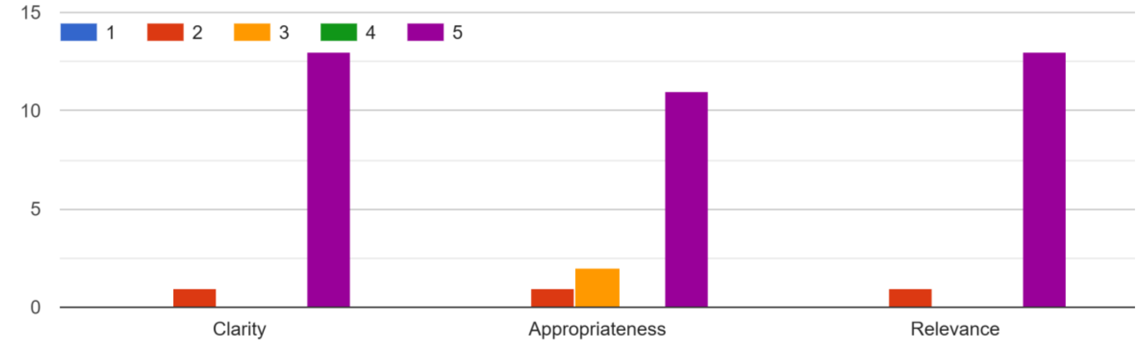


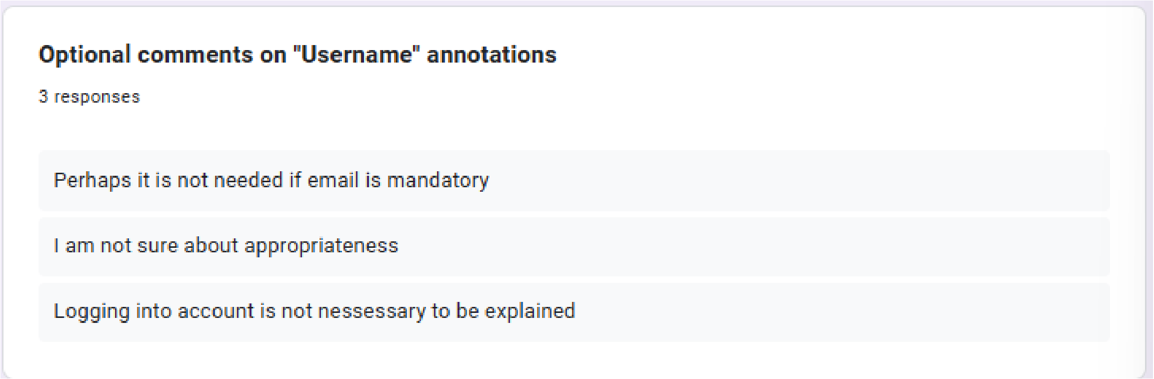
Optional comments on "Phone Number" annotations

1 response

I am not sure about appropriateness

Username





Optional comments on "Username" annotations

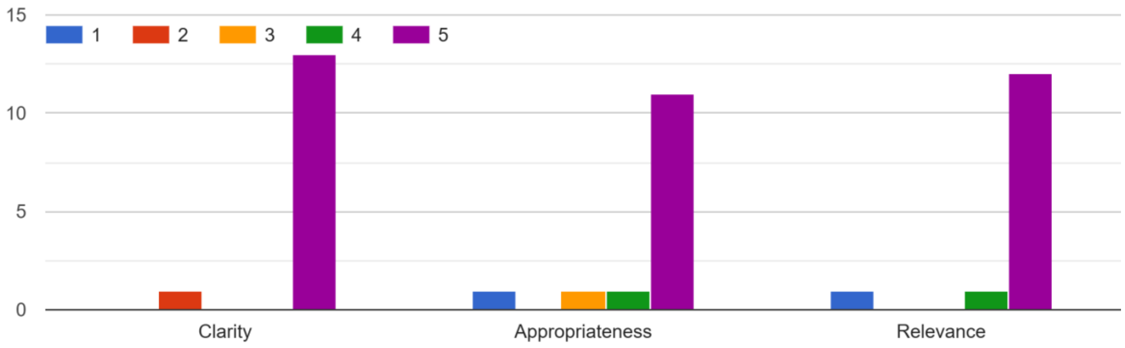
3 responses

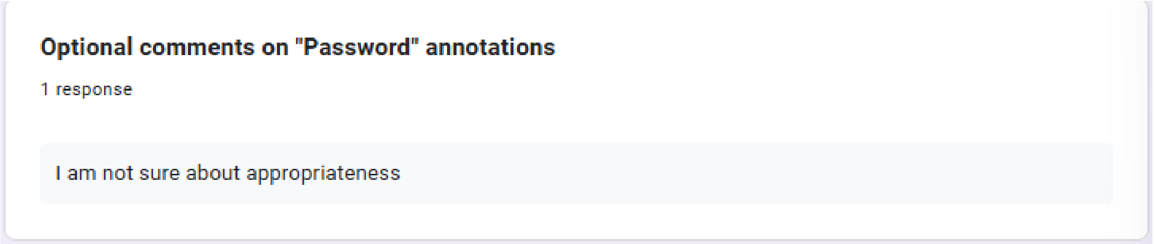
Perhaps it is not needed if email is mandatory

I am not sure about appropriateness

Logging into account is not nessessary to be explained

Password



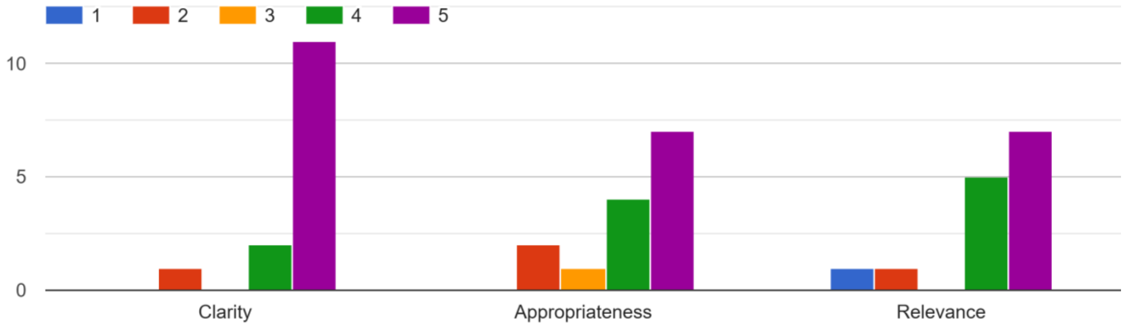


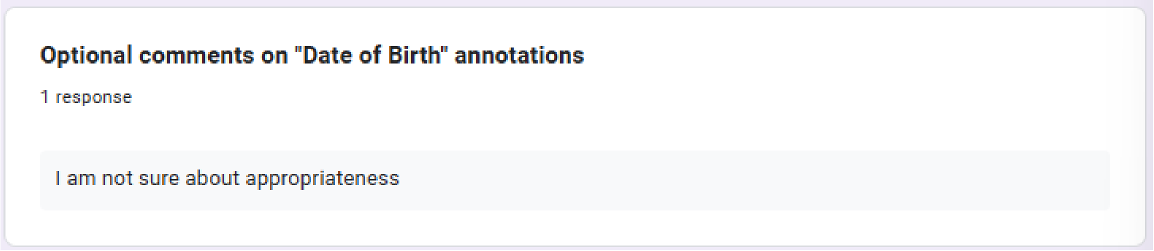
Optional comments on "Password" annotations

1 response

I am not sure about appropriateness

Date of Birth

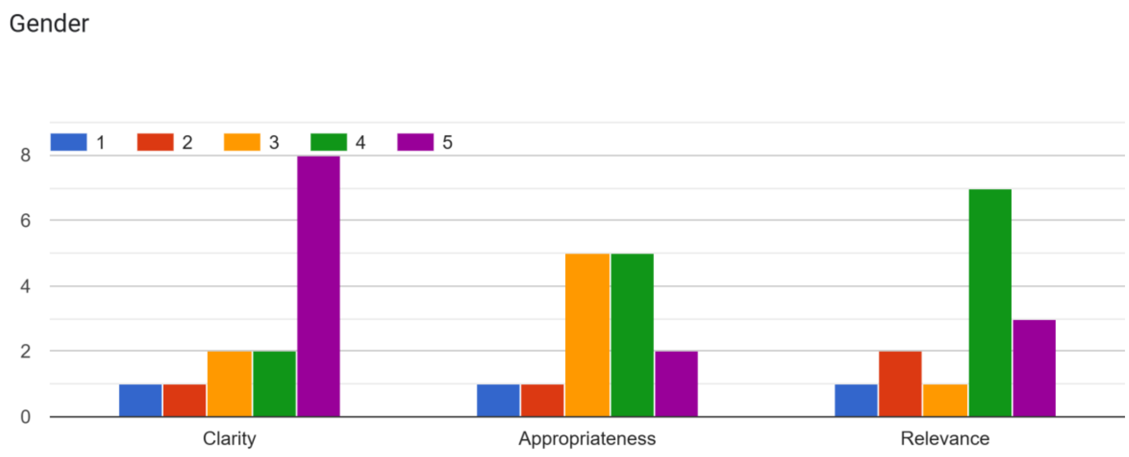




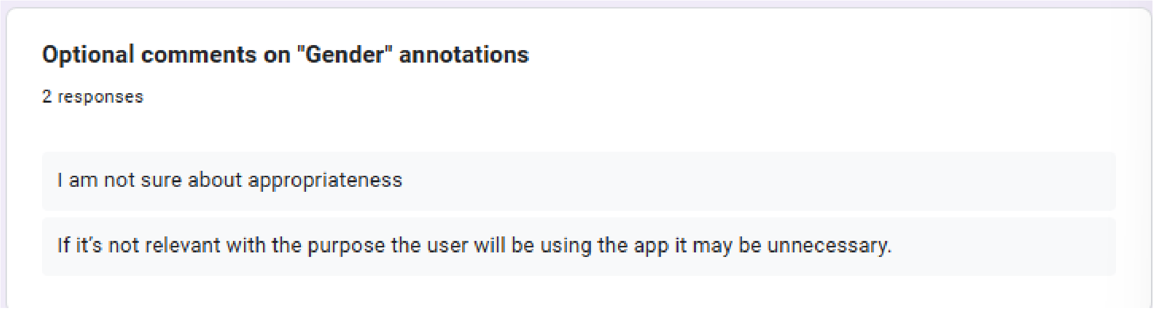
Optional comments on "Date of Birth" annotations

1 response

I am not sure about appropriateness



Gender

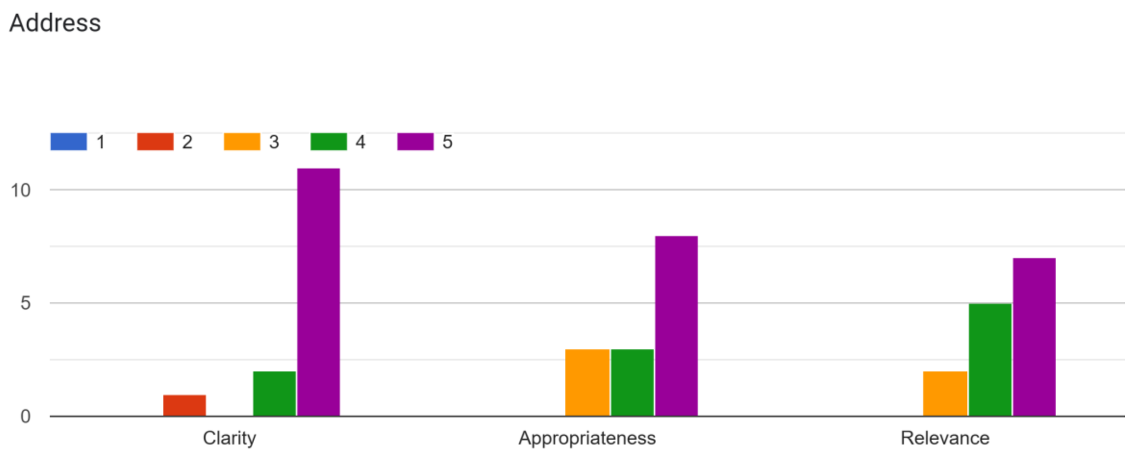


Optional comments on "Gender" annotations

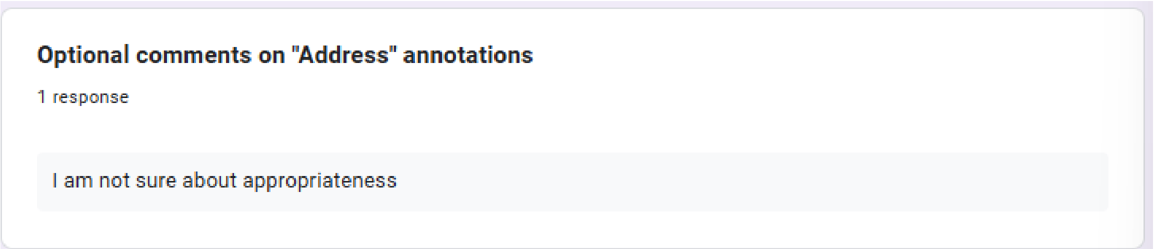
2 responses

I am not sure about appropriateness

If it’s not relevant with the purpose the user will be using the app it may be unnecessary.



Address

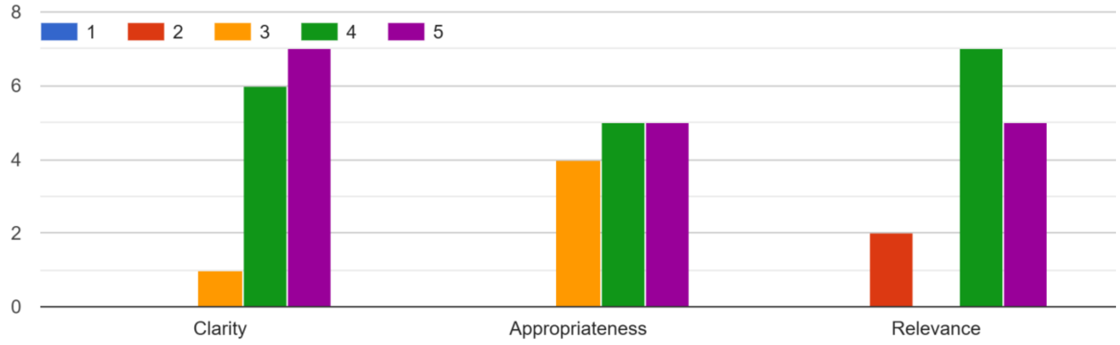


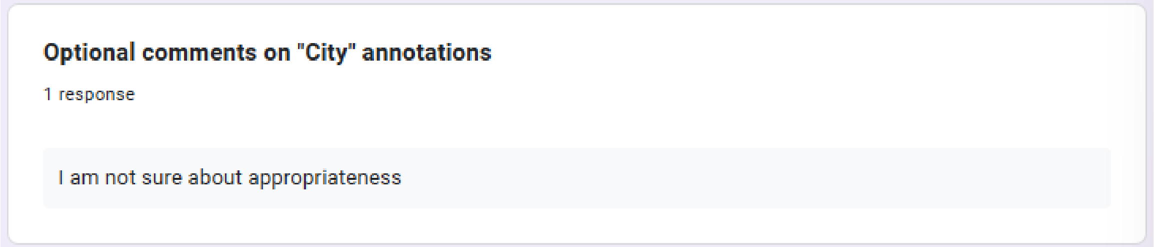
Optional comments on "Address" annotations

1 response

I am not sure about appropriateness

City



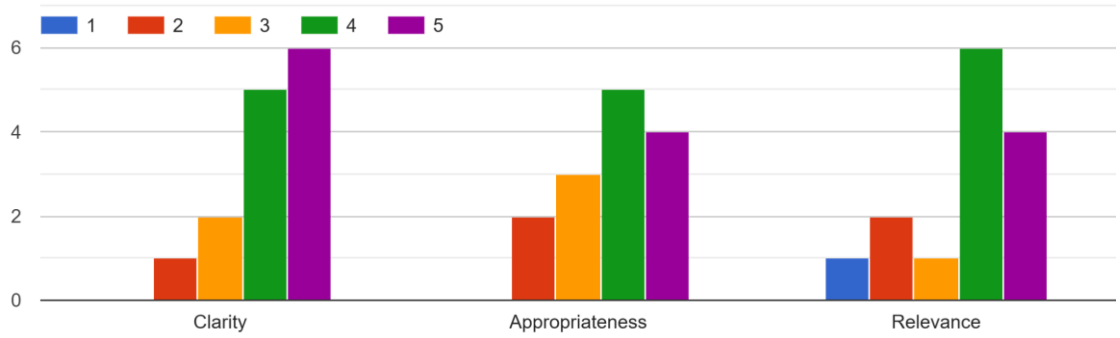


Optional comments on "City" annotations

1 response

I am not sure about appropriateness

State/Province

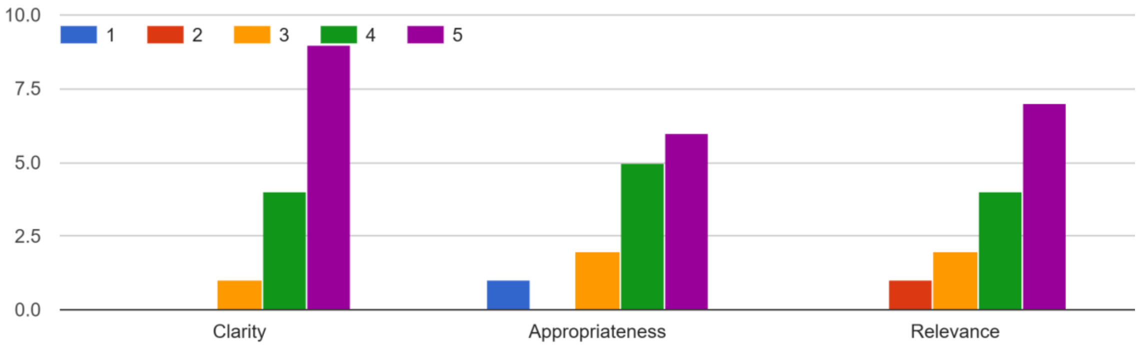


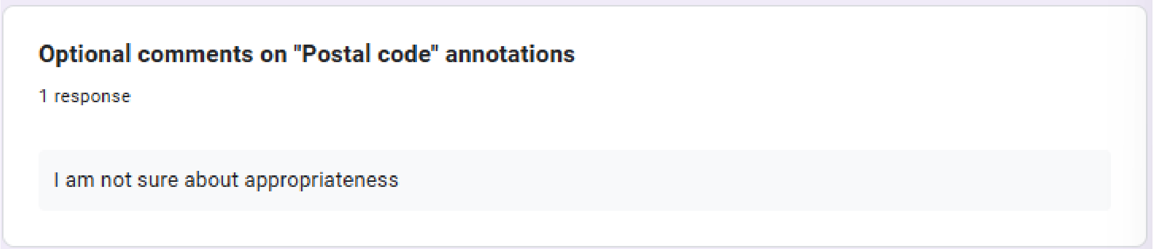
Optional comments on "State/Province" annotations

1 response

I am not sure about appropriateness

Postal code



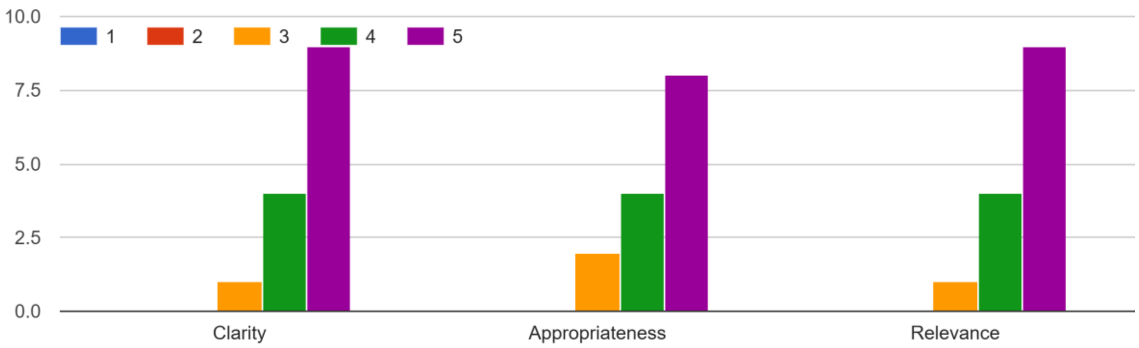


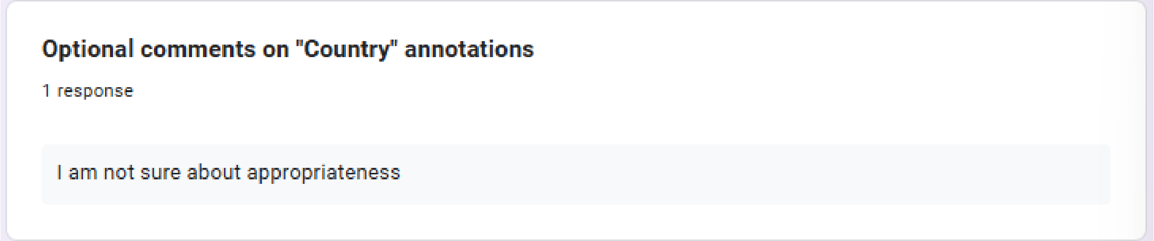
Optional comments on "Postal code" annotations

1 response

I am not sure about appropriateness

Country



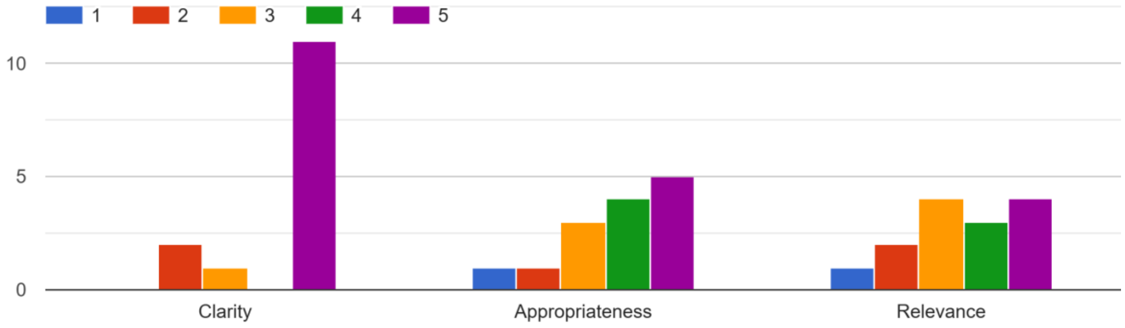


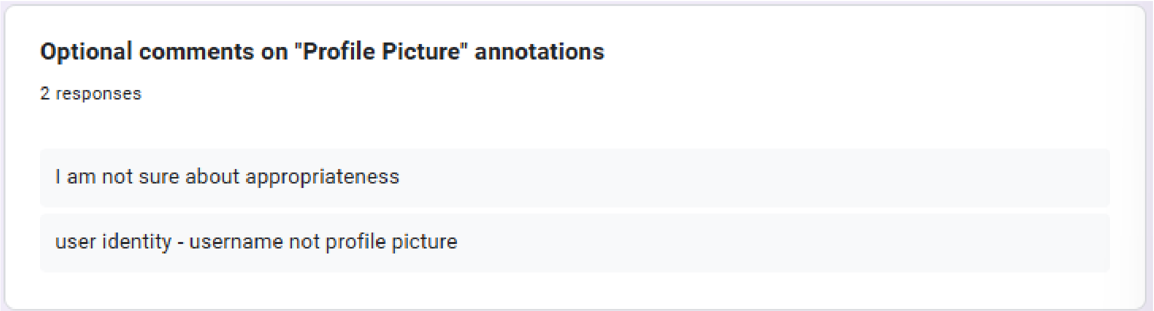
Optional comments on "Country" annotations

1 response

I am not sure about appropriateness

Profile Picture



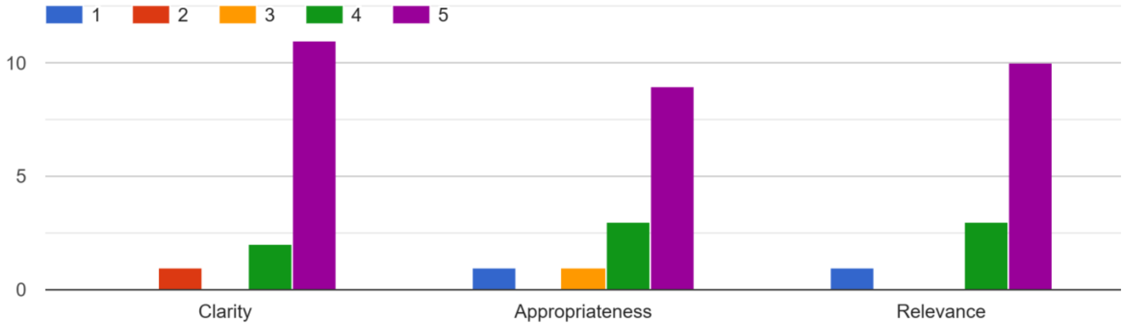

Optional comments on "Profile Picture" annotations

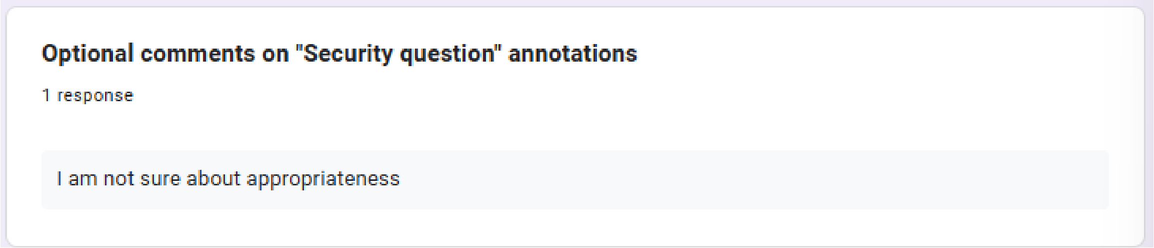
2 responses

I am not sure about appropriateness

user identity - username not profile picture

Security question

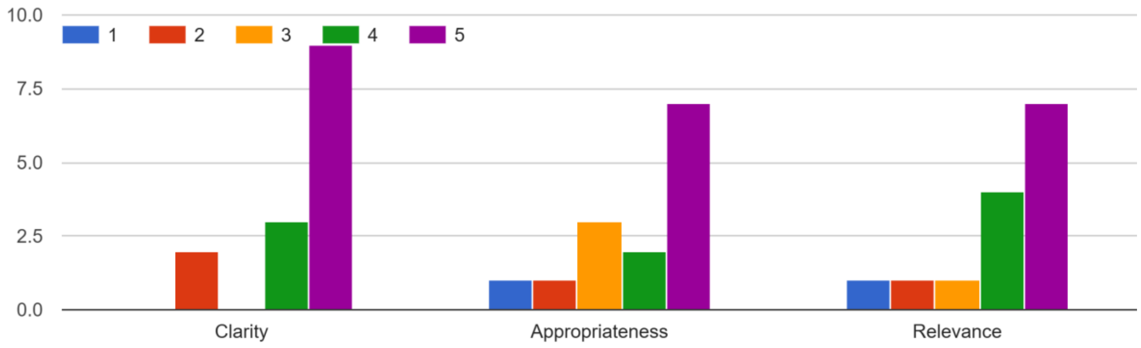


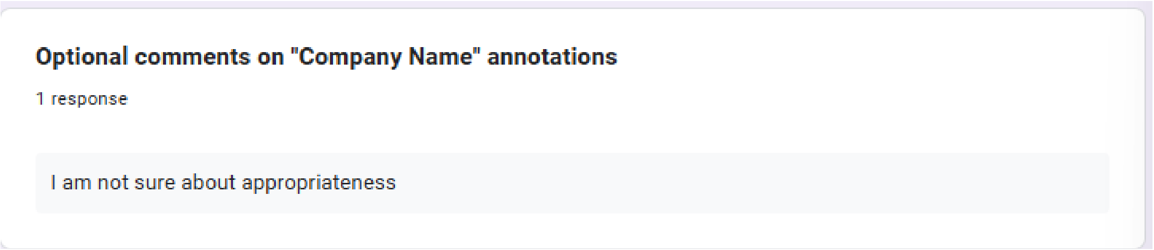

Optional comments on "Security question" annotations

1 response

I am not sure about appropriateness

Company Name

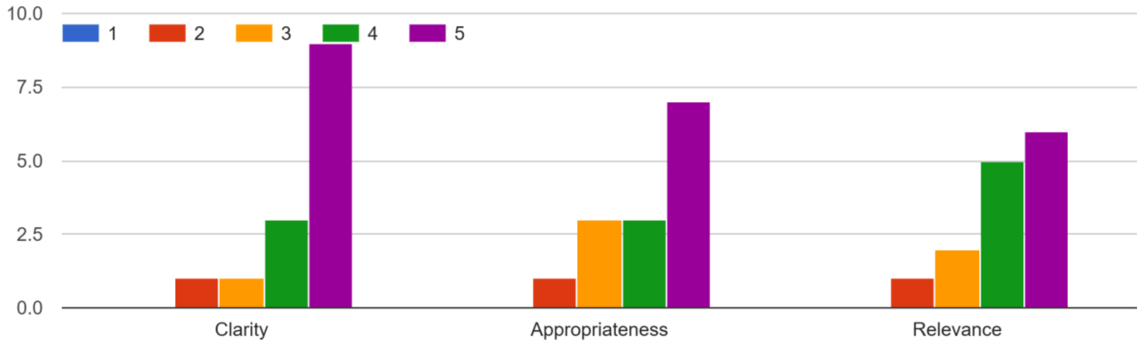


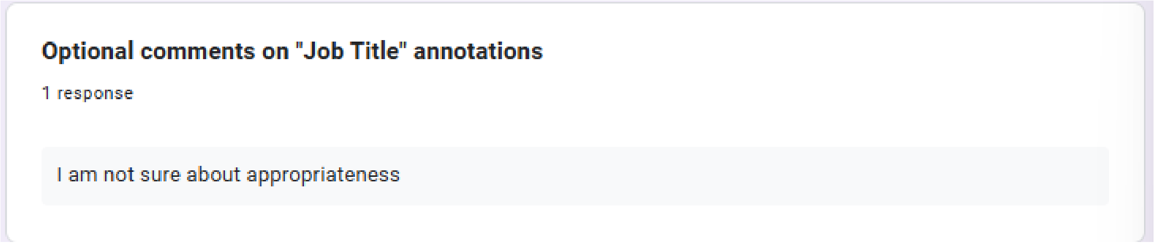

Optional comments on "Company Name" annotations

1 response

I am not sure about appropriateness

Job Title

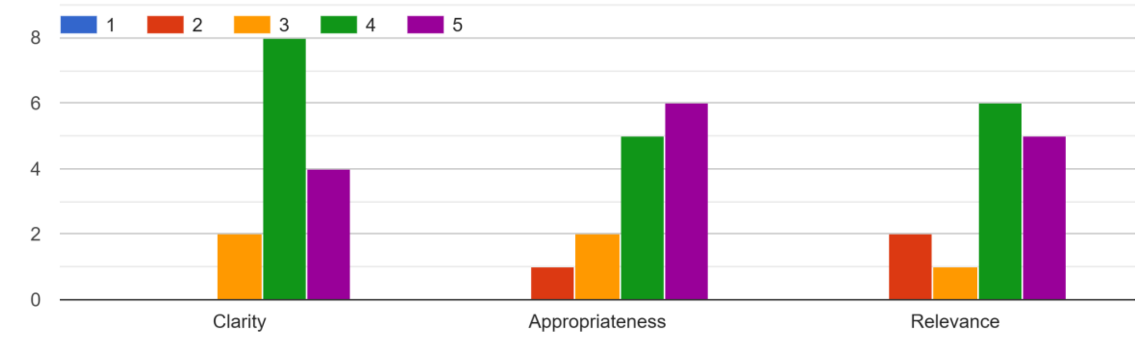


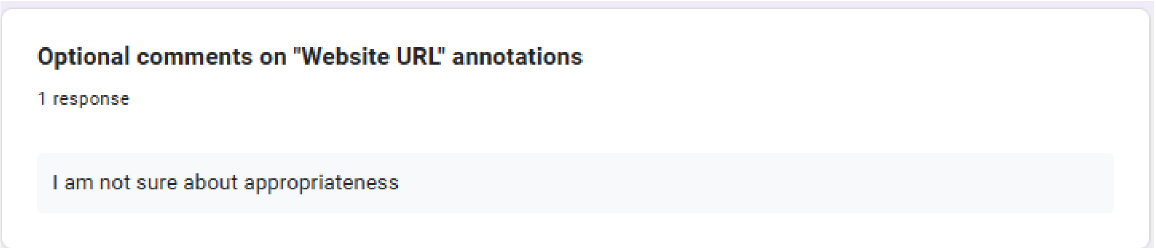

Optional comments on "Job Title" annotations

1 response

I am not sure about appropriateness

Website URL



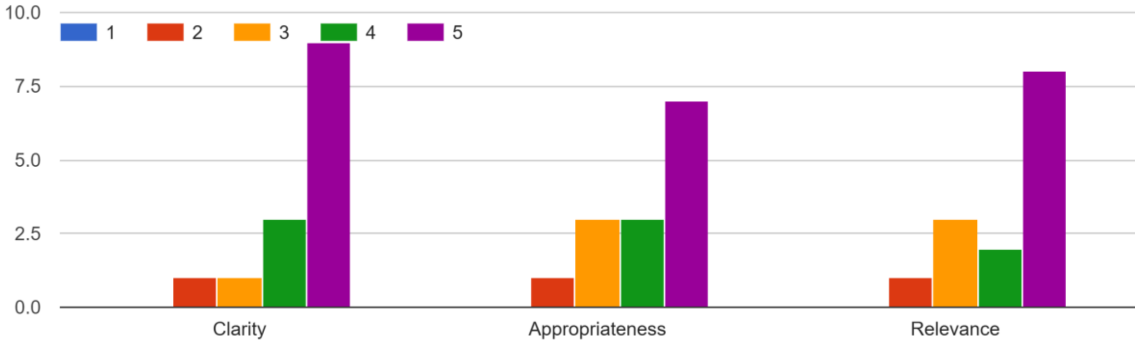


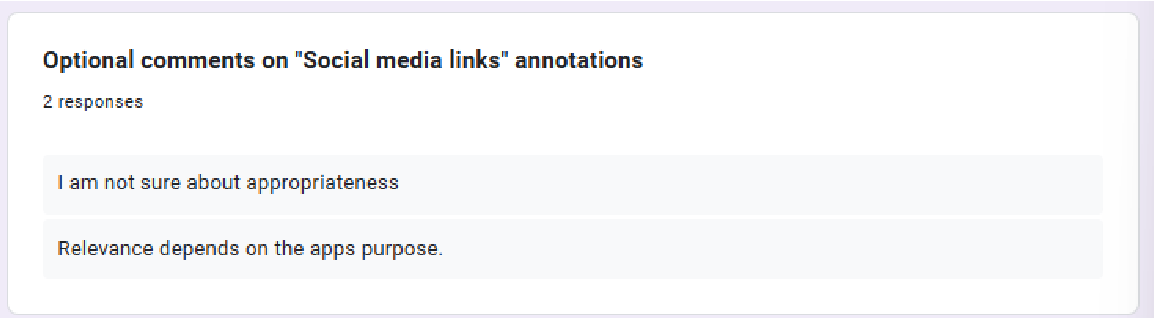
Optional comments on "Website URL" annotations

1 response

I am not sure about appropriateness

Social media links





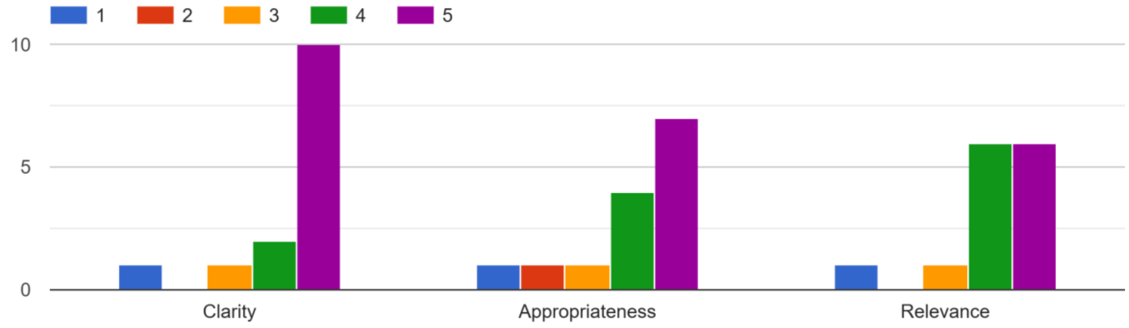
Optional comments on "Social media links" annotations

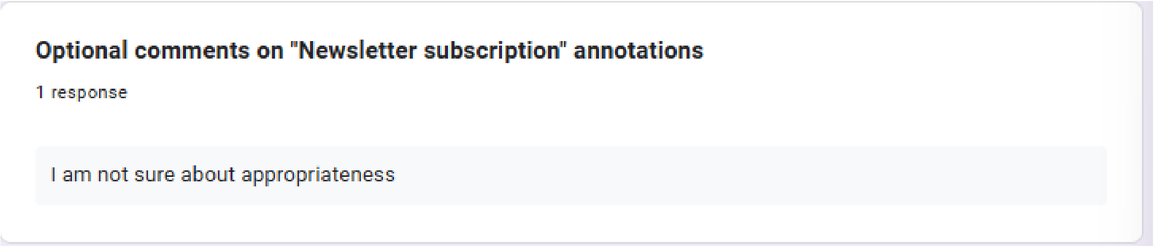
2 responses

I am not sure about appropriateness

Relevance depends on the apps purpose.

Newsletter subscription



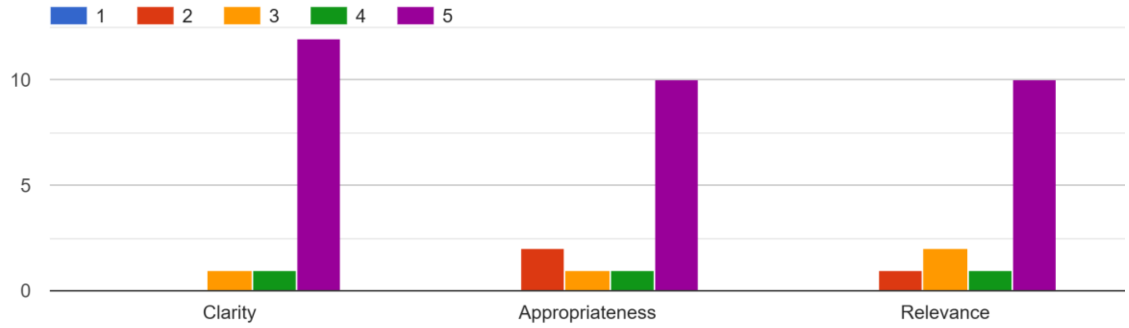


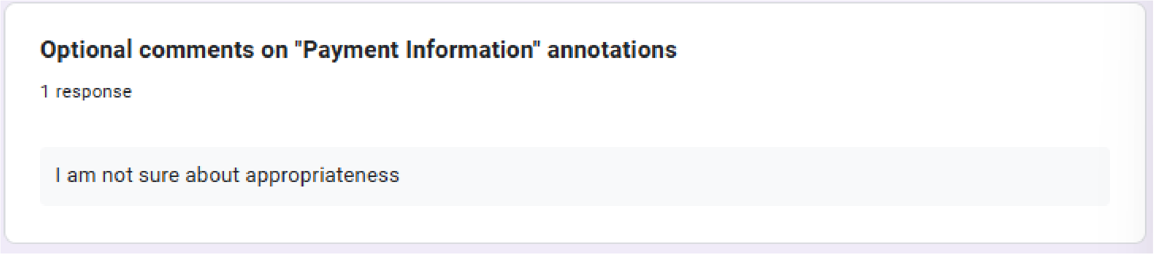
Optional comments on "Newsletter subscription" annotations

1 response

I am not sure about appropriateness

Payment Information

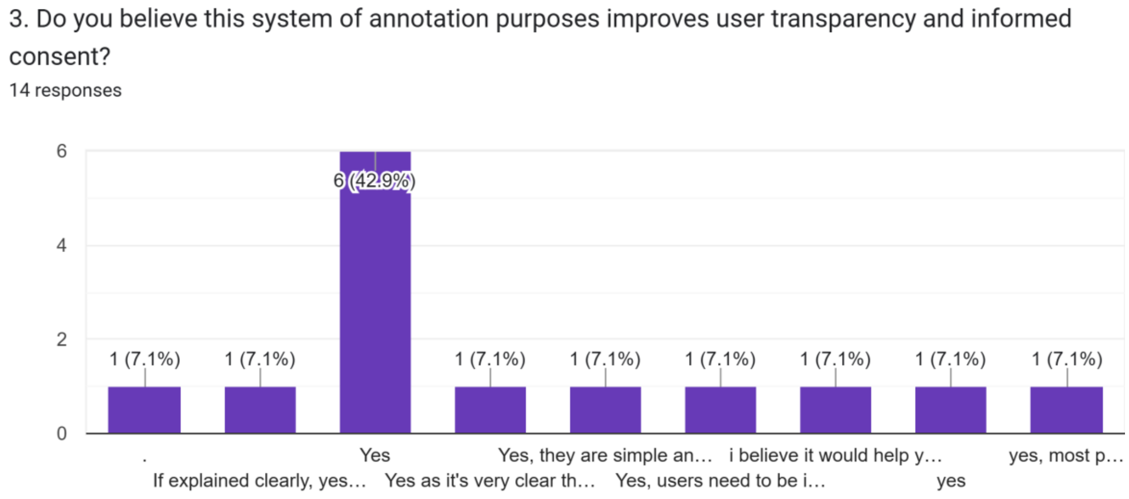




Optional comments on "Payment Information" annotations

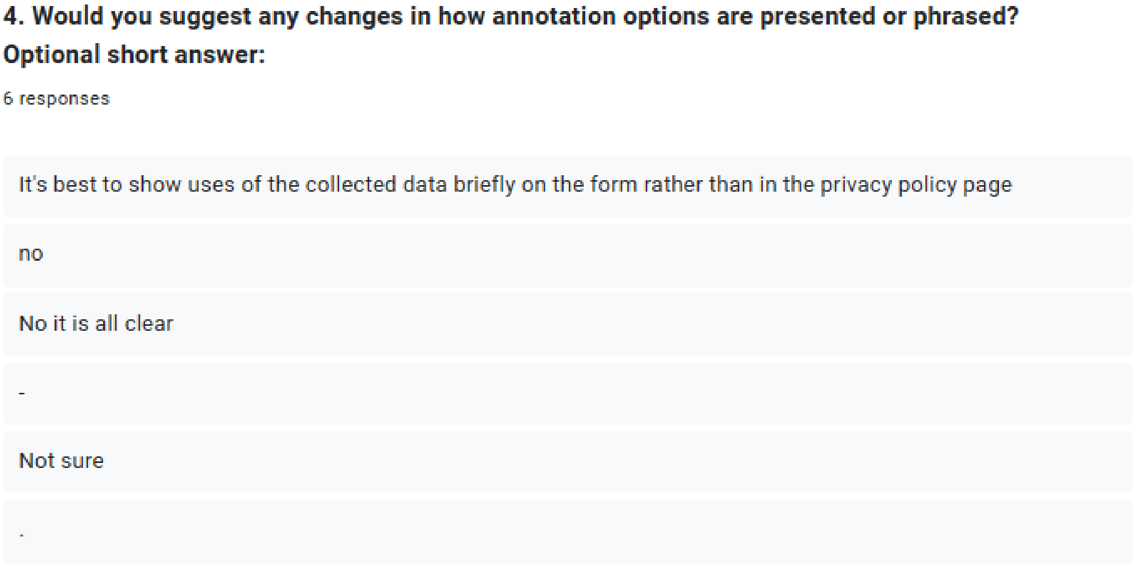
1 response

I am not sure about appropriateness



3. Do you believe this system of annotation purposes improves user transparency and informed consent?

14 responses



4. Would you suggest any changes in how annotation options are presented or phrased? Optional short answer:

6 responses

It's best to show uses of the collected data briefly on the form rather than in the privacy policy page

no

No it is all clear

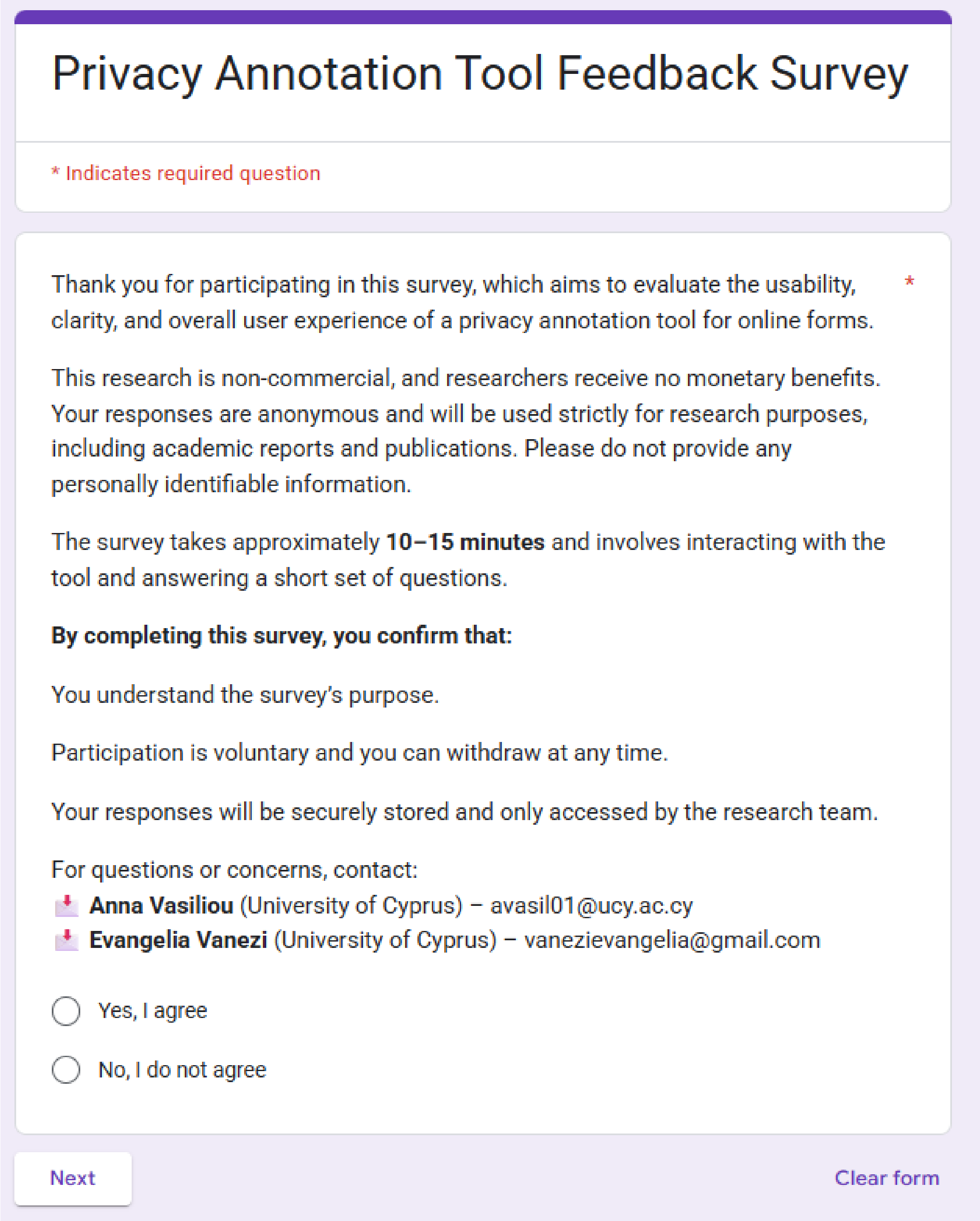
-

Not sure

.

Appendix D

This appendix includes the full questionnaire used in **Chapter 07** to evaluate the Privacy Annotation Tool's usability, visual appeal, and effectiveness. The survey was distributed to users as part of the final evaluation phase, aiming to collect feedback on their overall experience with the tool.



Privacy Annotation Tool Feedback Survey

* Indicates required question

Thank you for participating in this survey, which aims to evaluate the usability, clarity, and overall user experience of a privacy annotation tool for online forms. *

This research is non-commercial, and researchers receive no monetary benefits. Your responses are anonymous and will be used strictly for research purposes, including academic reports and publications. Please do not provide any personally identifiable information.

The survey takes approximately **10–15 minutes** and involves interacting with the tool and answering a short set of questions.

By completing this survey, you confirm that:

You understand the survey's purpose.

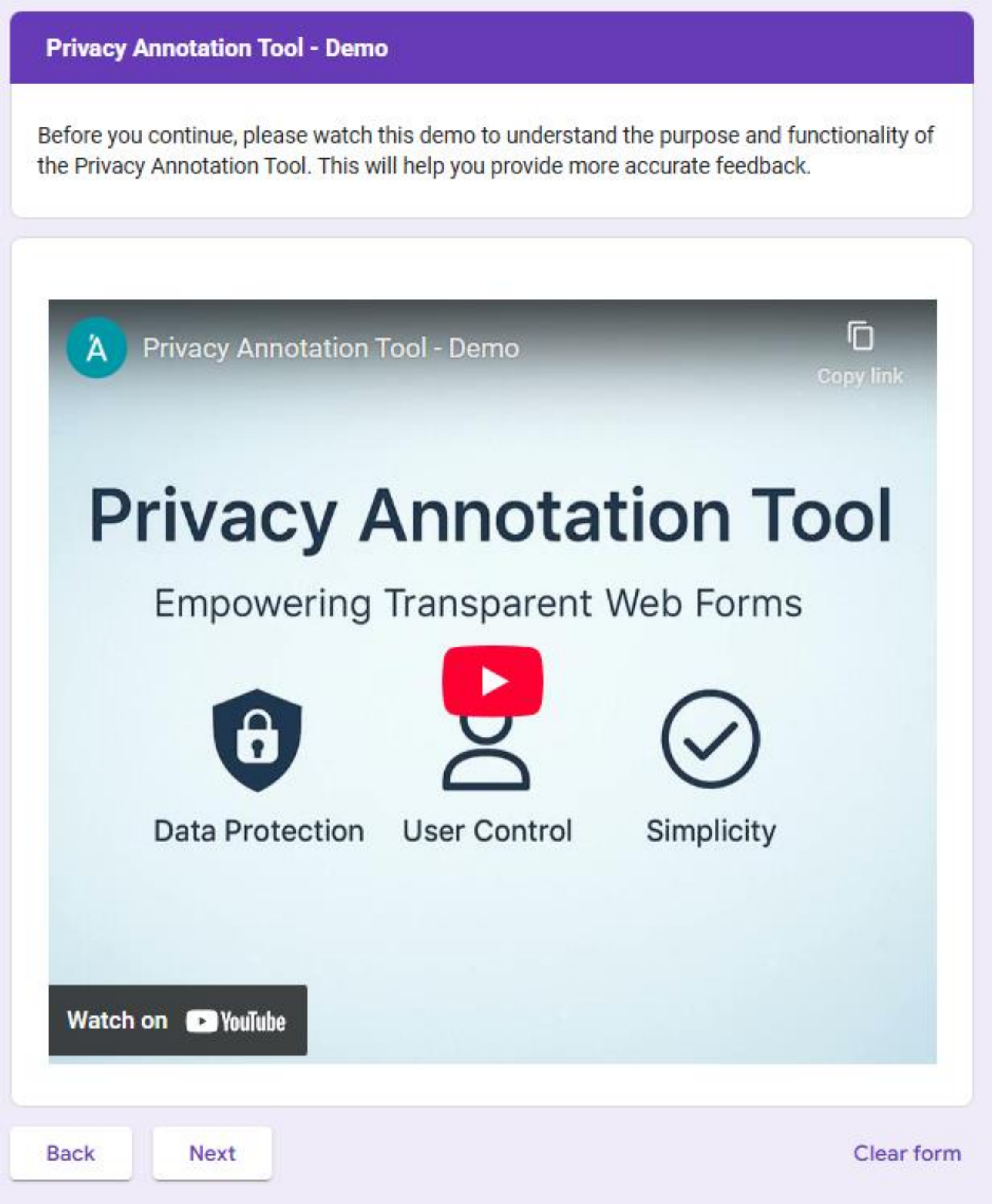
Participation is voluntary and you can withdraw at any time.

Your responses will be securely stored and only accessed by the research team.

For questions or concerns, contact:
📩 **Anna Vasiliou** (University of Cyprus) – avasil01@ucy.ac.cy
📩 **Evangelia Vanezi** (University of Cyprus) – vanezievangelia@gmail.com

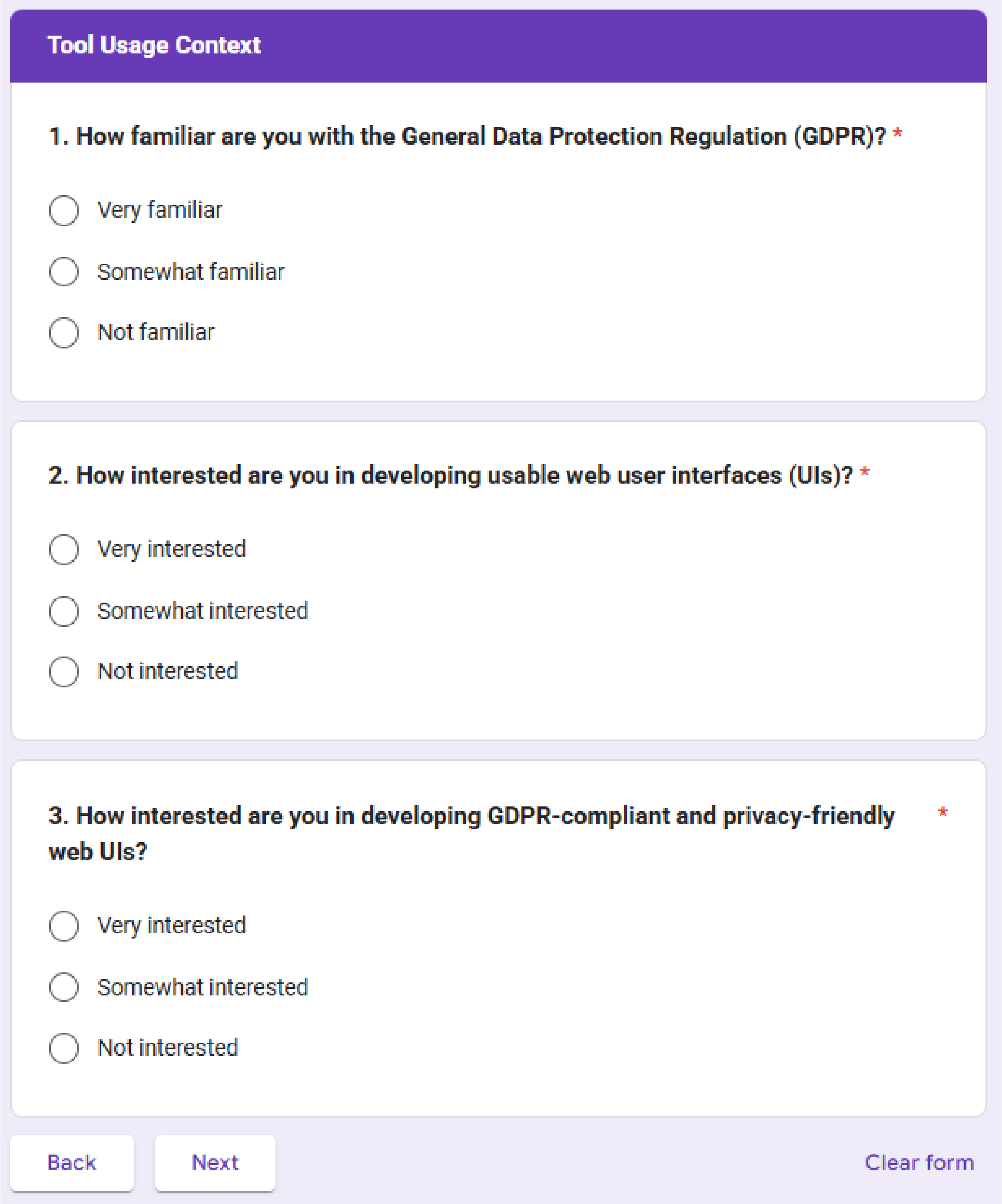
○ Yes, I agree

○ No, I do not agree



Privacy Annotation Tool - Demo

Before you continue, please watch this demo to understand the purpose and functionality of the Privacy Annotation Tool. This will help you provide more accurate feedback.



Tool Usage Context

1. How familiar are you with the General Data Protection Regulation (GDPR)? *

○ Very familiar

○ Somewhat familiar

○ Not familiar

2. How interested are you in developing usable web user interfaces (UIs)? *

○ Very interested

○ Somewhat interested

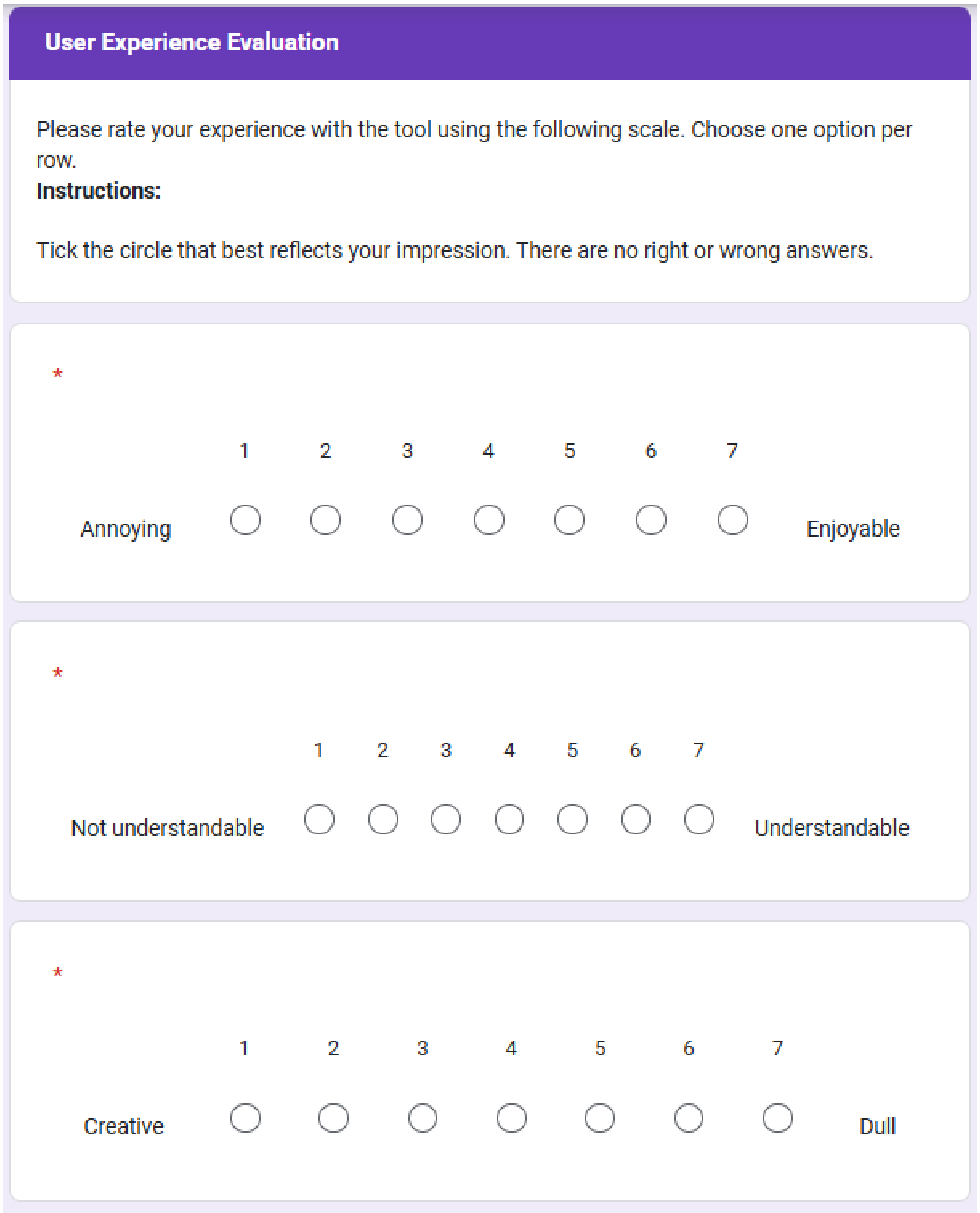
○ Not interested

3. How interested are you in developing GDPR-compliant and privacy-friendly web UIs? *

○ Very interested

○ Somewhat interested

○ Not interested



User Experience Evaluation

Please rate your experience with the tool using the following scale. Choose one option per row.
Instructions:

Tick the circle that best reflects your impression. There are no right or wrong answers.

*

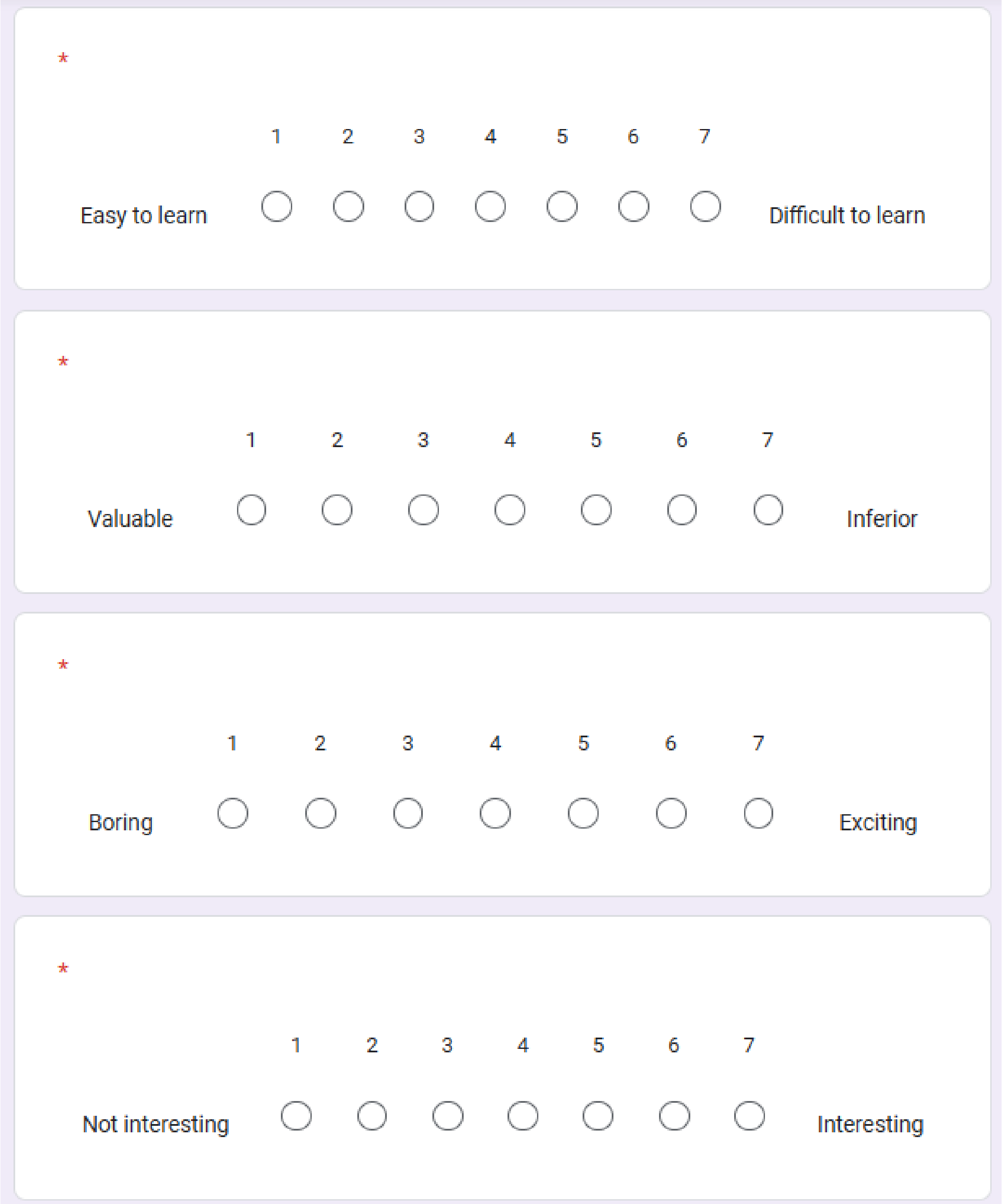
	1	2	3	4	5	6	7	
Annoying	○	○	○	○	○	○	○	Enjoyable

*

	1	2	3	4	5	6	7	
Not understandable	○	○	○	○	○	○	○	Understandable

*

	1	2	3	4	5	6	7	
Creative	○	○	○	○	○	○	○	Dull



*

	1	2	3	4	5	6	7	
Easy to learn	○	○	○	○	○	○	○	Difficult to learn

*

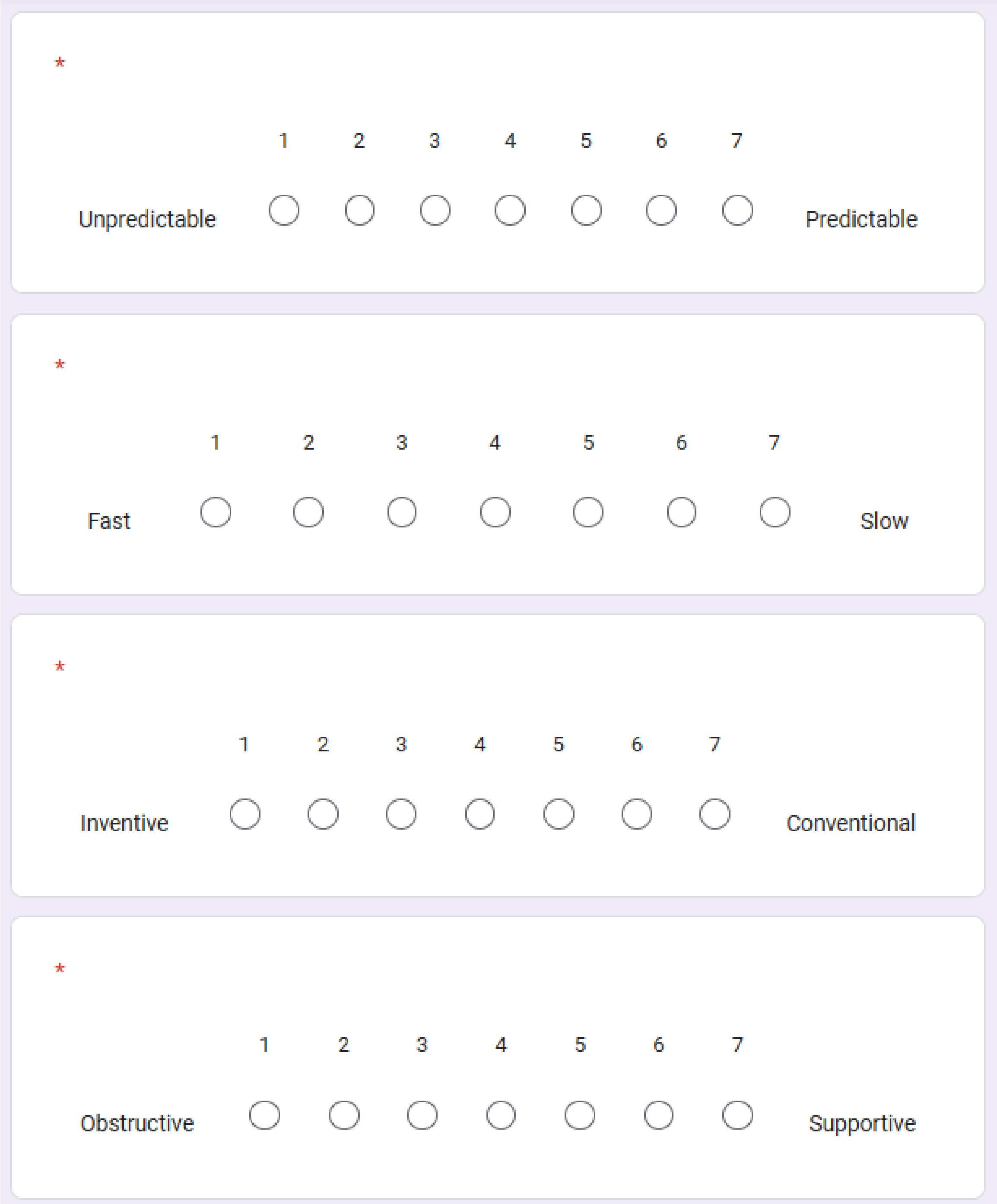
	1	2	3	4	5	6	7	
Valuable	○	○	○	○	○	○	○	Inferior

*

	1	2	3	4	5	6	7	
Boring	○	○	○	○	○	○	○	Exciting

*

	1	2	3	4	5	6	7	
Not interesting	○	○	○	○	○	○	○	Interesting



*

	1	2	3	4	5	6	7	
Unpredictable	○	○	○	○	○	○	○	Predictable

*

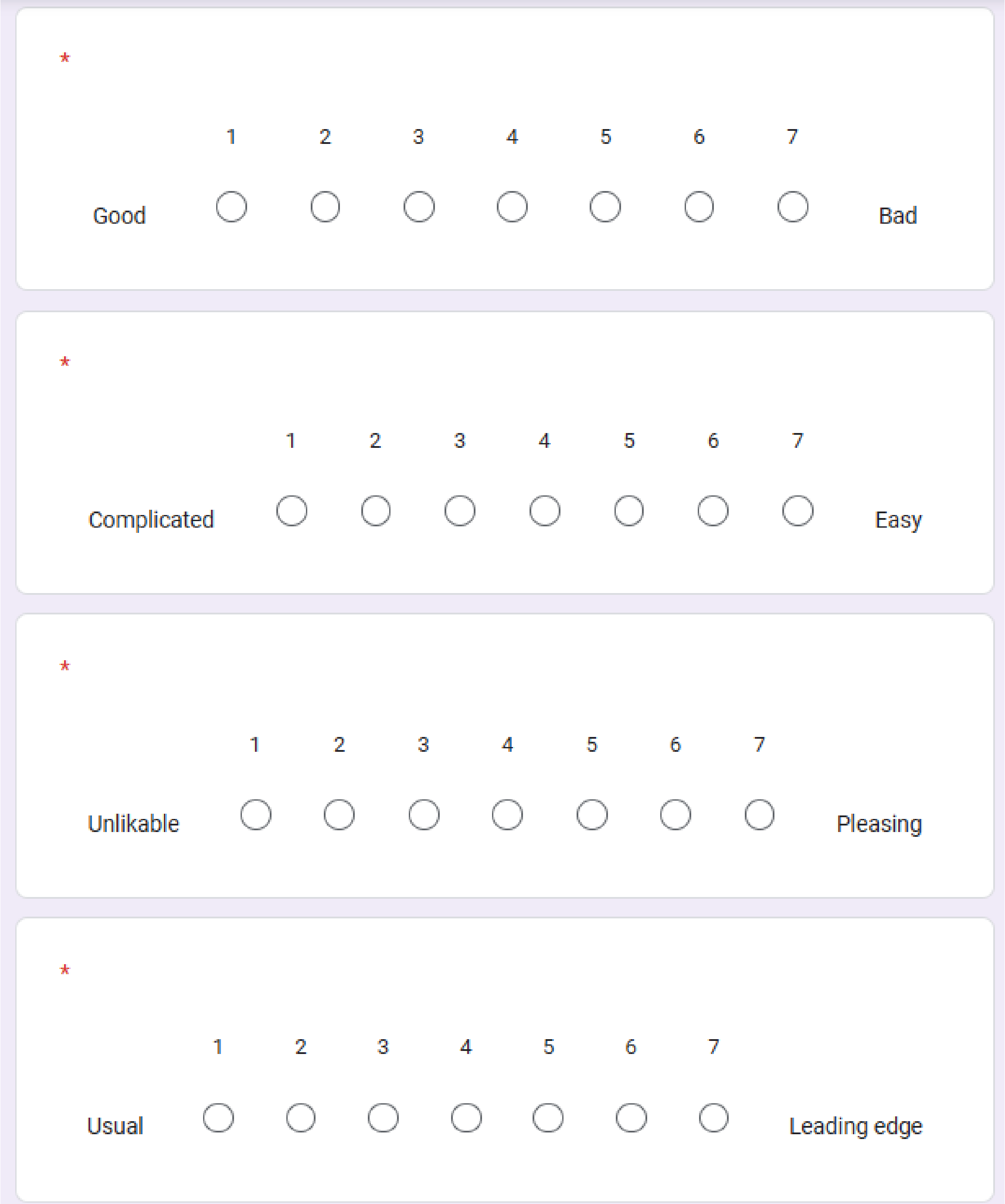
	1	2	3	4	5	6	7	
Fast	○	○	○	○	○	○	○	Slow

*

	1	2	3	4	5	6	7	
Inventive	○	○	○	○	○	○	○	Conventional

*

	1	2	3	4	5	6	7	
Obstructive	○	○	○	○	○	○	○	Supportive



*

	1	2	3	4	5	6	7	
Good	○	○	○	○	○	○	○	Bad

*

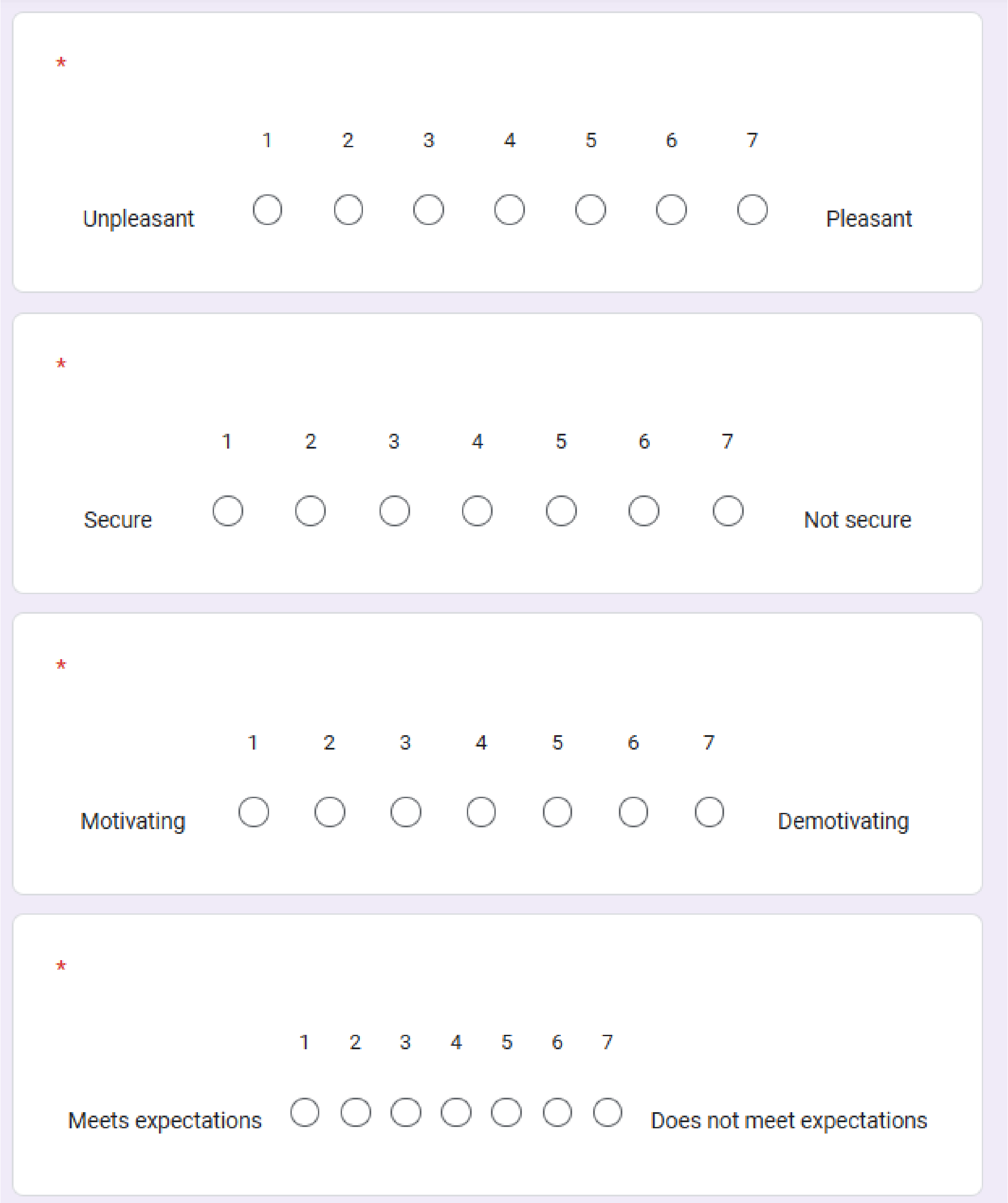
	1	2	3	4	5	6	7	
Complicated	○	○	○	○	○	○	○	Easy

*

	1	2	3	4	5	6	7	
Unlikable	○	○	○	○	○	○	○	Pleasing

*

	1	2	3	4	5	6	7	
Usual	○	○	○	○	○	○	○	Leading edge



*

	1	2	3	4	5	6	7	
Unpleasant	○	○	○	○	○	○	○	Pleasant

*

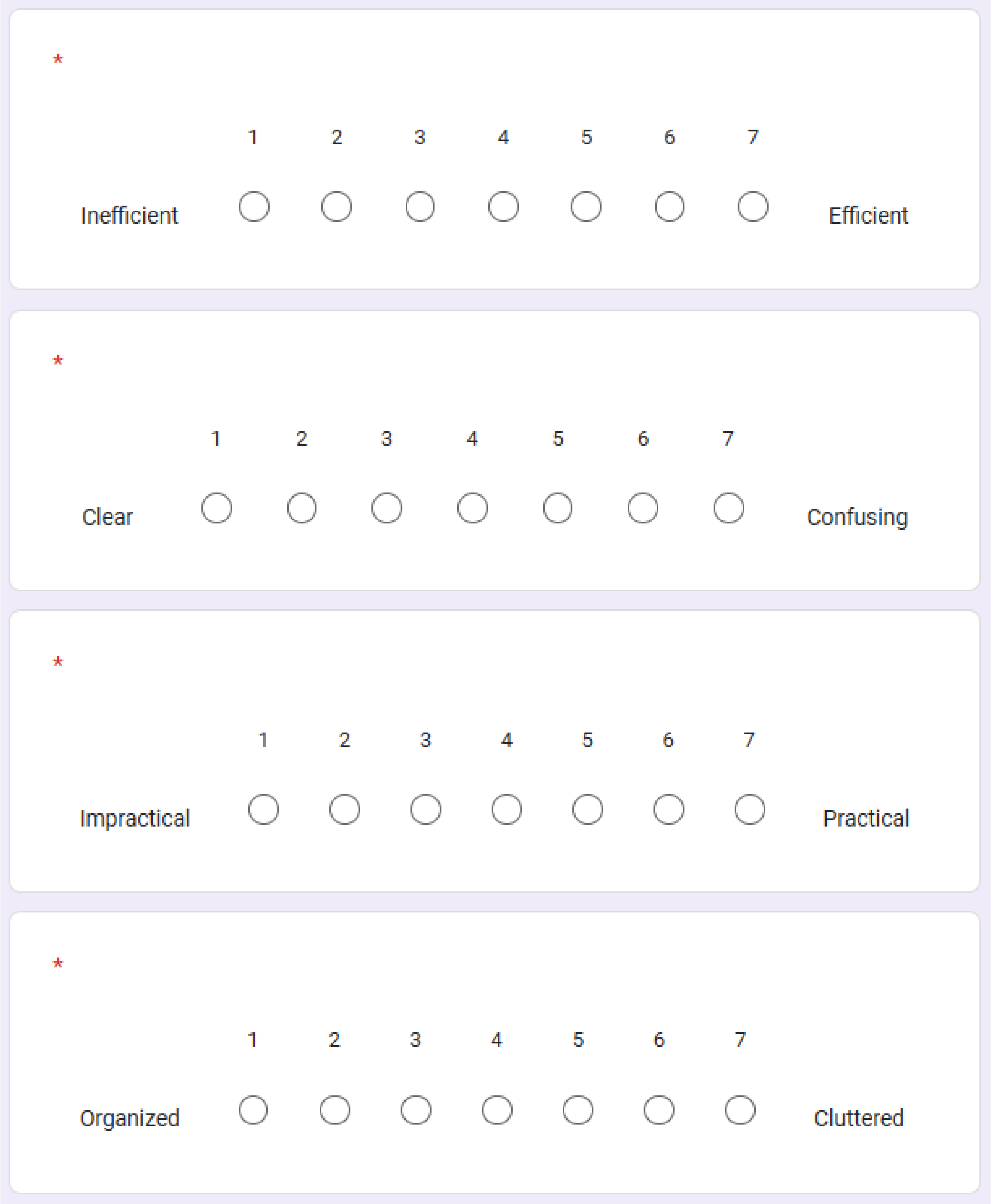
	1	2	3	4	5	6	7	
Secure	○	○	○	○	○	○	○	Not secure

*

	1	2	3	4	5	6	7	
Motivating	○	○	○	○	○	○	○	Demotivating

*

	1	2	3	4	5	6	7	
Meets expectations	○	○	○	○	○	○	○	Does not meet expectations



*

	1	2	3	4	5	6	7	
Inefficient	○	○	○	○	○	○	○	Efficient

*

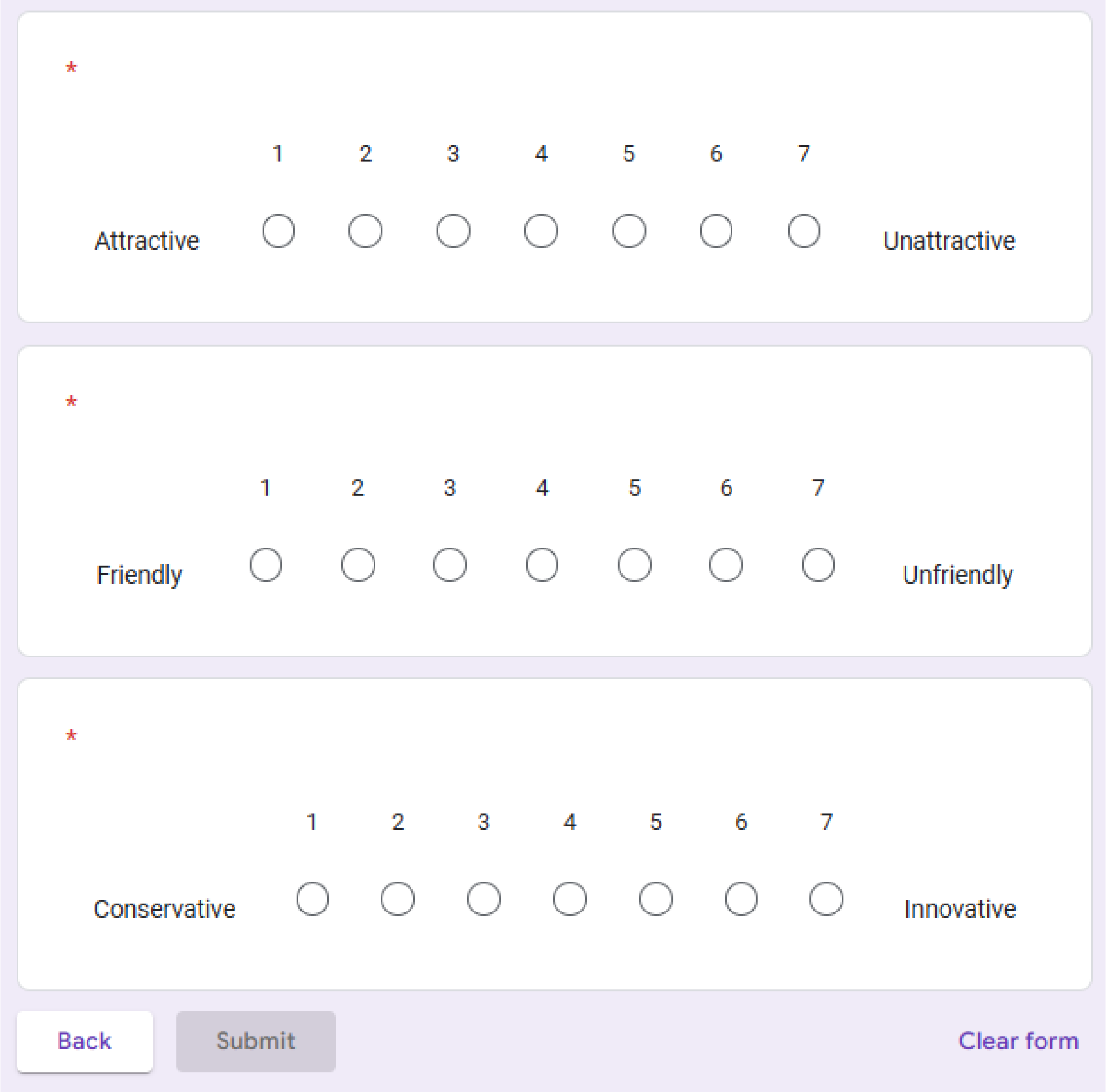
	1	2	3	4	5	6	7	
Clear	○	○	○	○	○	○	○	Confusing

*

	1	2	3	4	5	6	7	
Impractical	○	○	○	○	○	○	○	Practical

*

	1	2	3	4	5	6	7	
Organized	○	○	○	○	○	○	○	Cluttered



*

	1	2	3	4	5	6	7	
Attractive	○	○	○	○	○	○	○	Unattractive

*

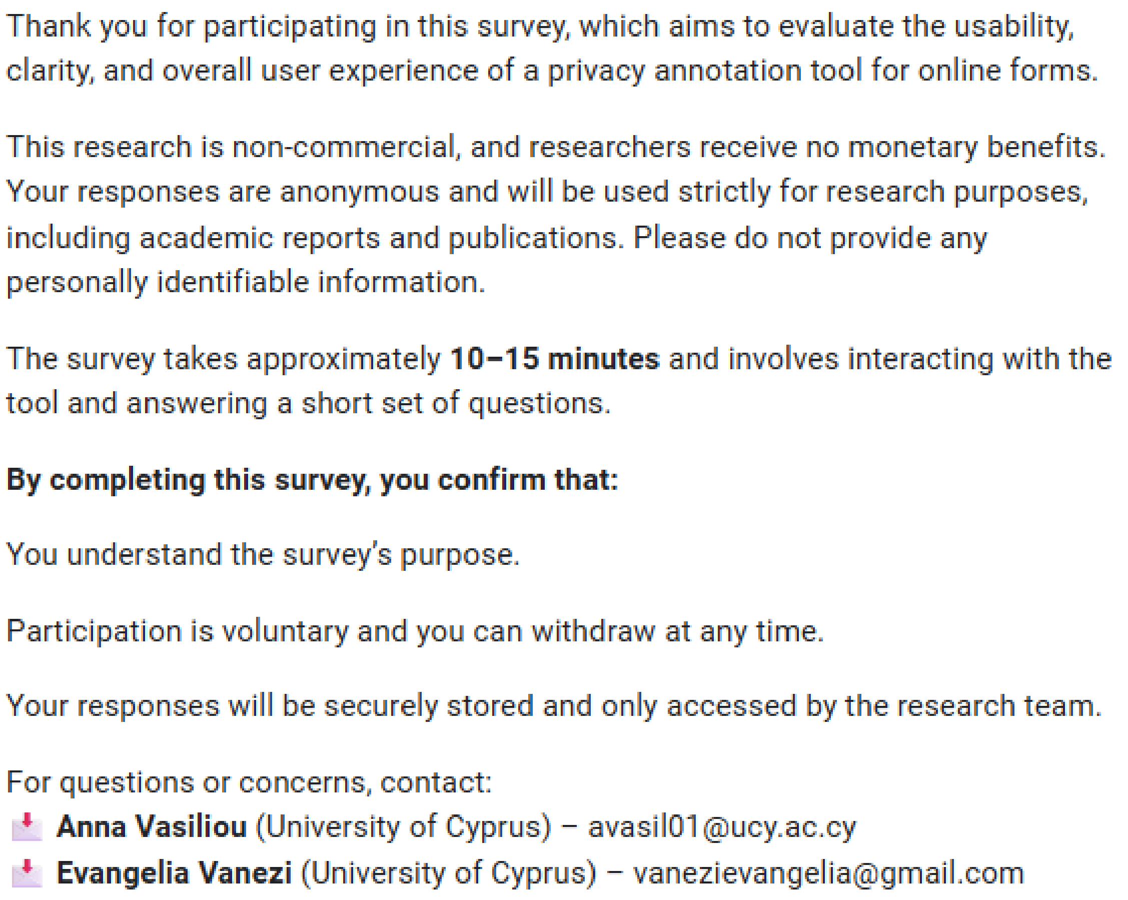
	1	2	3	4	5	6	7	
Friendly	○	○	○	○	○	○	○	Unfriendly

*

	1	2	3	4	5	6	7	
Conservative	○	○	○	○	○	○	○	Innovative

Appendix E

This appendix presents the complete results of the user evaluation survey discussed in **Chapter 07**. It includes all participant responses and rating distributions related to the tool's usability, efficiency, and overall user experience. These results were used to assess the tool's performance and validate its effectiveness in supporting privacy-aware form design.



Thank you for participating in this survey, which aims to evaluate the usability, clarity, and overall user experience of a privacy annotation tool for online forms.

This research is non-commercial, and researchers receive no monetary benefits. Your responses are anonymous and will be used strictly for research purposes, including academic reports and publications. Please do not provide any personally identifiable information.

The survey takes approximately **10–15 minutes** and involves interacting with the tool and answering a short set of questions.

By completing this survey, you confirm that:

You understand the survey's purpose.

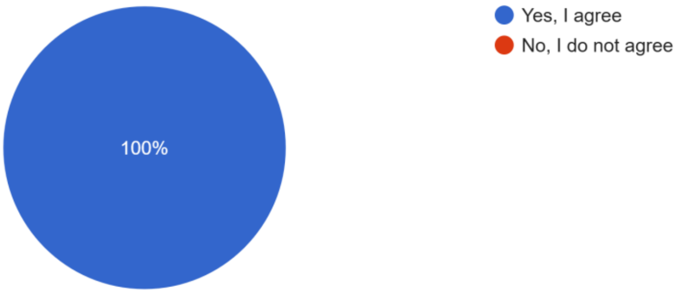
Participation is voluntary and you can withdraw at any time.

Your responses will be securely stored and only accessed by the research team.

For questions or concerns, contact:
📩 **Anna Vasiliou** (University of Cyprus) – avasil01@ucy.ac.cy
📩 **Evangelia Vanezi** (University of Cyprus) – vanezievangelia@gmail.com

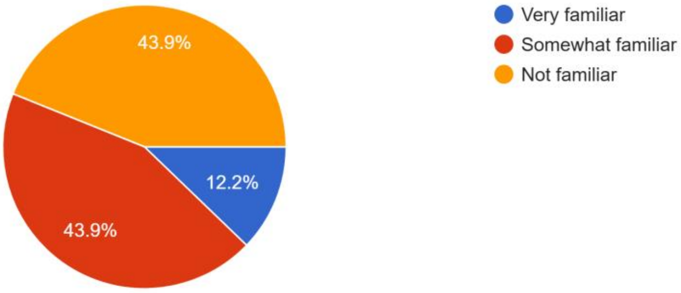
Thank you for participating in this survey, which aims to evaluate the usability, clarity, and overall user experience of a privacy annotation tool for o...University of Cyprus) – vanezievangelia@gmail.com

41 responses



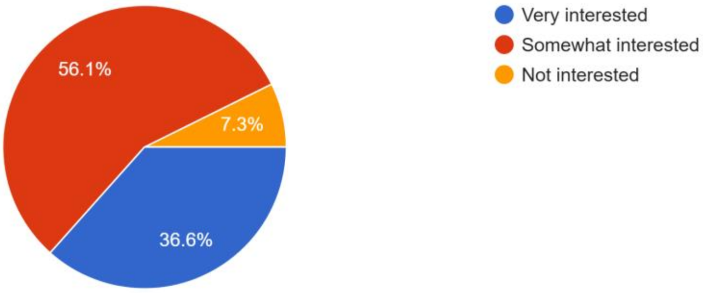
1. How familiar are you with the General Data Protection Regulation (GDPR)?

41 responses



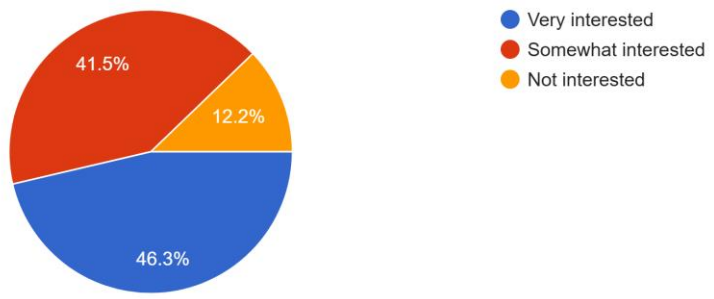
2. How interested are you in developing usable web user interfaces (UIs)?

41 responses

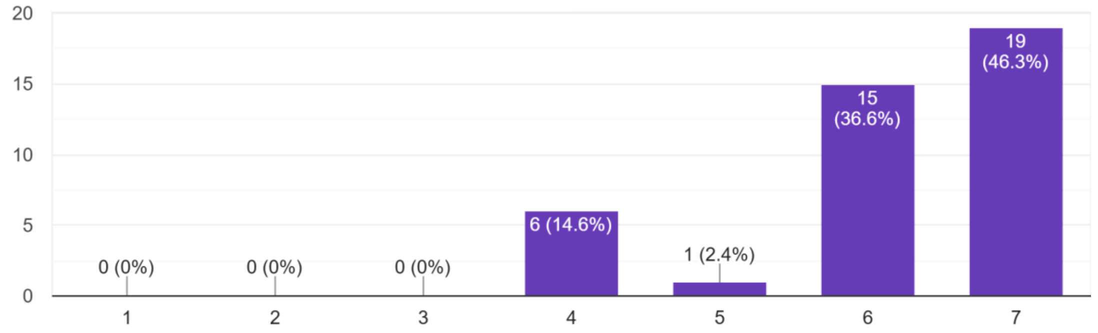


3. How interested are you in developing GDPR-compliant and privacy-friendly web UIs?

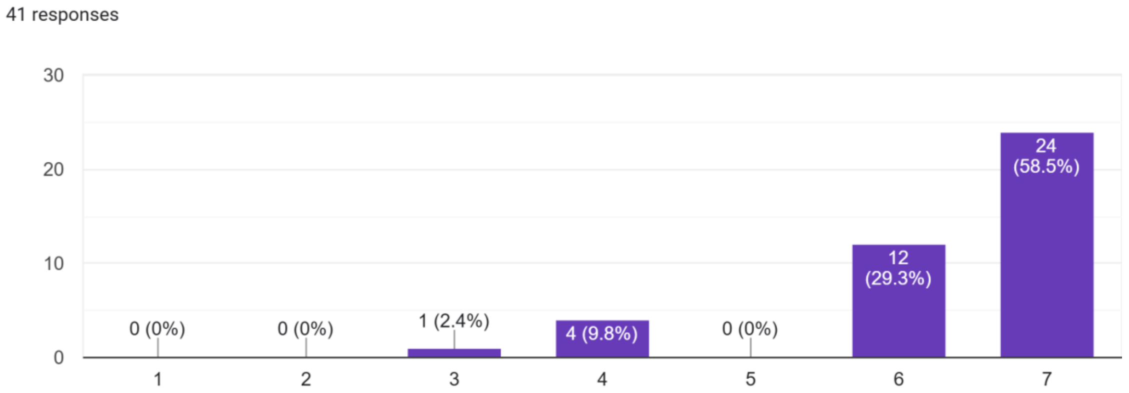
41 responses



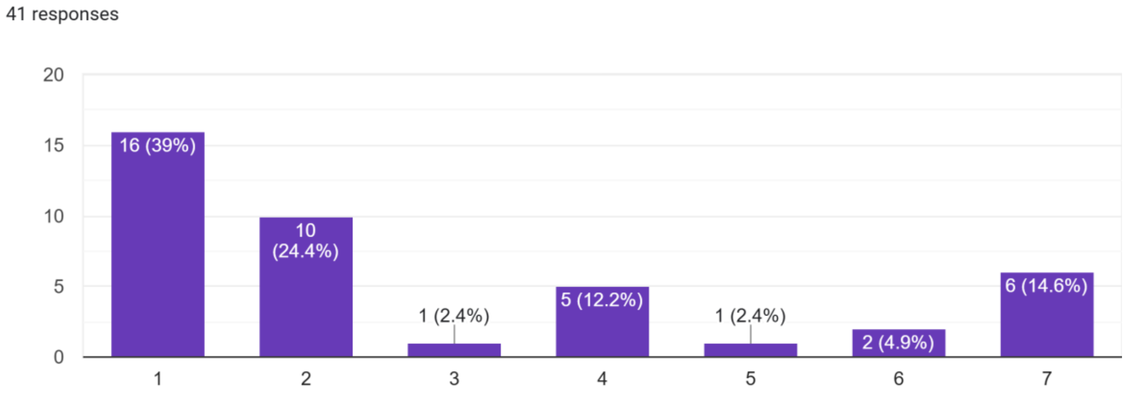
41 responses



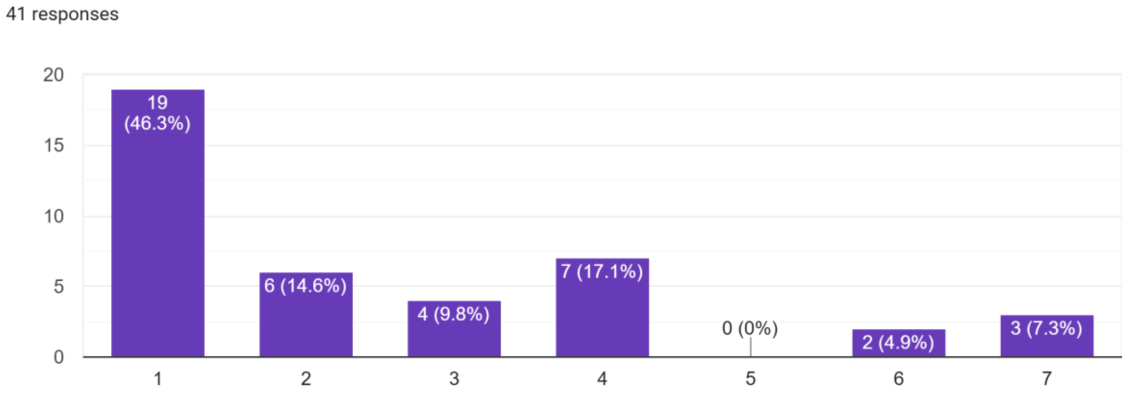
annoying vs enjoyable



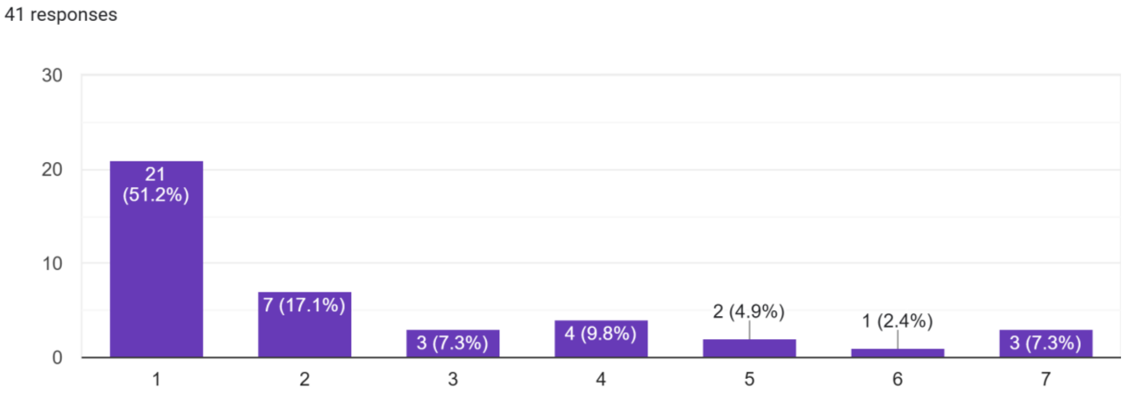
not understandable vs understandable



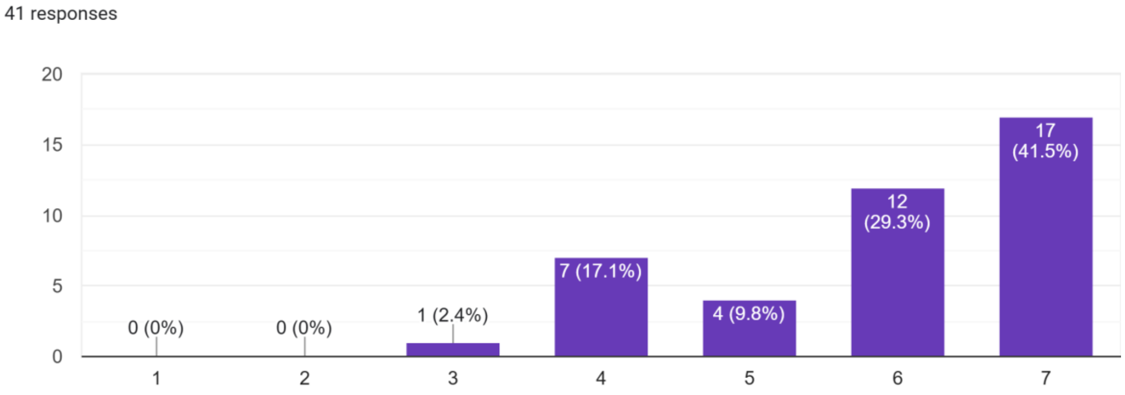
creative vs dull



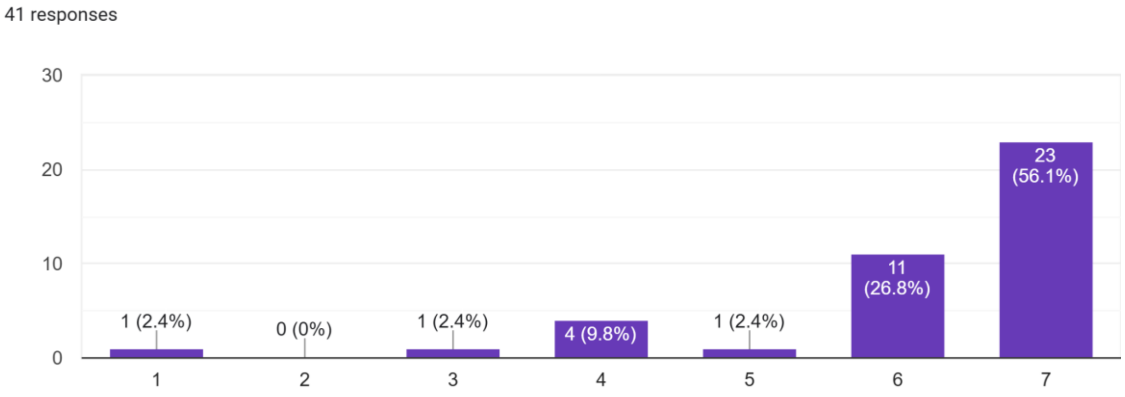
easy to learn vs difficult to learn



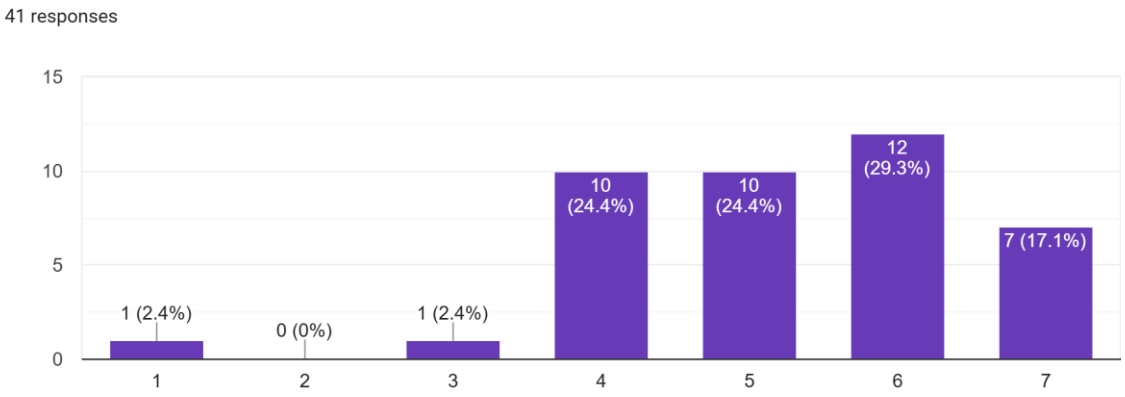
valuable vs inferior



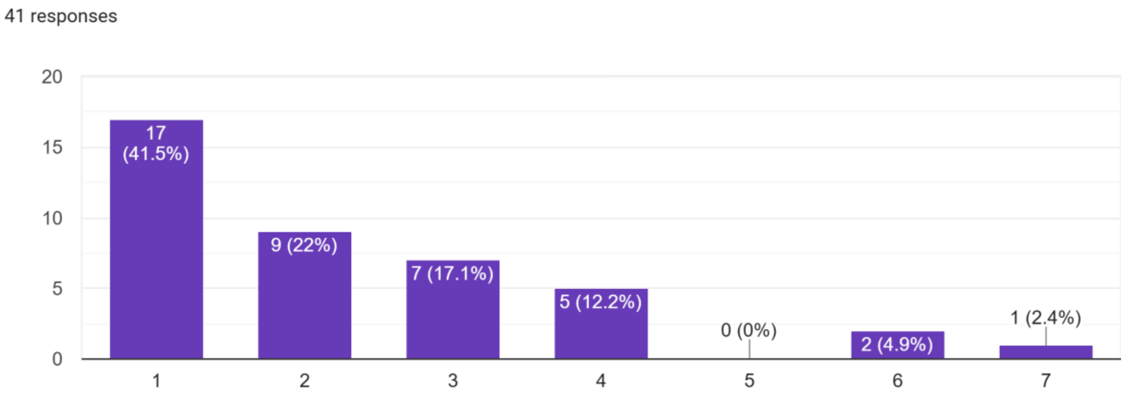
boring vs exciting

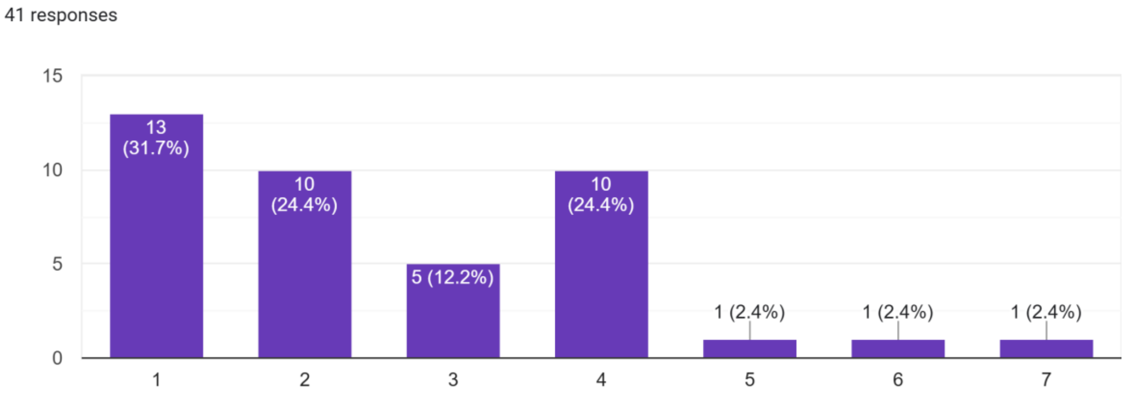


not interesting vs interesting



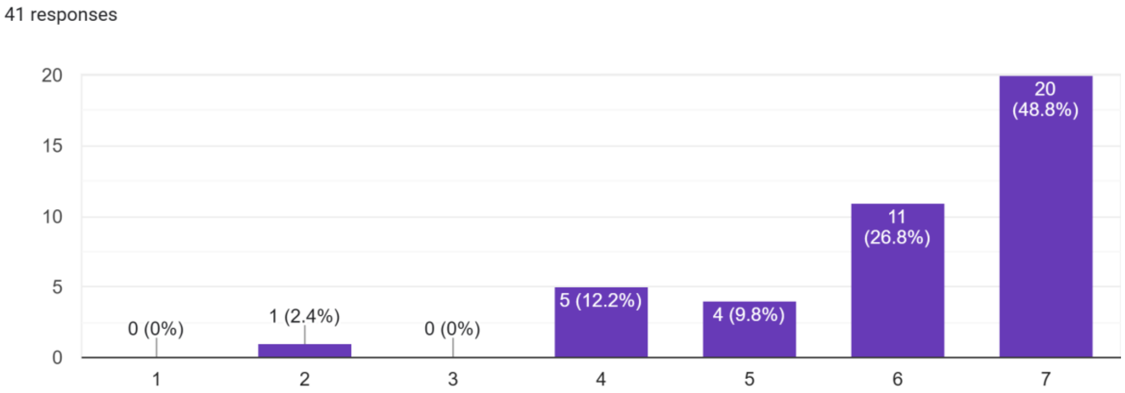
unpredictable vs predictable



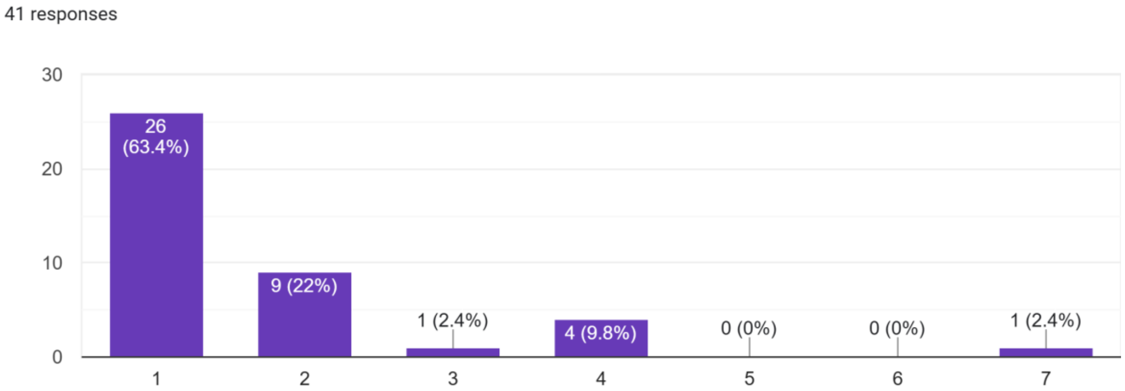


fast vs slow

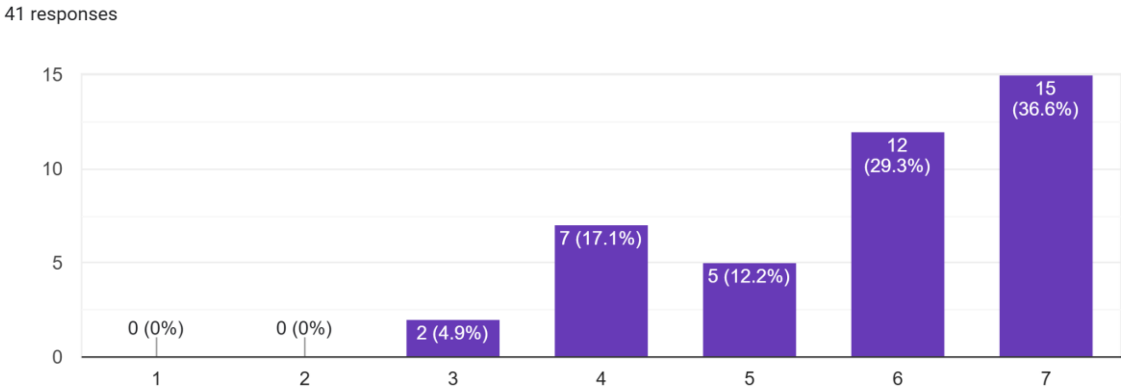
inventive vs conventional



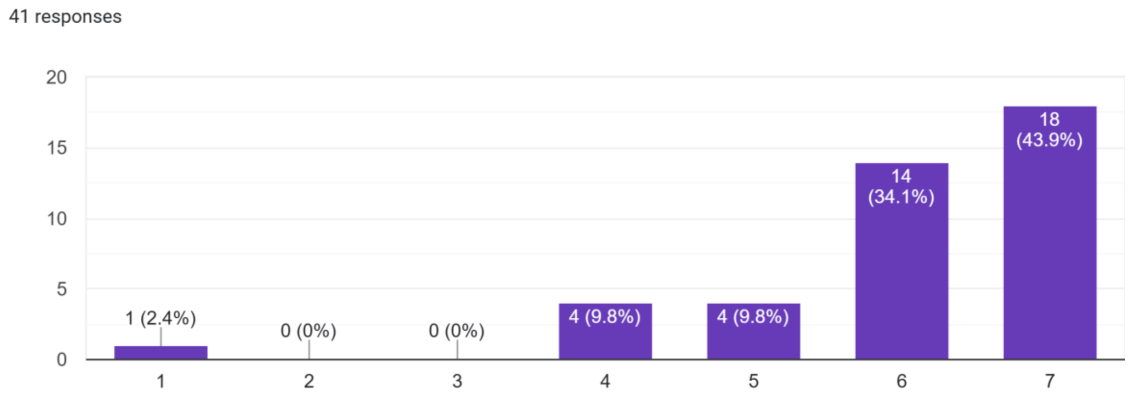
obstructive vs supportive



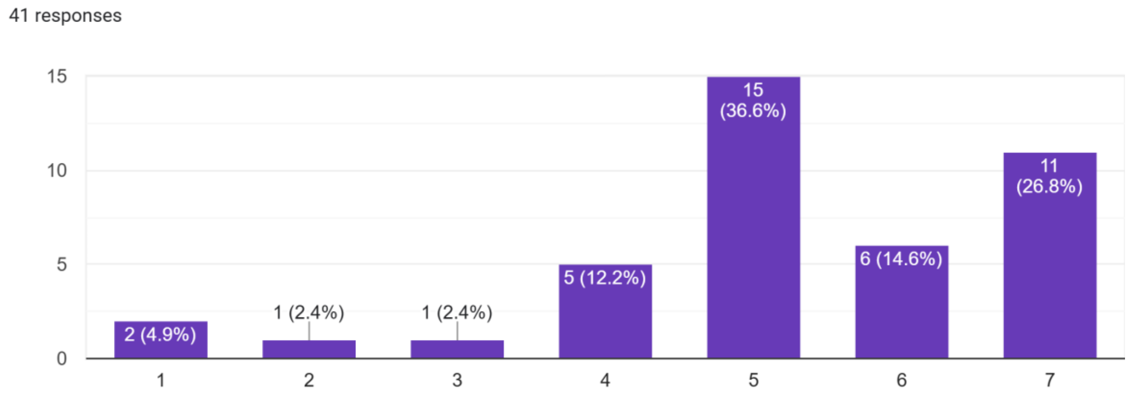
good vs bad



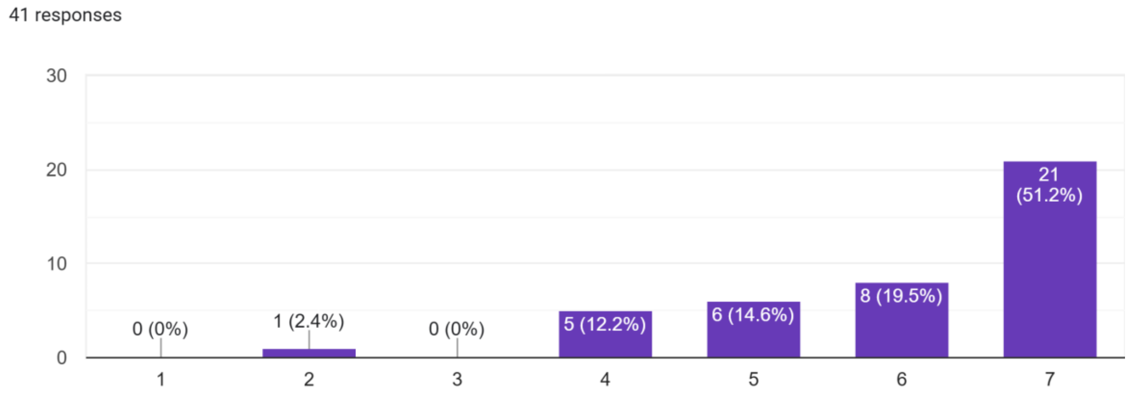
complicated vs easy



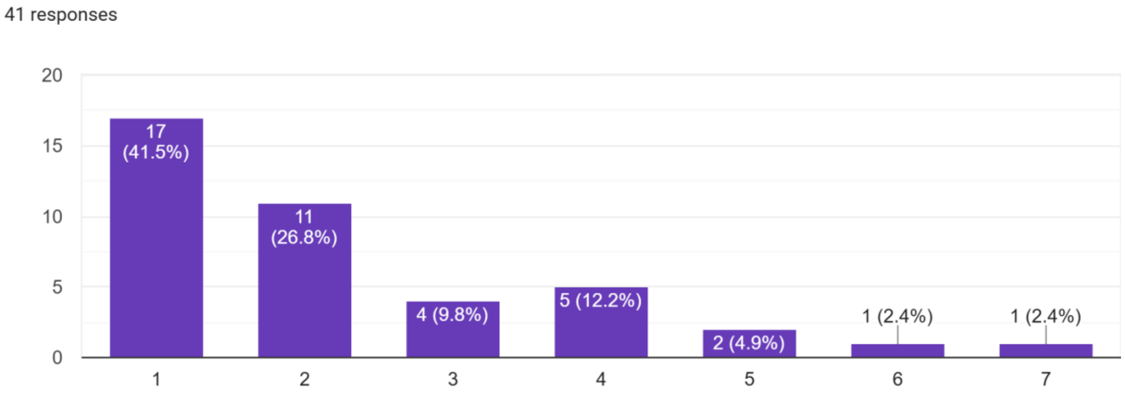
unlikable vs pleasing



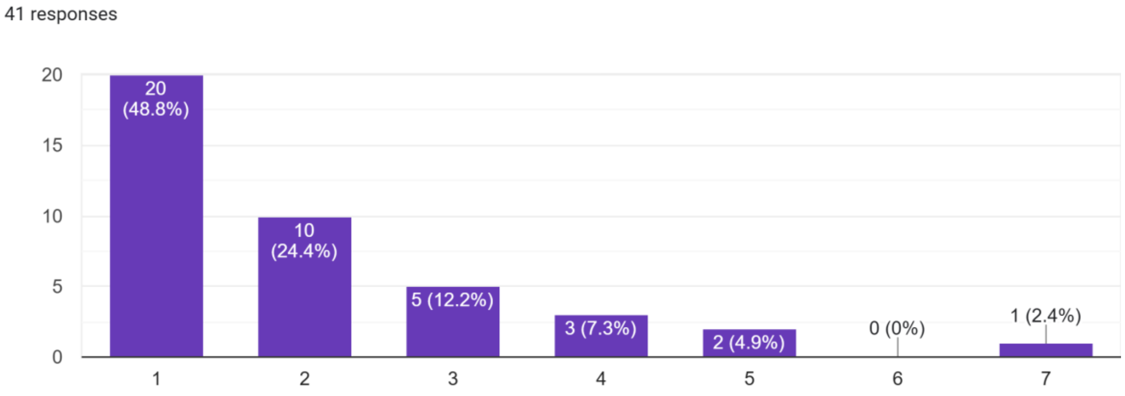
usual vs leading edge



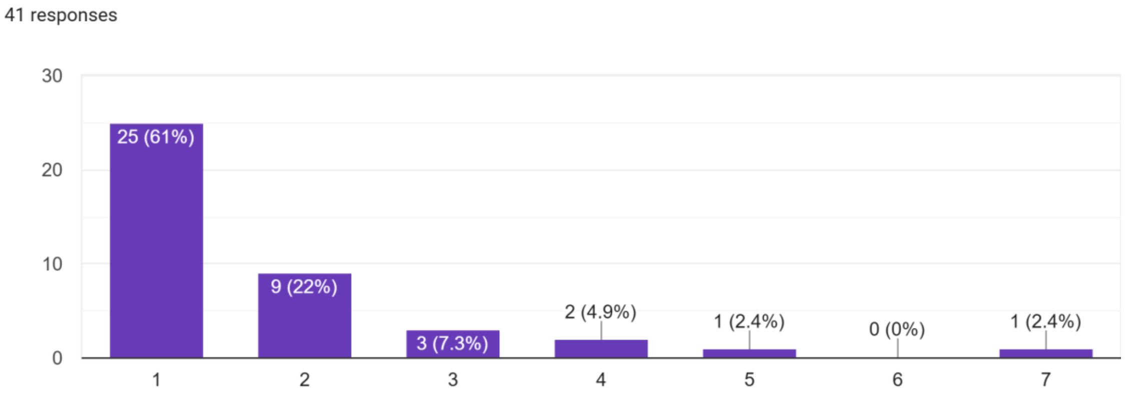
unpleasant vs pleasant



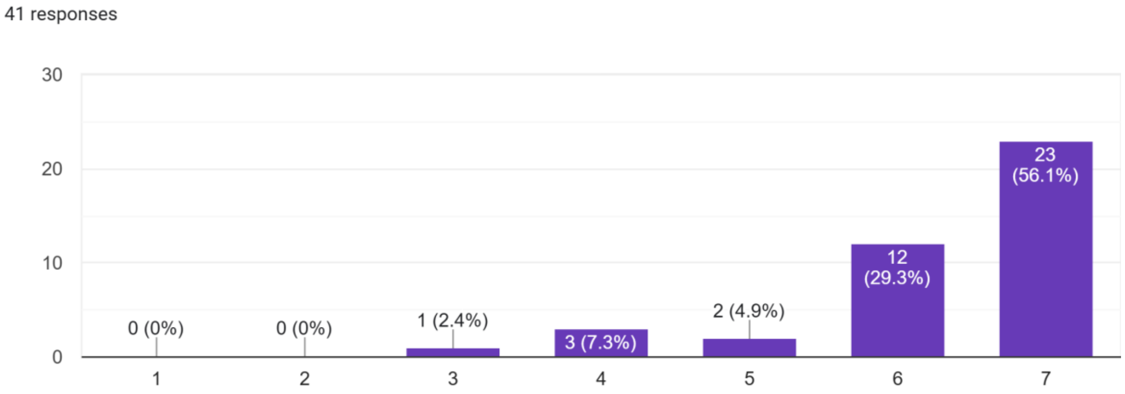
secure vs not secure

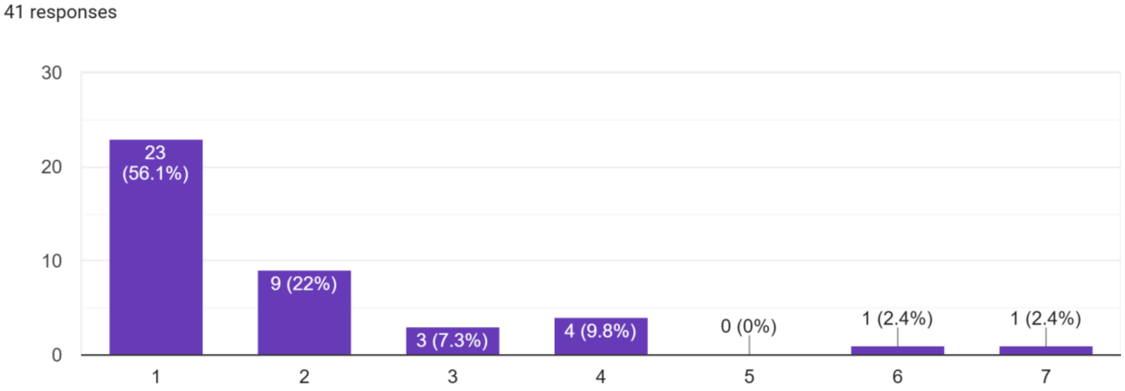


motivating vs demotivating



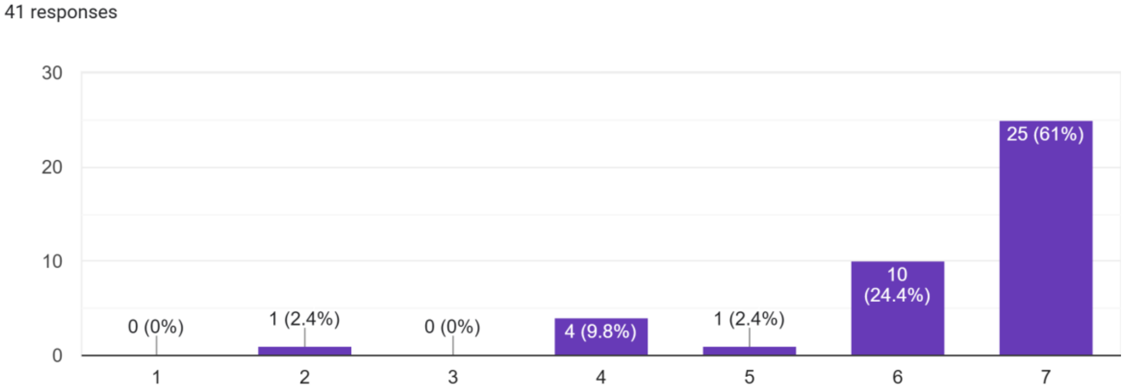
meets expectations vs does not meet expectations



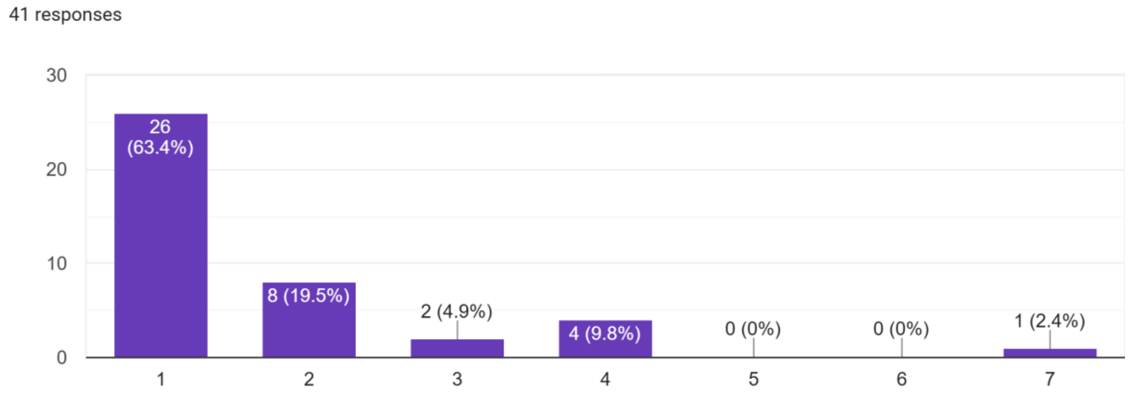


inefficient vs efficient

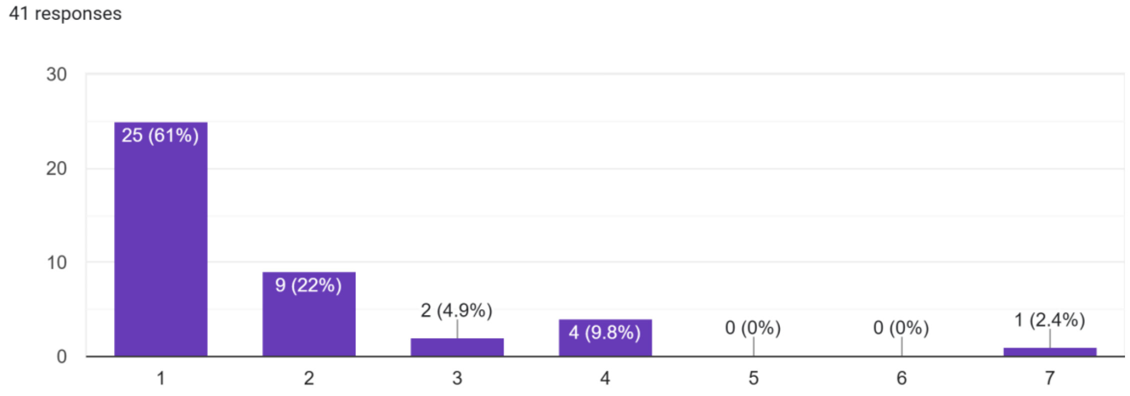
clear vs confusing



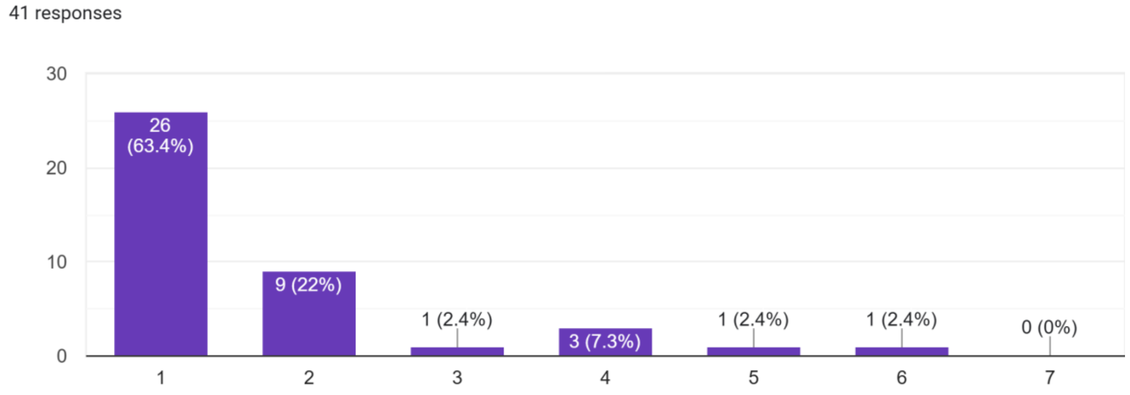
impractical vs practical



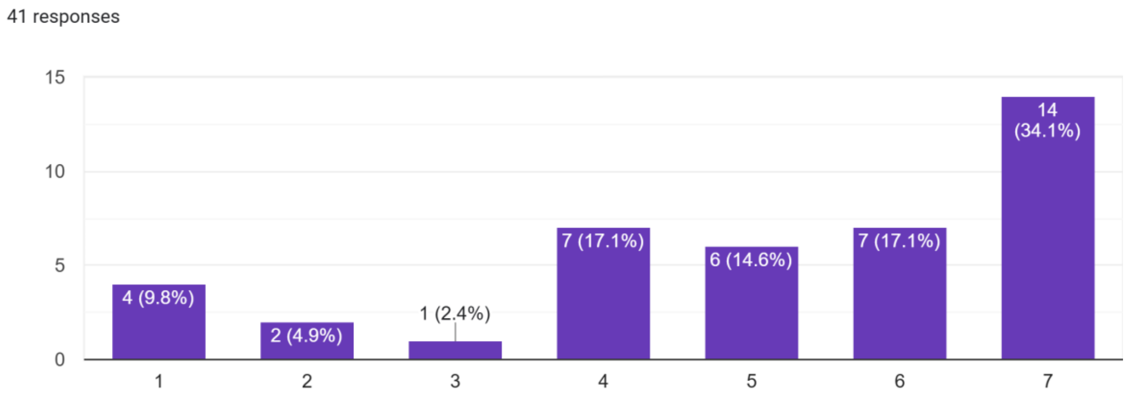
organized vs cluttered



attractive vs unattractive



friendly vs unfriendly



conservative vs innovative