University of Dublin

TRINITY COLLEGE

Developing a Privacy Canvas Model

Maurice Buckley

B.A.(Mod.) Computer Science

Final Year Project April 2019
Supervisor: Dr Dave Lewis

School of Computer Science and Statistics

O'Reilly Institute, Trinity College, Dublin 2, Ireland

Declaration

I hereby declare that this project is entirely my own work and that it has not been submitted as an exercise for a degree at this or any other university.

________________________________ _________________

Maurice Buckley Date

Permission to Lend

I agree that the Library and other agents of the College may lend or copy this report upon request.

________________________________   _________________

Maurice Buckley   Date

Table of Contents

Acknowledgements

Firstly, I would like to thank every person/group who participated in the Privacy Canvas study including those who went out of their way to help me find participants. For anyone to give up their free time around examinations etc deserves a tremendous amount of respect. I would also like to thank my family for their continuous support throughout my time here at Trinity College Dublin.

Finally, I would like to give my upmost thanks to my supervisor Dr David Lewis for providing his extensive support throughout this project. By making sure I was always on track, he made the daunting task of completing a final year project an enjoyable one.

Abstract

The recent introduction of the General Data Protection Regulation has brought with it a profound change on how businesses collect and process data. GDPR and its implications must now be considered a fundamental part of every business and must be considered from as early as possible in the lifecycle of every business. This brings with it its own issues due to the lack of knowledge about this newly introduced and extremely complicated regulation, particularly by young innovators. There needs to be suitable stepping stone into the world of GDPR that encapsulates its principles.

The Privacy Canvas is for early innovators with little knowledge of GDPR. It provides a first step towards understanding GDPR and GDPR compliance by using the canvas alongside the Business Model Canvas, effectively implementing privacy by design. Unlike other privacy and data protection tools, the Privacy Canvas provides a learning tool suitable for the early innovation stage.

1. Introduction

1.1 The Problem

In the twenty-first century, privacy and data protection has become a huge part of everyday life, particularly in the working world where businesses must uphold strict policy's and laws to protect themselves and their customers from data breaches. Failure to meet these privacy demands can result in huge fines and sanctions that can have a lasting effect on any business, large or small. The importance of adhering to data protection laws has increased dramatically with the introduction of the General Data Protection Regulation (GDPR) on the 25th of May 2018.

GDPR directly concerns all organisations within EU member states and any non-EU member state organisation that handles information to do with EU citizens. It imposes strict new rules regarding the collection, storage and use of personal data belonging to EU citizens in which failure to comply with these rules can result in huge fines to businesses or organisations. Prior to GDPR, fines of up to £500,000 could have been issued depending on the severity of the breach but with the introduction of the new regulation, fines can reach as much as 4% of annual global turnover or £20 million, with the fine being the larger of the two options (ITG, 2019).

Due to these new strict regulations and even stricter punishments, it is abundantly clear to any organisation or business that privacy and data protection is now an essential part of running any company. Businesses since the announcement and introduction of GDPR have been on catchup trying to change the operation of their business to now comply with GDPR which has imposed a huge cost due to the restructuring, redesign and change of policy, not to mention the cost of the mandatory training of staff. To avoid such heavy costs and problems later in a business's lifecycle, privacy and data protection must now be treated as an integral part of any business or project during the early innovation stages. Privacy by design should be a fundamental rule when starting any business and therefore privacy and data protection should be considered as the business model and plan is being created.

The problem most unexperienced entrepreneurs and most of the general population have is that they don't understand GDPR and don't know where to begin in attempting to prepare themselves for its implications. There needs to be a first step to GDPR compliance that initiates the discussion within a business that helps prepare them to meet these new obligations and protect themselves by incorporating privacy by design into their business model.

1.2 Project Aim

The Privacy Canvas was initially created as part of a final year project by former student at Trinity College Dublin Peter O'Leary in April 2018. As well as continuing his work and improving where possible, this author has taken his own approach to the Privacy Canvas and how it addresses privacy and data protection concerns. This project aims to address these privacy and data protection issues businesses have in three main ways; provide an easy to use iterative tool like the Business Model canvas which addresses privacy concerns to be used alongside the Business Model Canvas, create a tool suitable to be the first step towards understanding GDPR and GDPR compliance, and by effectively putting privacy by design into practice early on in the business innovation stage. The Privacy Canvas also has a technical implementation that was used for evaluation of this project while also demonstrating the proof of concept of a virtual Privacy Canvas.

The Business Model Canvas (BMC)

The Business Model Canvas (Osterwalder & Pigneur, 2010) is an easy to use tool that helps a group or person create an early model of their business during the innovation stage. The Business Model Canvas is highly practical due to its simplistic nature and how it creates a visual representation of their business that can be iterated over time after pivot points in the business's development. Visually representing information like this is very effective for any group as it creates a brainstorming atmosphere and opens the discussion within the group for possible changes and improvements. The Business Model Canvas has become very successful and popular within the business world and has been adopted by many.

This project intends to address the privacy and data protection concerns a business may face during early innovation stage by following the lead of the Ethics Canvas (Lewis, Reijers, & Pandit, 2018), a canvas similar to the BMC which addresses ethical issues, by redesigning the BMC to address privacy and data protection concerns. It is intended to take advantage of the popularity of the BMC and create a canvas to be developed with the BMC which will open the discussion on privacy within a new business or project and be the first step to GDPR compliance. This project will evaluate its use alongside the Business Model Canvas.

GDPR First Step

The general level of knowledge of everything GDPR including compliance and its consequences is extremely low, particularly in early innovators innovators leaving or just left college. My aim is to create a canvas tool that requires no previous knowledge of GDPR and introduces all the main concepts and compliance regulations in an easy to use and painless manner. It is my hope that the Privacy Canvas could be the first stepping stone for people trying to learn about GDPR by opening the thought process on privacy and data protection and as it will present it in a far less daunting way than other GDPR introductions. The Privacy Canvas could also be a pre cursor to a "Data Protection Impact Assessment"(DPIA) which is designed for more established businesses that hold highly sensitive data and not suitable to any business or organisation during the early innovation stage.

Privacy By Design

Privacy by design involves incorporating privacy and data protection into every step a business or organisation makes. It is a very important part of GDPR, and it can be described as "Organisations must implement technical and organisational measures to show that they have considered and integrated data compliance measures into their data processing activities." (Boardman, Mullock and Mole, 2017).

Businesses who follow the principles of privacy by design by always considering privacy and data protection implications during every action they make are far better prepared to meet GDPR obligations and therefore are protecting themselves in the future. By incorporating the Privacy Canvas into the early stages of the innovation process and continually iterating it as the business develops, I believe the business will be putting privacy by design into practice and effectively demonstrating compliance which as privacy by design is a principle of GDPR.

1.3 Readers Guide

The layout of this report is as follows:

Chapter 1: Introduction

Chapter 1 has introduced this project by briefly stating the problem and how it can be addressed.

Chapter 2: Motivation and Background

This Chapter covers the background research that went into this project including analysing the field, similar problems and solutions and my critique of the field that covers privacy and data protection.

Chapter 3: Method/Design

This chapter covers the various requirements that the Privacy Canvas has as well as the thought process behind my design. It will also cover the technical implementation and the design issues encountered.

Chapter 4: Research and Evaluation

This chapter will cover everything to do with my research and evaluation including my testing process, ethical approval and results.

Chapter 5: Conclusion

This chapter will summarise my project and cover my personal evaluation, learnings and close with closing remarks and future work.

2. Motivation and Background

This Chapter covers the background research that went into this project including analysing the field, similar problems and solutions, and my critique of the field that covers privacy and data protection.

2.1 Surveying the field

Today's online world has pushed the issue of privacy and data protection to the forefront which has therefore led to the mass creation of various online tools or compliance checkers. A quick google of "GDPR compliance" will show a plethora of these so-called privacy enhancing tools (PETs) that do little else than take advantage of this sprawling new market by charging subscriptions or memberships. Most of these compliance checkers are like a Data Protection Impact Assessment (DPIA) that test your level of compliance and give you a score rather than being a tool that helps you implement privacy by design by demonstrating compliance over time. It is also clear that the current available tools don't necessarily help organisations address privacy and data protection concerns during the early innovation stage. They are more suited to established businesses with greater GDPR needs and therefore have bigger GDPR implications. They also have far more knowledge and experience of GDPR because of this. There needs to be a tool suitable for the un-informed population when it comes to GDPR and provide a suitable first step towards understanding GDPR and being GDPR compliant.

It is my opinion that there is a gap in the market for tools that help implement privacy by design. The General Data Protection Regulation puts enough emphasis on the importance of privacy by design that it should be considered a necessity in all modern businesses and that should be reflected in the availability of privacy by design enhancing tools. The European Union Agency for Network and information Security (ENISA) defined a fascinating control matrix for evaluating privacy enhancing tools (PETs) in their report "PETs controls matrix - A systematic approach for assessing online and mobile privacy tools" (D'Acquisto et al., 2016). In this report they state that the assessment of privacy by design is a core focus of their control matrix even though there is not a specific assessment criterion. Instead they analyse how the numerous GDPR principles are put into action like accuracy, purpose limitations and transparency to name but a few. This has greatly impacted my thought process on how to best tackle privacy by design and has therefore had a huge influence on the design of the Privacy Canvas by focusing a great deal on the GDPR/privacy by design principles.

2.2 Similar Problems

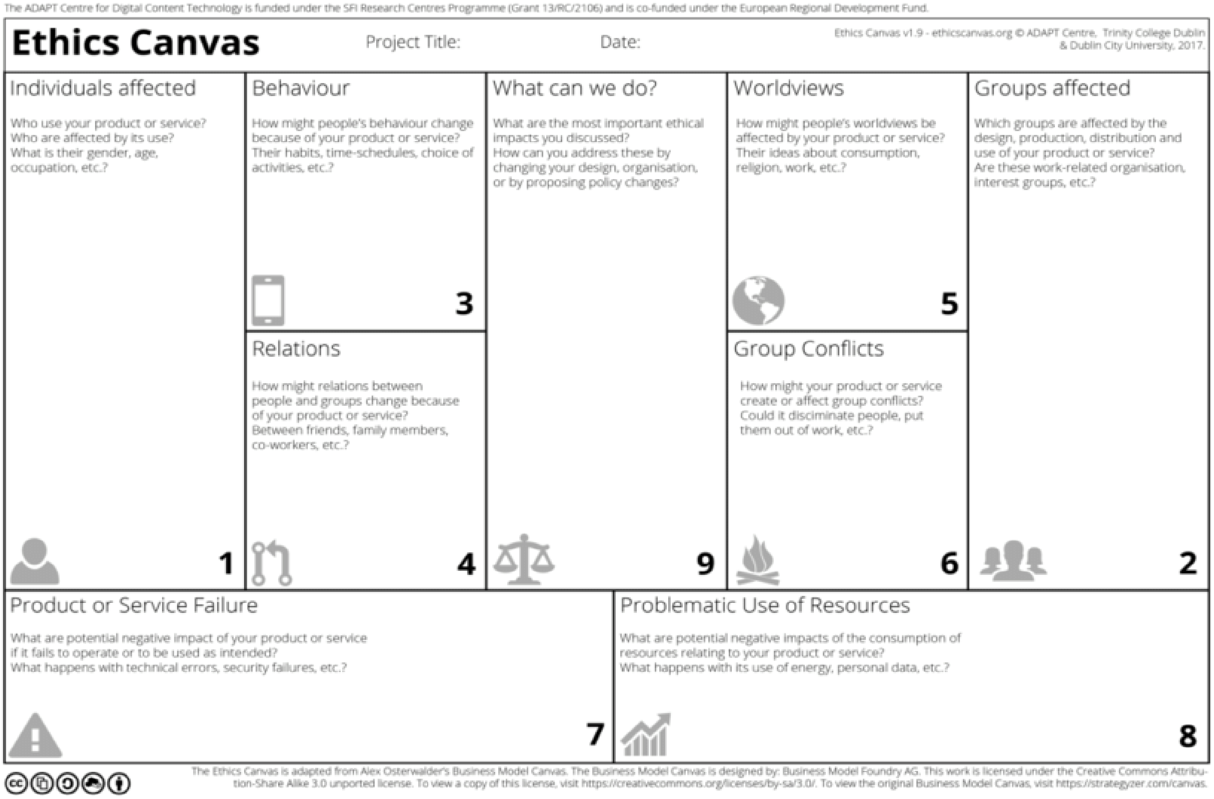
The Ethics Canvas

The Ethics Canvas (Lewis, Reijers, & Pandit, 2018) is a tool in which this project heavily analysed and studied due to the numerous similarities between the two projects. The Ethics Canvas is a canvas type tool which has also been based on the Business Model Canvas to tackle ethical concerns in the world of research and innovation of technology in a cooperative manner. It was developed here at Trinity College Dublin in the Adapt centre for digital content technology.

The Ethics Canvas like the BMC is divided into nine specific blocks. Unlike the BMC, they tackle ethical concerns and have been subdivided further into four main groups enhancing the way the canvas is completed. Blocks one and two identify relevant stakeholders. Blocks three to six consider the ethical implications on the previously identified stakeholders whereas blocks seven and eight consider the ethical impacts that are not stakeholder specific. The last block, nine, was a place where users of the Ethics Canvas could consider how to overcome these discussed ethical implications. These four groups of blocks together made up the canvas (Lewis, Reijers, & Pandit, 2018). This projects author found this design methodology very interesting and noticed how it enhanced the flow of the canvas when it would be created its users. The author took huge inspiration in the design methodology and transferred the thought process behind it to the Privacy Canvas where possible.

The evaluation of the Ethics Canvas conducted by the Ethics Canvas team also offered motivation to this project as their findings regarding the usefulness of the canvas and the effect the canvas had, in terms of impact on design or business model, was positive. The outcome of these findings gave this author confidence that a similar canvas that targets privacy and data protection concerns, the Privacy Canvas, would be effective.

Figure 1: The Ethics Canvas(Lewis, Reijers, & Pandit, 2018)



The ADAPT Centre for Digital Content Technology is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund.

Ethics Canvas Project Title: Date:

Ethics Canvas v1.9 - ethicscanvas.org © ADAPT Centre, Trinity College Dublin & Dublin City University, 2017.

Individuals affected

Who use your product or service?
Who are affected by its use?
What is their gender, age, occupation, etc.?

1

Behaviour

How might people's behaviour change because of your product or service?
Their habits, time-schedules, choice of activities, etc.?

3

Relations

How might relations between people and groups change because of your product or service?
Between friends, family members, co-workers, etc.?

4

What can we do?

What are the most important ethical impacts you discussed?
How can you address these by changing your design, organisation, or by proposing policy changes?

9

Worldviews

How might people's worldviews be affected by your product or service?
Their ideas about consumption, religion, work, etc.?

5

Group Conflicts

How might your product or service create or affect group conflicts?
Could it disciminate people, put them out of work, etc.?

6

Groups affected

Which groups are affected by the design, production, distribution and use of your product or service?
Are these work-related organisation, interest groups, etc.?

2

Product or Service Failure

What are potential negative impact of your product or service if it fails to operate or to be used as intended?
What happens with technical errors, security failures, etc.?

7

Problematic Use of Resources

What are potential negative impacts of the consumption of resources relating to your product or service?
What happens with its use of energy, personal data, etc.?

8

The Ethics Canvas is adapted from Alex Osterwalder's Business Model Canvas. The Business Model Canvas is designed by: Business Model Foundry AG. This work is licensed under the Creative Commons Attribution-Share Alike 3.0 unported license. To view a copy of this license, visit https://creativecommons.org/licenses/by-sa/3.0/. To view the original Business Model Canvas, visit https://strategyzer.com/canvas.

2.2 Critique Of the Field

The analysis of other resources which also help identify and address privacy and data protection concerns was of great importance to this project. Studying these various tools and resources gave this author an understanding of what works well and what doesn't when it comes to privacy and data protection. It also gave insight to what is missing in this area or what is not addressed correctly, like privacy by design. Two resources in particular were analysed in depth which gave this author a great appreciation of their work as well providing an understanding of what could be improved/addressed.

Privacy Canvas (Peter O'Leary, 2018)

As briefly described during the introduction of this project, the Privacy Canvas was originally developed as part of a final year project in 2018 here at Trinity College Dublin. It was designed as a canvas style brainstorming tool for data protection issues, being a proof of concept that such a canvas would have a use in the world of digital application design. Design of the canvas itself was designed as an analogy to the Business Model Canvas where the topics it covers were adapted to suit a Privacy Canvas. The evaluation of the canvas was carried out by getting small groups, who are developing or have developed an application that stores personal data, to fill out their own Privacy Canvas on paper followed by a questionnaire. The results of this study were predominantly positive which gave this author a strong insight into what works well and what doesn't when redesigning the canvas.

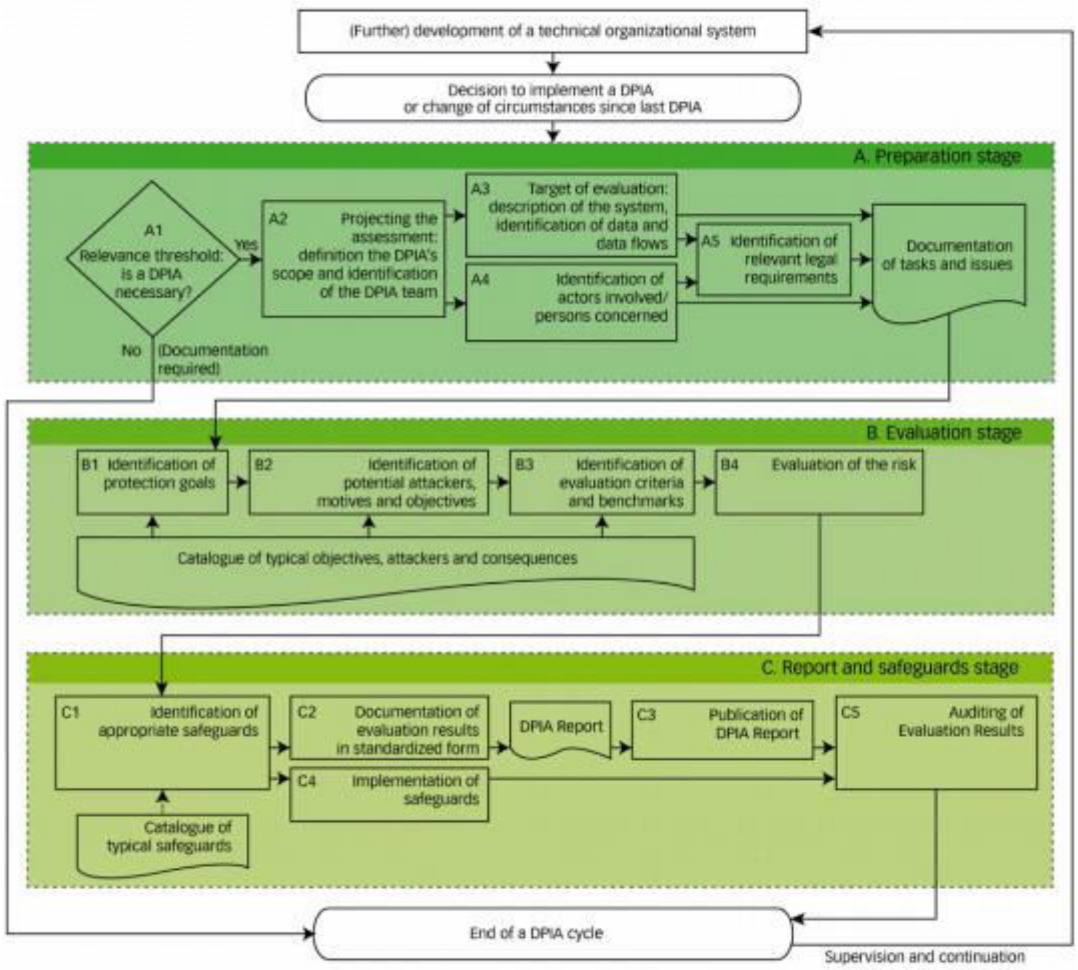
While this project is based on the original Privacy Canvas (O'Leary,2018), this author has adapted the project to try enhance the Privacy Canvas as a tool for privacy and data protection while also taking his own novel approach to the problem as well as implementing an online version to be used for testing. This approach includes a complete redesign of the canvas and evaluating its use alongside the Business Model Canvas, which is required as a precursor to testing. This project also attempts to create a learning tool more suitable as a first step towards GDPR while also targeting privacy by design with more detail by using the whole canvas to demonstrate privacy by design rather than one of the blocks on the canvas.

Data Protection Impact Assessment(DPIA)

Article 35 of the General Data Protection Regulation describes the execution of a Data Protection Impact Assessment (DPIA), which is mandatory under law for all organisations who collect and process "high risk" data (GDPR Article 35, 2016). A DPIA analyses and identifies data protection concerns and must be carried out following strict requirements laid out in article 35 which state when a DPIA is necessary, how it is to be conducted and post assessment requirements to name a few. One of these requirements under article 35(7)(d) is that : *"the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."* Which means that after the privacy concerns have been formally identified, measures must be put in place to address them.

In the informative paper "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation" (Bieker et al., 2016), it goes into great detail describing all aspect of a DPIA and has produced the following diagram to help provide an over view of this exhausting process which they have divided into three stages; preparation stage, evaluation stage and the reports and safeguards stage. During the preparation stage the need for a DPIA is considered. If it is deemed necessary, a DPIA team is put together and the relevant information is gathered. During the evaluation stage, data protection goals as well as potential risks are identified and evaluated. Finally, during the report and safeguard stage after privacy and data protection concerns have been assessed, the results are comprehensively documented, and relevant safeguards are identified and implemented. The DPIA report is required to be published to facilitate evaluation and comparison from various data protection authorities and the general public (Bieker et al.,2016).

Figure 2: DPIA process (Bieker et al., 2016)


(Further) development of a technical organizational system
Decision to implement a DPIA or change of circumstances since last DPIA
A. Preparation stage
A1 Relevance threshold: is a DPIA necessary?
Yes
No
(Documentation required)
A2 Projecting the assessment: definition the DPIA's scope and identification of the DPIA team
A3 Target of evaluation: description of the system, identification of data and data flows
A4 Identification of actors involved/ persons concerned
A5 Identification of relevant legal requirements
Documentation of tasks and issues
B. Evaluation stage
B1 Identification of protection goals
B2 Identification of potential attackers, motives and objectives
B3 Identification of evaluation criteria and benchmarks
B4 Evaluation of the risk
Catalogue of typical objectives, attackers and consequences
C. Report and safeguards stage
C1 Identification of appropriate safeguards
C2 Documentation of evaluation results in standardized form
DPIA Report
C3 Publication of DPIA Report
C5 Auditing of Evaluation Results
C4 Implementation of safeguards
Catalogue of typical safeguards
End of a DPIA cycle
Supervision and continuation

It is clear from the brief summary above, that the process of a DPIA is a long and strenuous task which requires great detail and understanding which may not be suitable for a new business in the innovation stage. The Privacy Canvas would be more suitable to a less established organisation who would not have their own legal department or data protection controller with far greater knowledge of GDPR and its implications. The Privacy Canvas would work far better with an organisation during the innovation stage who are likely to be following the agile development process by allowing continuous development or change and not restrict the organisation to certain assessment criteria outlined in a Data Protection Impact Assessment. The Privacy Canvas could be used as a precursor to a DPIA to help with its implementation further down the line.

2.3 Summary

Although there are many different tools available online in the field of privacy and data protection, there are not many tools that are like the Privacy Canvas which are more tailored towards growing businesses in the innovation stage and targets privacy by design. It is this authors opinion that if such a Privacy Canvas could be correctly created and implemented, learning from similar solutions like the Ethics Canvas and the previous Privacy Canvas, there would be a valuable use for it during the development stage of any digital application design.

3. Method/Design

This chapter covers the design intentions of the Privacy Canvas has as well as the thought process behind my design. It will also cover the technical implementation and the design issues encountered.

3.1 Intentions

As previously stated, the intended purpose of the Privacy Canvas is to be created alongside the creation of a Business Model Canvas and be a suitable first step towards GDPR in terms of requiring no previous knowledge of GDPR and being a suitable learning tool about GDPR for beginners during the innovation stage. The aim is to use the popularity of the BMC and make a Privacy Canvas that is used hand in hand with the BMC. The advantage of creating a brainstorming tool for privacy and data protection to be used when creating your business model is that you are effectively implementing privacy by design, a pillar of GDPR.

As the Privacy Canvas is based on the canvas model like the Business Model Canvas, it will follow the same canvas design principles of being divided into nine main blocks, each with their own unique importance. By sticking to this model, anyone who is creating a Business Model Canvas will also be able to create the Privacy alternative as they will be familiar with its canvas layout and design. The toughest challenge of the Privacy Canvas design is trying to create something that is suitable for someone with no knowledge of GDPR, but still have educational value, and making sure the canvas isn't daunting to attempt, like most GDPR related things are. It is this authors opinion that the best way to tackle this problem is to keep the casual brainstorming nature of the Business Model Canvas while also introducing key GDPR concepts and principals informally. The Privacy Canvas will open the discussion on key GDPR concepts but will not assess the user like most GDPR tools available. By removing the assessment aspect that most GDPR tools incorporate, the Privacy Canvas eliminates the intimidating element that is associated with GDPR and maintains the casual, helpful tone that is intended. The fact that the canvas is a brainstorming tool which has no right or wrong answer also aids this casual feel of the canvas. The blocks of the canvas will target the GDPR principles by introducing them informally in each block and starting the discussion around them, during this innovation stage. It is my hope that by introducing these key concepts and creating a thought process involving them, that when the business/organisation meet these concepts again further down the line during something like a Data Protection Impact Assessment, they will be far more prepared as they are familiar with the principles and have already considered them throughout the development of their business.

3.2 Canvas Design

The General Data Protection Regulation in total is 99 articles long which gave this project the difficult task of extensively researching GDPR and deciding how to incorporate the main concepts into a nine block Canvas while remaining true to the project's intentions described above. This author decided to base the canvas blocks mainly around the widely discussed "GDPR Principles". The GDPR principles vary in wording and numbers depending on the source but according to the data protection commission of Ireland, the eight principles are described below:

1. **Process it lawfully, fairly, and in a transparent manner;**
2. **Collect it only for one or more specified, explicit and legitimate purposes, and do not otherwise use it in a way that is incompatible with those purposes;**
3. **Ensure it is adequate, relevant and limited to what is necessary for the purpose it is processed;**
4. **Keep it accurate and up-to-date and erase or rectify any inaccurate data without delay;**
5. **Where it is kept in a way that allows you to identify who the data is about, retain it for no longer than is necessary;**
6. **Keep it secure by using appropriate technical and/or organisational security measures;**
7. **Be able to demonstrate your compliance with the above principles; and**
8. **Respond to requests by individuals seeking to exercise their data protection rights (for example the right of access).**

Figure 3. (The Eight Principles of Data Protection | Data Protection Commission, 2019)

By remaining true to these principles throughout the Privacy Canvas, the canvas would be instilling the main GDPR concepts into the user's mind and thought process.

From analysing the evaluation of the previous Privacy Canvas (O'Leary, 2018), multiple users commented that the flow of filling out the canvas was disrupted by having to traverse to canvas consistently to create the next block. O'Leary admits that this is something he overlooked and that it influenced the design flow of the user to a negative effect. This is something that I considered very important to address if I am to be successful in improving the Privacy Canvas. This author took inspiration from the Ethics Canvas (Lewis, Reijers, & Pandit, 2018) in how best to deal with this issue. The Ethics Canvas team decided to sub-divide their blocks into four main groups, with each group consisting of blocks that are somewhat related. They grouped the first two blocks together which identified relevant stakeholders, blocks three to six consider the ethical implications on these identified stakeholders, blocks seven and eight consider the ethical impacts that are not necessarily stakeholder specific, and the last block was a block where ideas to overcome these ethical impacts could be discussed which I thought was an exceptional way to finish a canvas. The Ethics Canvas' influence can be observed in The Privacy Canvas' layout as it too has been subdivided into four groups which are described below:

Blocks 1-3: These blocks are about the data subjects and the data that is being stored.

Blocks 4-6: How the business/project cooperates with the data subjects.

Blocks 7-8: Privacy and how the data is being protected.

Block 9: Preparation for a data breach.

The Individual Blocks and the thought process behind them are described next, as well as the helpful information that is provided in the user manual which aids the user when brainstorming about each block:

1. Data Group(s)

What type of people do you hold personal data on? Employees/Customers/Adults/Children etc?

A very simple opening block but fundamental for the purpose of the Privacy Canvas. The user must identify who they are holding data on. The block is first as completing it will help the user finish the rest of the canvas.

2. Data Type

What type of data do you hold? Children data? Sensitive data? Biometric data(data that could identify a person)?

A similar block to block one in terms of importance and complexity. Positioned straight after block one as they are very alike.

3. Purpose and Accuracy

What is the purpose of keeping this data? Is the data being updated to uphold its accuracy? Is there a time limitation on the storage of the data? Is the data only being used for the initial required use?

The last member of the first group which is solely to do with the data subjects and the data itself. Purpose and accuracy are multiple principles of GDPR. They relate to principals two, three and four described above, showing the importance of this multi-faceted block.

4. Consent

Has consent been asked for data collection or will it be asked? Is it presented clearly? Is consent revocable?

Another principle of GDPR which relates to principle two described above. Consent is a huge part of GDPR and is a necessity for any business planning on collecting data.

5. Transparency

Is there transparency in the processing and use of the data? I.e: Info notices, paper trails etc.

Directly relates to GDPR principle one about transparency , lawfulness and fairness. GDPR requires extensive paperwork regarding all processing of data so it is very important to introduce the idea of paper trails etc early on during the innovation stage.

6. Data Rights

Can data subjects access their data on request? Can the data be erased? Can data subjects object to certain types of use of the data eg: direct marketing? Will data subjects be notified on a data breach?

The last of the second block which relates to how your organisation cooperates with data subjects. Directly linked to GDPR principle eight. The rights of data subjects must be upheld and be considered throughout the innovation stage

7. Storage

Is there a storage time limitation? What technical measures have been taken to protect personal data from un-authorised access? What level of security is needed?

Relates to principle five of GDPR. The importance of storage almost goes without saying in terms of privacy and data protection but must still be addressed on the canvas due to this fundamental part of GDPR.

8. Data Governance

What measures have been implemented/completed to reduce the risk/impact of a breach? Eg: Data Protection Impact Assessment (DPIA), audits, policy reviews, data protection officer, privacy canvas, certifications.

The last of the third group about privacy and how the data is being protected and also related to principle six of GDPR. Regards the non-technical steps taken to address privacy and data protection. It is an area where the Privacy Canvas could be discussed as an action the organisation has completed regarding privacy.

9. Breach

What happens after a data breach? Who is notified? Do you maintain an internal breach register? Possibility of administration fines.

The final block doesn't relate to any GDPR principle. It takes a similar approach as the Ethics Canvas as the final block isn't a preventative block but rather one that helps overcome the implications of a data breach. Very important to be at least considered in every organisation, the earlier the better.

There is a tenth block which is there for notes only. It does not contribute to the project. That covers all the blocks. Seven out of eight principles were directly addressed leaving only GDPR principle seven left that states how you should be able to demonstrate compliance with the principles. The Privacy Canvas as a whole addresses this principle by incorporating them into each block. The Canvas also effectively implements privacy by design for the same reason, particularly when used alongside the Business Model Canvas.

3.3 Technical Implementation

The purpose of the implementation of the online/virtual Privacy Canvas is to take the canvas to the next step by allowing the evaluation of the canvas to be carried out online rather than on paper like the previous Privacy Canvas. It was also a proof of concept that the canvas translates well from paper and is suitable to be created online like the Business Model Canvas.

Before starting this project, this author was given access to the Ethics Canvas code base from this project's supervisor, who was a leading member of the Ethics Canvas team. The purpose of receiving the code base was that this project did not require any novel technical implementation but rather a proof of concept of a virtual Privacy Canvas. The Ethics Canvas had most of the required features needed as it also a canvas model. Using this code base greatly benefited the project as I didn't have to build this web application from nothing, saving me a countless amount of time that could be diverted towards research of GDPR, the design of the canvas and its evaluation which had greater importance. Refactoring the extensive Ethics Canvas code did however provide some of its own challenges and issues which will be described later in this chapter. The application uses the python-based Django web framework. The front end uses JavaScript frameworks, mainly Vue.js with some jQuery, and HTML and CSS for mark-up and styling. PHP is used for the backend and the database is abstracted by Django. All work on the canvas was completed and tested through a virtual machine using Debian.

Requirements

The requirements to run the canvas code:

Python 3.6.4

Django 2.0.5

Channels 2.1.1

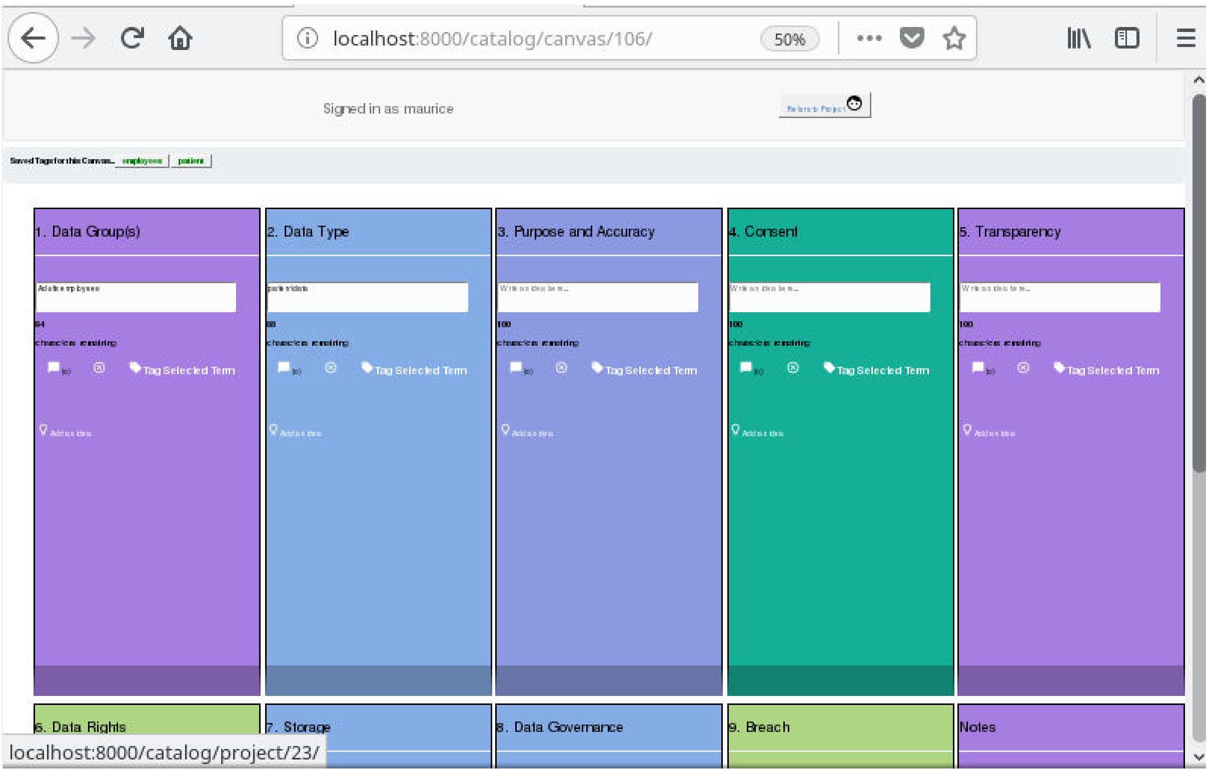
Channels_redis (listening on port 6379)

3.4 Features

Privacy Canvas

The canvas page where users create their own Privacy Canvas by filling out each block. On each block you can add numerous ideas which are one hundred characters long each. This is the most important page of the project as it is where the Privacy Canvas is being evaluated in terms of the theoretical canvas design. The first screenshot is zoomed out to show the whole canvas, the second is what users mainly saw when attempting the canvas.

Figure 4. Privacy Canvas



localhost:8000/catalog/canvas/106/

Signed in as maurice

Saved Tags for this Canvas... employees | patient

1. Data Group(s)
Add the employees
84
characters remaining

2. Data Type
park visitors
88
characters remaining

3. Purpose and Accuracy
Write an idea here...
100
characters remaining

4. Consent
Write an idea here...
100
characters remaining

5. Transparency
Write an idea here...
100
characters remaining

6. Data Rights

7. Storage

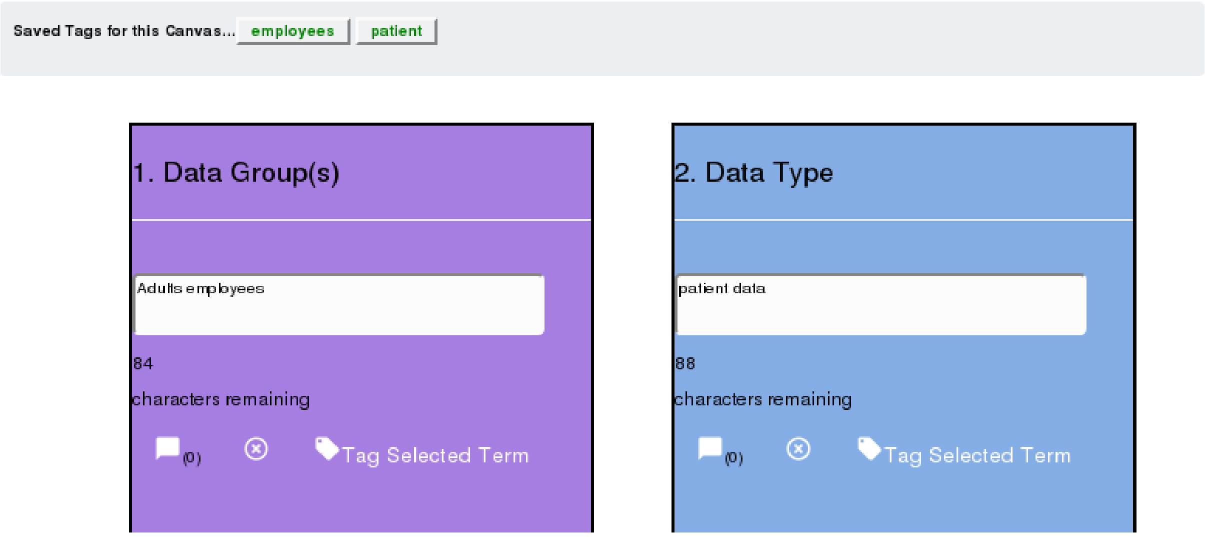
8. Data Governance

9. Breach

Notes

localhost:8000/catalog/project/23/

Figure 5. Privacy Canvas (Zoomed in)



Adults employees

84

characters remaining

patient data

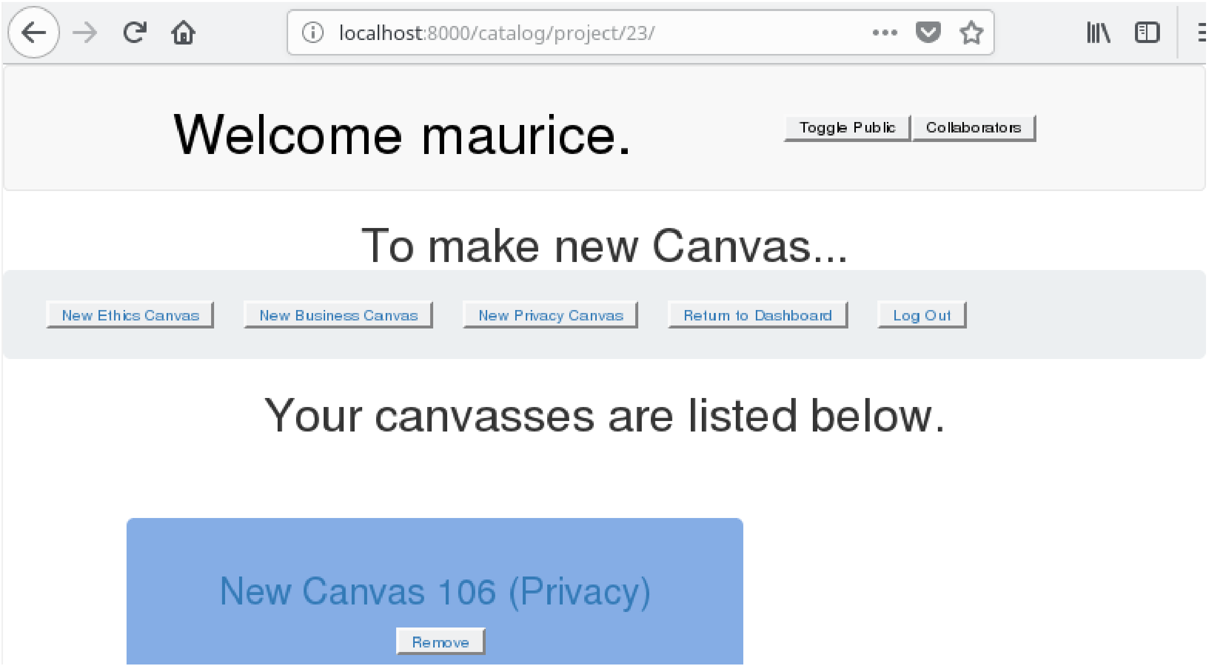
88

characters remaining

Project Homepage

The project homepage is where all the canvases you have created are stored, including the Business Model Canvas alternative if also created there. All Canvases are saved and can be returned to at any time. The ability to easily create, store and change is very beneficial to the canvas model as the ability to iterate your design as your business develops or pivots is fundamental to the ideology behind them.

Figure 6. Project Page



localhost:8000/catalog/project/23/

Welcome maurice.

To make new Canvas...

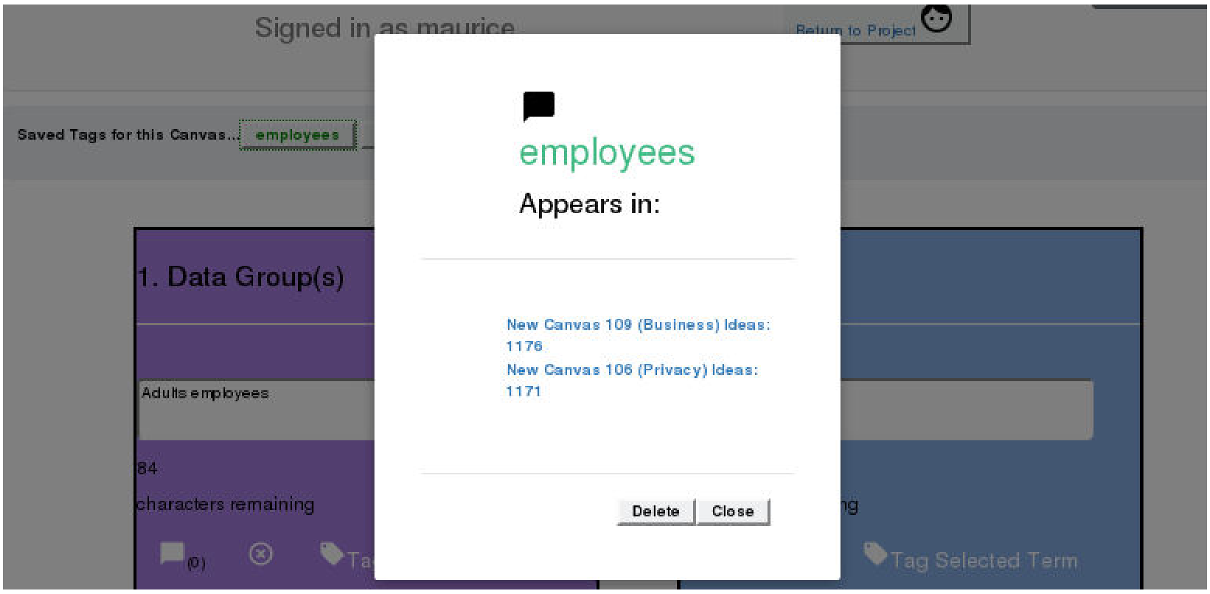
Your canvasses are listed below.

New Canvas 106 (Privacy)

Tags

Users have the ability to tag keywords as they create their canvases which shows what ideas are related by having the tag string as a substring of the idea fields content. The user can click on the tag and the location of where this tag exists elsewhere is displayed. The user can click on a location and that canvas will open in a new tab. The ability to easily view similar canvases benefits the creation of a Privacy Canvas alongside the business alternative.

Figure 7. Tag example



Signed in as maurice

Saved Tags for this Canvas... employees

employees

Appears in:

New Canvas 109 (Business) Ideas: 1176

New Canvas 106 (Privacy) Ideas: 1171

1. Data Group(s)

Adults employees

84

characters remaining

3.5 Design Issues

Overall there was no major issues, just little speed bumps along the way as expected. Having to refactor the very large Ethics Canvas code base had its own issues, mainly my unfamiliarity with the very large code base and web design in general but provided an interesting learning opportunity for me. Getting the canvas code to run took a significant amount of time. Having to work through a virtual machine was a nuisance but was done so under the recommendation of the previous worker on the code base as getting a UNIX terminal in windows would cause more pain than was needed. Any Linux distribution would have worked but the virtual machine was sufficient for the purpose of this project as a proof of concept but did affect the usability of the application and its appearance. I also had no previous knowledge of GDPR which provided its own challenge for the design of the canvas itself. It was extremely important that the canvas would tackle the correct GDPR concepts so that the canvas had value as a learning tool and demonstrate privacy by design. This required the author to have extensive research on GDPR and the area of privacy and data protection in general.

4. Research + Evaluation

This chapter will cover everything to do with my research and evaluation of the Privacy Canvas including my testing process, ethical application and results.

4.1 Testing Process

The testing process follows the lead of the previous Privacy Canvas from last year, with some changes, as it is the most effective way to test the canvas given the scope and timeframe of the project. The Privacy Canvas was tested by eight individuals/groups which met with the author over the course of the project.

The participants were briefed using the information sheet, consent form and user manual with the author also available for questions. Participants completed a copy of the Privacy Canvas on a laptop or computer with the prerequisite of the completion of a Business Model Canvas. The canvas could be completed individually or by a group. Filling out the privacy canvas will not require the user to write their name or any other personal data. The participants will then be sent an electronic questionnaire to record their experience of using the canvas. The questionnaire consisted of fifteen questions, with the first ten questions being a standard system usability scale. The questionnaire results will be anonymized, and this information will be used by the researcher to assess the effectiveness of the canvas. The total expected completion time of the study was no more than thirty minutes. The information sheet, consent form, questionnaire and user manual can all be found in the appendix at the end of this report.

4.2 Participants

Volunteer participants were male or female and over the age of eighteen, mainly consisting of third level students at Trinity College Dublin. Participants are required to have completed a Business Model Canvas as a prerequisite of participation for the purpose of evaluating the Privacy Canvases use alongside the business alternative. They must also have developed or currently developing an application that stores personal data. Previous knowledge of GDPR was not required, very little knowledge was in fact encouraged for the purpose of evaluating the canvas as a first step towards GDPR.

Participants were gathered in a few ways. The students of MSc course CS7CS2 of Trinity College were emailed asking for volunteers to participate in the study as they have completed a Business Model Canvas as part of their continuous assessment. Trinity's Tangent and LaunchBox programs also posted on their respective social media pages, with thousands of followers, and said:

"Want to get started thinking about GDPR compliance for your start-up? Contact Maurice <bucklem8@tcd.ie> to try out his "Privacy Canvas"… Like a lean canvas, but for data security".

Tangent and LaunchBox are start-up incubators where start-ups and other businesses in the early innovation stage receive guidance and funding. These start-ups would be the exact target market wanted for the Privacy Canvas, so I was delighted to hear about the interest in the canvas from the various managers of these programs who offered to post about it online. Lastly, this author gathered the remaining participants from recruiting students who had developed or are currently developing suitable applications. The completed Privacy Canvases can be found in the appendix at the end of this report.

4.3 Ethical Approval

As the Privacy Canvas is a research project which involves human participation and gathers information in the form of the canvas and questionnaires, it was compulsory to be reviewed by the independent research ethics committee belonging to the school of computer science and statistics. Ethical approval was required before the commencement of the study/testing could take place.

The ethical approval application form consisted of an information sheet, consent form, research proposal, questionnaire and was to be signed by this project's supervisor and myself. Thankfully this project was not in violation with the ethical guidelines and was given ethical approval without much delay. The full ethics application can be found in the appendix at the end of this report.

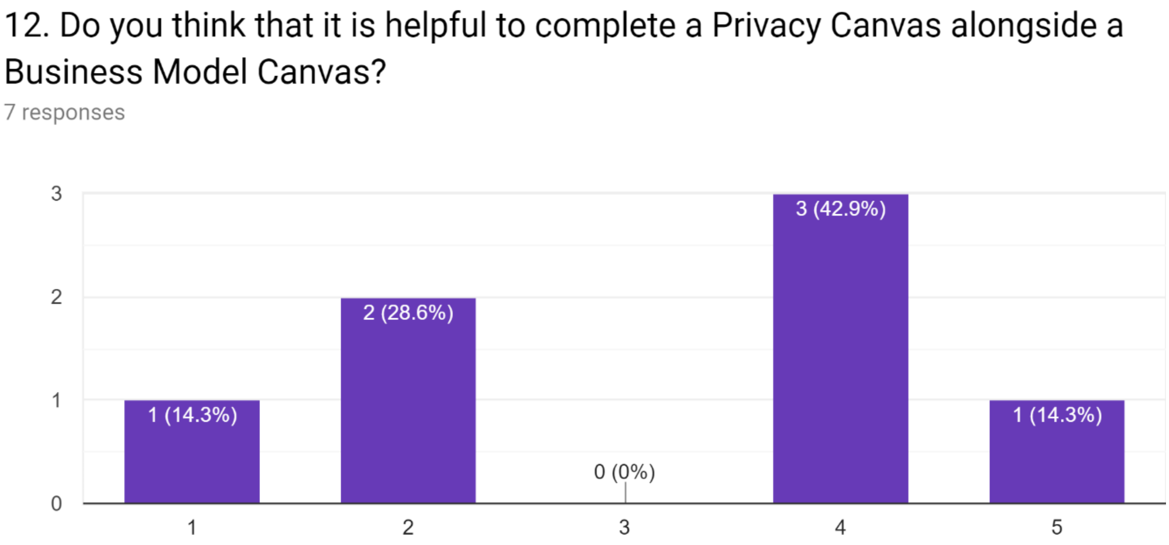
4.4 Results

The Privacy Canvas was evaluated by users of the system completing a questionnaire in their own time as well as giving general feedback to the author while testing was going on and after. The questionnaire consisted of fifteen questions with the first ten being the industry standard system usability scale (SUS), and the last five questions are more targeted to the concept of the Privacy Canvas itself. I decided to include the SUS as it has proven to be a dependable method of evaluating systems usability over its thirty-year lifecycle and is very well known in the field. The scale is evaluated by users answering ten questions using a Likert scale with one being strongly disagree and five being strongly agree. These answers after some calculations give a score out of a hundred, which is not a percentage. Sixty-eight being the average score for a SUS.

Questionnaire Score

The system usability scale answers were very encouraging which reassured the proof of concept of the Privacy Canvas virtual implementation. 85.8% of users gave a positive answer when asked if they would like to use this system again with no negative answers and only one neutral answer. 85.8% again disagreed that the system was unnecessarily complex with only one negative response. 100% of users agreed that the system was easy to use with 57.1% of them strongly agreeing. 100% of users disagreed that they would need the help of a technical person to use this system. 57.2% of users found that the functions of the system were well integrated with the other 42.9% giving a neutral response. When asked if there was too much inconsistency in the system, 100% of users disagreed with this statement. 85.8% imagined that most people would learn to use this system easily and 85.8% also disagreed that they found the system cumbersome to use. 57.2% of users felt confident using the system with 14.3% of the users disagreeing. Finally, 100% of users disagreed with the statement that they needed to learn a lot of things before using this system. These results were extremely positive, giving an overall score of 82.86/100 for the SUS with 68 being average and 80.3+ considered an A.

The final five questions were not as positive and in fact were very inconsistent in their answers with an even spread of positive and negative answers. This went against the feedback received from the users about the Privacy Canvas as the feedback was extremely positive. I believe I am at fault for this due to what I thought was a good decision in how I structured the remaining questions. I decided to flip the scale from one being strongly disagree to now one being strongly agree for the final five questions. My thought process was to keep user's vigilante to make sure they weren't just brainlessly answering the questionnaire, but I believe this backfired as I think only some users noticed this change in the answering format. A follow up email to some of the participants confirmed this theory which coincided with the high variance of the answers of the questions. Most questions had an almost even split (almost even due to odd number of surveys completed) when it came to positive or negative responses. An example of this is shown below in where users were asked if they thought it was helpful to complete a privacy canvas alongside a Business Model Canvas where three agreed and four disagreed. I therefore believe that the final five questions should be discredited due to the strong evidence of the error in the answering format which evidently affected the results as they do not coincide with the SUS scale and the general feedback received. The full questionnaire results can be found at the end of this report including a link to the online survey. Readers of this project should draw their own conclusions from these findings.



12. Do you think that it is helpful to complete a Privacy Canvas alongside a Business Model Canvas?

7 responses

Feedback

Feedback regards the general feedback received from users while evaluating the Privacy Canvas where users were asked for their thoughts on the canvas. The feedback received was predominantly very positive and coincided with the aims of this project of the Privacy Canvas being a suitable first step towards GDPR and privacy by design.

Most users had very little knowledge of GDPR before attempting the canvas and hadn’t thought about some of the concepts while developing their digital application, particularly about data governance and transparency in the processing of personal data. This reassured the author that Privacy Canvas was suitable as a first step towards GDPR and its ability to introduce these concepts to the un-experienced people in the early innovation stage of their product, in terms of GDPR.

Two participants of the study have a strong history of working with start-ups and other groups in the early innovation stage which enhanced the credibility of their feedback as they work daily with the exact target market of the intended users of the Privacy Canvas. One of the participants was a programme manager at Tangent and LaunchBox who was fascinated with the concept of the Privacy Canvas and saw great potential for its use with his start-up groups who all complete a Business

Model Canvas. It was without the author asking that this participant asked permission to post about the Privacy Canvas on their social media pages with thousands of followers about the canvas and advertising this study which provided more participants. This author drew great satisfaction from this as it was beyond what he could have wished for as a proof of concept for the Privacy Canvas. This user works with many early innovators daily and believed in the potential of the canvas as a useful first step tool for GDPR and agreed with the concept that its use alongside the BMC would be beneficial and help demonstrate privacy by design. This feedback was also compounded from the other participant who works with start-ups who also saw the potential of the Privacy Canvas. This user in fact saw another use for the canvas which the author was unfamiliar with. This user said that the Privacy Canvas could be incorporated into a “customer Journey map” which is a visual representation of a customer’s interaction with your business.

Some users commented that the canvas wasn’t applicable to their business which was to be expected by the author as the Privacy Canvas is very general to allow many different types of businesses to use it rather than it be tailored to a particular type of digital application. Participants who developed the Privacy Canvas for a previous application also had issues with some blocks of the canvas as GDPR hadn’t come into effect when they were growing that business. This meant that some requirements of GDPR like consent and data governance were not required at the time and therefore the user had no need to implement the relevant features.

4.5 Difficulties

The research and evaluation of the Privacy Canvas provided many difficulties, some of which have been already discussed. A profound difficulty was finding volunteers to participate in the research study of the canvas. This was due to the increased difficulty of finding volunteers who met the criteria for participation including having completed a BMC and developed/developing an application that stores personal data. It was also difficult to find volunteers to give up their free time in the extremely busy month of April where exams and final assessments take place. In terms of testing itself, the previously described issue with the final questionnaire answer format was detrimental to the quality of the evaluation in which this author takes full blame for overlooking it. There was also an issue with one participant not completing the survey after testing the virtual implementation of the Privacy Canvas which could not be identified due to the anonymous answers. This affected the study as it decreased the number of survey responses which reduces the credibility of the study. Overall however, the study was sufficient for the purpose of this project and given more time I believe these issues could have been easily fixed.

5. Conclusion

This chapter will summarise my project close with future work and final thoughts.

5.1 Project Summary

This project opened by identifying the challenges that the new General Data Protection Regulation and its laws bring to every business. These new regulations have only been implemented for less than a year, so the solution to these challenges are only being developed and tried. The Privacy Canvas makes its own attempt to alleviate the pressure of GDPR early in the innovation stage of any new business. It does so by creating a tool to be used alongside the Business Model Canvas, which is suitable for early innovators with little experience dealing with privacy and data protection while also demonstrating compliance with privacy by design.

Extensive research into GDPR and the various state of the art tools available was conducted by this author in an effort to design the best possible tool he could to tackle the aims of this project. This resulted in an excessively thought out design that try's best to encapsulate the principles of GDPR while attempting to achieve the goals of the project that were laid out including a virtual implementation. To test the validity of this design, a comprehensive study was carried out involving the evaluation of the Privacy Canvas. Although this study had some flaws, this author believes that the Privacy Canvas achieved its initial aims of being a suitable first step GDPR tool that is used alongside the Business Model Canvas and therefore implements privacy by design.

Despite the fact the Privacy Canvas meets the initial aims of the project, there are always ways to improve. Difficulties in the research study have hindered the results of this project. These problems however would be an easy fix had the scope of this project extended past the end of the semester allowing the author to correct his mistakes and allow for a longer, more thorough evaluation.

5.2 Future Work

As with all college confined projects, there are many changes that could be made had the project more time to be completed. If given more time, this author would have put aside the previous study and conduct a whole new study for a more accurate analysis of the canvas and provide more evidence that the previous survey final questions, were flawed. This would also allow for the recruitment of far more participants, as the project would no longer have as much time constraints which would ease the difficult task of finding volunteers who meet the requirements.

To truly evaluate the use of the Privacy Canvas with the Business alternative, the research study would have to allow for multiple iterations of the Privacy Canvas per user as they also iterated their BMC after pivot points or changes in their business. This was not suitable given the current scope of the project, but if given the opportunity to work on the Privacy Canvas in the future, the addition of multiple iterations would be included in the study.

More time would also allow for the creation of a suitable Privacy Canvas web application built from scratch that is specifically tailored to the needs of the Privacy Canvas, rather than refactoring the design of the ethics alternative. An independent web application would have its benefits, however they would only be superficial to the requirements of this project as the refactored code base was sufficient for the needs of this project.

The Privacy Canvas like its business and ethics alternatives has a general design to meet the needs of many types of businesses/organisations and therefore may not work as well with certain business types. More time would allow for multiple designs that are more tailored to certain fields of the business world.

5.3 Closing Remarks

I am extremely grateful to this project for the numerous lessons and skills it has thought me. Going into this project with no previous knowledge of GDPR and having to refactor someone else’s code base provided many difficulties, but thankfully these difficulties could be overcome through hard work, dedication and guidance of this project’s supervisor.

This project was ultimately a proof of concept in a Privacy Canvas that helps tackle privacy and data protection concerns. This author firmly believes that there is in fact a gap in the market for tool like the Privacy Canvas that helps educate the uninformed when it comes to GDPR and as a tool that demonstrates privacy by design. The true impact of GDPR has yet to be seen due to its recent implementation but this author feels that privacy and data protection must now be considered from the earliest possible stage of a business’s development. Taking advantage of a very well-known and used tool like the Business Model Canvas is an effective start but work on tools like the Privacy Canvas must be continued. I have no doubt that in the following years as GDPR and its implications progresses, we will see many more tools that will attempt to tackle this problem, maybe even following the lead of the Privacy Canvas.

Appendix

Appendix 1: Ethics Application

Project Proposal

School of Computer Science and Statistics

Research Ethical Application Form

Project Title: Developing a Privacy Canvas Model

Project Purpose

This project aims to refine the "Privacy Canvas" by evaluating its use alongside the Business Model Canvas. This project intends to build on the work of the previous Privacy Canvas project which was completed by former student Peter O'Leary in April 2018. The Privacy Canvas is a tool that can be used by a business or on a project basis to help address privacy and data protection concerns. The Privacy Canvas has been modelled on the Business Model Canvas (Osterwalder & Pigneur, 2010), and can be used as a foundation for a business or project to address its data protection concerns. It is intended that the Privacy Canvas could be developed alongside the creation of a Business Model Canvas and could be further developed iteratively with the Business Model Canvas . A main motivation for this project is to consider the impact of the new "General Data Protection Regulation", which came into effect in May 2018, early on in the business innovation process.

This project is also Maurice Buckley's final year project for his fourth year as a Computer Science student in Trinity College Dublin.

Methods and Measurement

Participants will complete a copy of the Privacy Canvas on a laptop or computer with the prerequisite of the completion of a Business Model Canvas. This can be completed individually or by a group. Filling out the privacy canvas will not require the user to write their name or any other personal data. The participants will then be sent an electronic questionnaire to record their experience of using the canvas. The questionnaire results will be anonymized. This information will be used by the researchers to assess the effectiveness of the canvas.

Recruitment of Participants

Subjects will be selected from the MSc course CS7CS2 and other courses that have worked with the business canvas tool. The participants will be third level students between the ages of 18-30 and will include both males and females.
Subjects will also be selected from the colleges LaunchBox Program and other similar Innovation programs. These students will be able to take part in the study using their start-up projects.

Debriefing Arrangements

The debriefing section states that once their data is submitted it will not be possible to withdraw the data from the study, as it will be anonymized. Participants will be informed that their information will not be held for longer than needed to validate the study and will only be used for the purposes of the study. Participants will also be explicitly warned that once their data is submitted and anonymized, it cannot be withdrawn from the study as it will no longer be identifiable.

Ethical Considerations Raised

One ethical issue could be linking of the answers from the questionnaire and the data used to the student in the class. To combat this issue, no names are required to fill out the Privacy canvas and the questionnaires are filled in anonymously. The prerequisite of having a completed Business Model Canvas may be an ethical issue as it may interfere with the anonymity of the research. Another possible ethical issue is that Dave Lewis (this project’s supervisor) is involved in the grading of some of the students that may provide data for the project. The nature of a student’s replies and whether they choose to participate in the study will not affect their grade for any of their courses. Participants will be clearly informed that they may choose to opt out of the study and that all result will be kept anonymous.

Legislation

This research will comply with the legal requirements laid down in the Irish Data protection act 1998 in its revised version of the 14th of October 2014.

Information Sheet

TRINITY COLLEGE DUBLIN

INFORMATION SHEET FOR PARTICIPANTS

PRIVACY CANVAS

1. My name is Maurice Buckley, a final year student of Computer Science in Trinity College Dublin. This project aims to refine the "Privacy Canvas" by evaluating its use alongside the Business Model Canvas. The Privacy Canvas is a tool that can be used by a business or on a project basis to help address privacy and data protection concerns during the innovation process. The Privacy Canvas has been modelled on the Business Model Canvas and can be used as a foundation for a business or project to address its data protection concerns.

2. This project intends to build on the work of the previous Privacy Canvas project which was completed by former student Peter O'Leary in April 2018.

3. Participants will complete a copy of the Privacy Canvas on a laptop or computer and answer a questionnaire afterwards. The total time should take no longer than 45 minutes to complete. The completed privacy canvases and questionnaire answers will be used as empirical data for this project.

4. This project is voluntary, and participants have the right to withdraw or omit individual responses before they submit them. All information will be completely anonymously.

5. Participants were chosen due to prior completion of a Business Model Canvas or are currently in the innovation process where use of a privacy canvas could be applicable/beneficial.

6. The collected data will only be used by the researchers of this project and the anonymity of the data will remain in analysis, publication and presentation of resulting data and findings.

7. Participation in this project will not benefit the result of any module or coursework and will not be used for or against the participant.

8. To keep the anonymity of the data, please do not personalise the privacy canvas or questionnaire with any personal information that could be used to identify the participant.

9. The data will be stored for the duration of the project.

10. In the extremely unlikely event that illicit activity is reported I will be obliged to report it to the appropriate authorities

11. The project lead researcher can be contacted any time for any further questions relating to the participants participation in this project by emailing bucklem8@tcd.ie

Questionnaire Questions

Online questionnaire can be found at:

https://docs.google.com/forms/d/e/1FAIpQLSeMwXVJ3wBe3JivptDpTPZQcH95Y5LPQYe7MiRYz0PlbqwCCQ/viewform?usp=sf_link

Privacy Canvas Questionnaire Questions

All questions will be answered by picking 1 of 5 options from strongly agree to strongly disagree apart from questions in the which the participant is asked to give a more detailed response. Some questions possible answers will be inverted to strongly disagree to strongly agree to ensure the participant remains vigil and alert. The Questionnaire will be made and completed online and the first 10 questions will be the System Usability Scale (SUS).

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

11. Did completion of the Privacy Canvas help you address and give you a better understanding of privacy and data protection concerns for your project/business?
12. Do you think that it is helpful to complete a Privacy Canvas alongside a Business Model Canvas?
13. The privacy and data protection concern for my project/business were not applicable to the Privacy Canvas? If so please elaborate.
14. The Privacy Canvas helped identify privacy or data concerns that were not previously thought about.
15. The Privacy Canvas would be a useful tool in the project/business innovation process?

Informed Consent Form

TRINITY COLLEGE DUBLIN

INFORMED CONSENT FORM

LEAD RESEARCHERS: Maurice Buckley

BACKGROUND OF RESEARCH: This project aims to refine the "Privacy Canvas" by evaluating its use alongside the Business Model Canvas. The Privacy Canvas is a tool that can be used by a business or on a project basis to help address privacy and data protection concerns during the innovation process. The Privacy Canvas has been modelled on the Business Model Canvas.

This project is being undertaken by the researcher Maurice Buckley as part of his final year in Computer Science in Trinity College Dublin. This project builds upon on the work of the previous Privacy Canvas project which was completed by former student Peter O'Leary in April 2018.

PROCEDURES OF THIS STUDY: Participants will complete a copy of the Privacy Canvas on a laptop or computer and answer a questionnaire afterwards with the prerequisite of the completion of a Business Model Canvas. The total time should take no longer than 45 minutes to complete. The completed privacy canvases and questionnaire answers will be used as empirical data for this project. The data will remain anonymous and therefore should hold no risk to the participant.

PUBLICATION: The data collected will be used as part of the researcher's final year project and will be presented to and assessed by members of Trinity College Dublin. Individual results will be aggregated anonymously, and research reported on aggregate results.

DECLARATION:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.

- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- If the research involves viewing materials via a computer monitor> I understand that if I or anyone in my family has a history of epilepsy then I am proceeding at my own risk.
- I have received a copy of this agreement.

PARTICIPANT'S NAME:

PARTICIPANT'S SIGNATURE:

Date:

Statement of investigator's responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

RESEARCHERS CONTACT DETAILS: bucklem8@tcd.ie

INVESTIGATOR'S SIGNATURE:

Date:

Appendix 2: User Manuel

Privacy Canvas

About the Privacy Canvas

The Privacy Canvas is a tool that can be used by a business or on a project basis to help address privacy and data protection concerns during the innovation stages of that business/project. The Privacy Canvas has been modelled on the Business Model Canvas (Osterwalder & Pigneur, 2010), and can be used to help incorporate privacy by design early in that project or business' growth. The Canvas will help people understand GDPR and help them protect their business/project by starting the discussion on it, even if the business or project owners have limited knowledge of GDPR. The Privacy Canvas could be used similarly to a "Data Protection Impact Assessment (DPIA)" except for non high-risk projects. It is intended that the Privacy Canvas be developed alongside the creation of a Business Model Canvas and possibly an Ethics Canvas (Online Ethics Canvas, 2017), and could be further developed iteratively with the Business Model Canvas.

A main motivation for this project is to consider the impact of the new "General Data Protection Regulation", which came into effect in May 2018. This project is also Maurice Buckley's final year project for his fourth year as a Computer Science student at Trinity College Dublin.

How It Works

The Canvas has been divided into blocks 1-9 which each hold a particular purpose, described below:

Blocks 1-3: These blocks are about the data subjects and the data that is being stored.

Blocks 4-6: How the business/project cooperates with the data subjects.

Blocks 7-8: Privacy and how the data is being protected.

Block 9: Preparation for a data breach.

About Each Block

1. Data Group(s)

What type of people do you hold personal data on? Employees/Customers/Adults/Children etc?

2. Data Type

What type of data do you hold? Children data? Sensitive data? Biometric data(data that could identify a person)?

3. Purpose and Accuracy

What is the purpose of keeping this data? Is the data being updated to uphold its accuracy? Is there a time limitation on the storage of the data? Is the data only being used for the initial required use?

4. Consent

Has consent been asked for data collection or will it be asked? Is it presented clearly? Is consent revocable?

5. Transparency

Is there transparency in the processing and use of the data? I.e: Info notices, paper trails etc.

6. Data Rights

Can data subjects access their data on request? Can the data be erased? Can data subjects object to certain types of use of the data eg: direct marketing? Will data subjects be notified on a data breach?

7. Storage

Is there a storage time limitation? What technical measures have been taken to protect personal data from un-authorised access? What level of security is needed?

8. Data Governance

What measures have been implemented/completed to reduce the risk/impact of a breach? Eg: Data Protection Impact Assessment (DPIA), audits, policy reviews, data protection officer, privacy canvas, certifications.

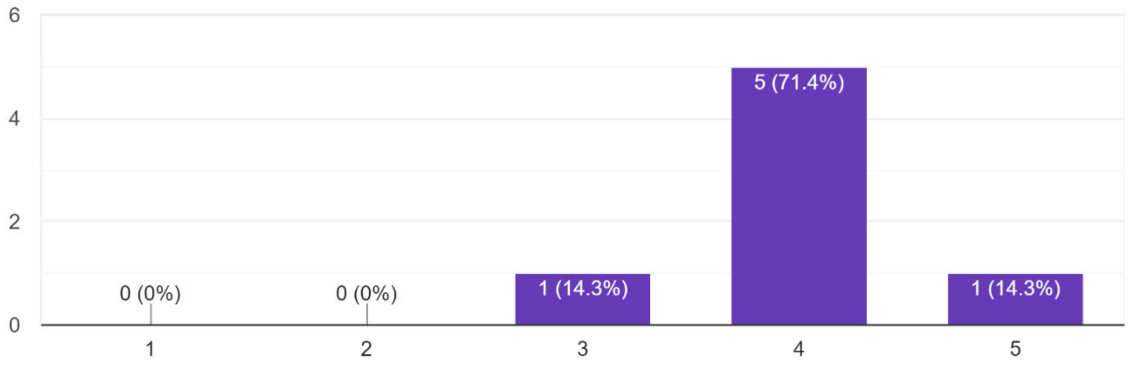
9. Breach

What happens after a data breach? Who is notified? Do you maintain an internal breach register? Possibility of administration fines.

Appendix 3: Questionnaire Scores

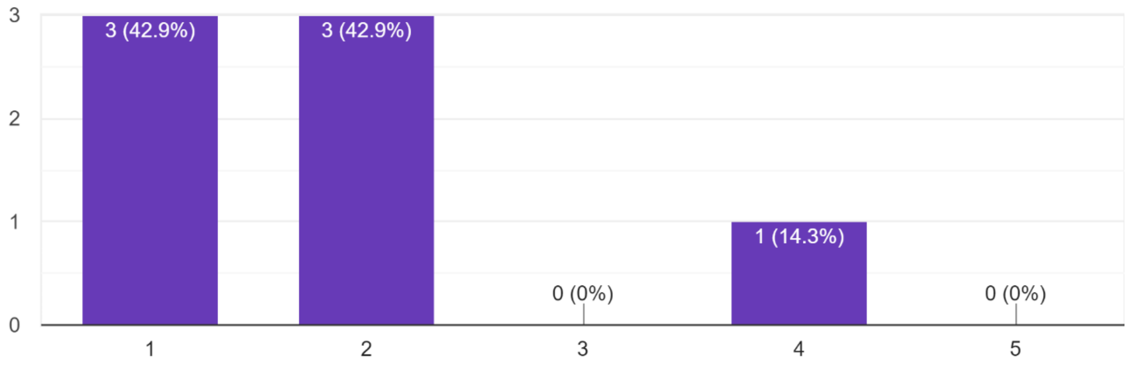
1. I think that I would like to use this system frequently.

7 responses



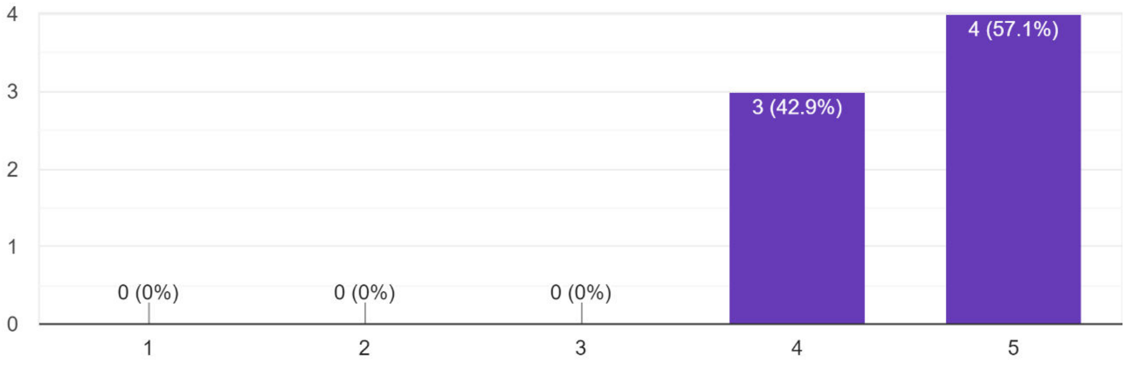
2. I found the system unnecessarily complex.

7 responses



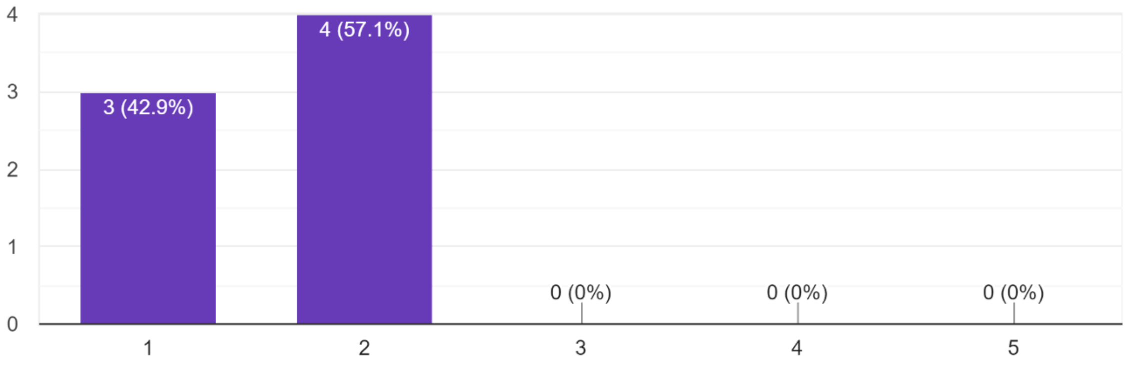
3. I thought the system was easy to use.

7 responses



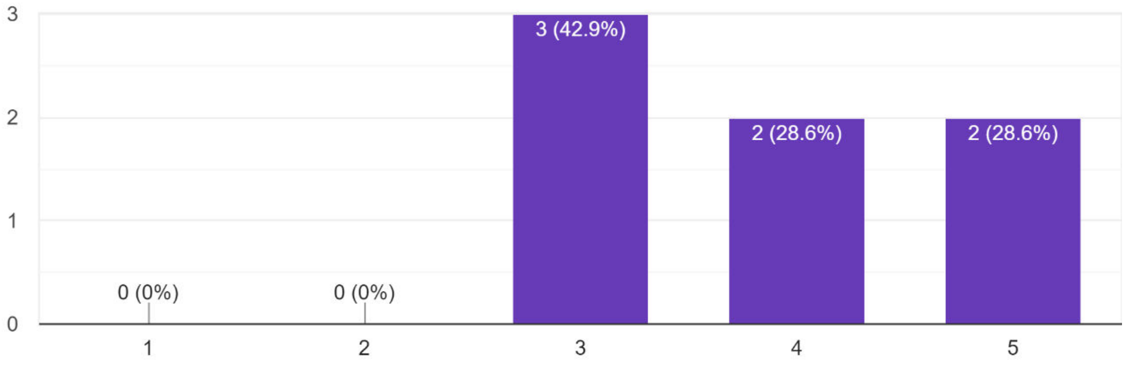
4. I think that I would need the support of a technical person to be able to use this system.

7 responses



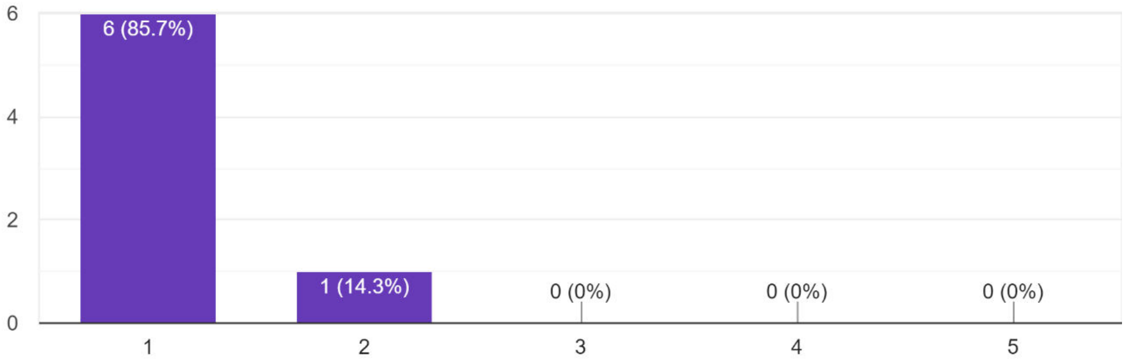
5. I found the various functions in this system were well integrated.

7 responses



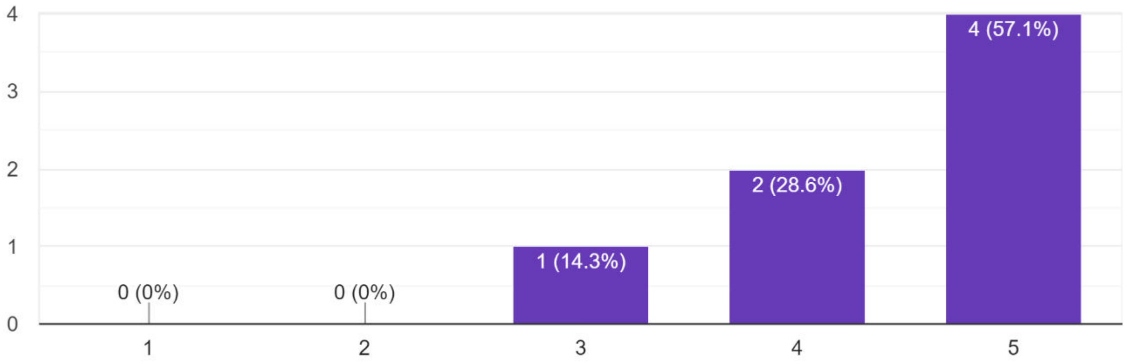
6. I thought there was too much inconsistency in this system.

7 responses



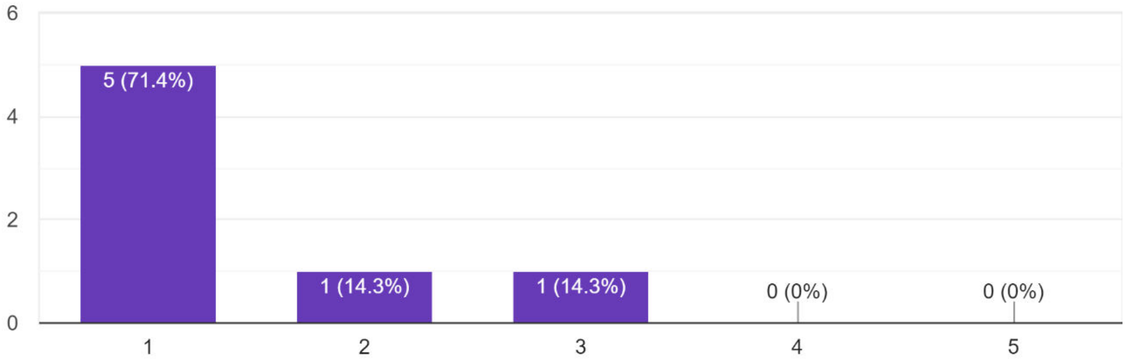
7. I would imagine that most people would learn to use this system very quickly.

7 responses



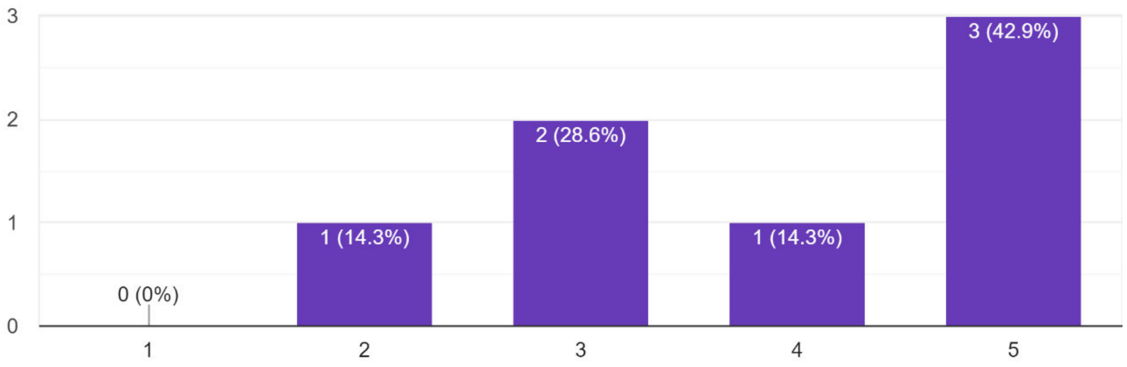
8. I found the system very cumbersome to use.

7 responses



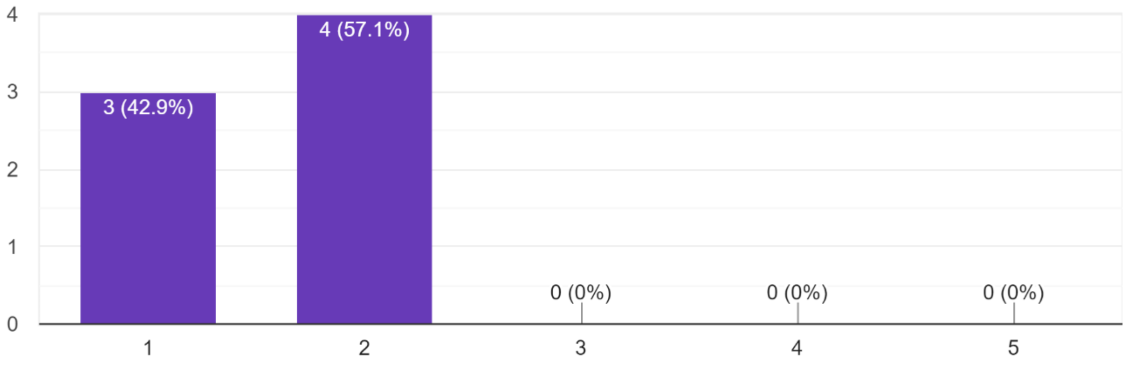
9. I felt very confident using the system.

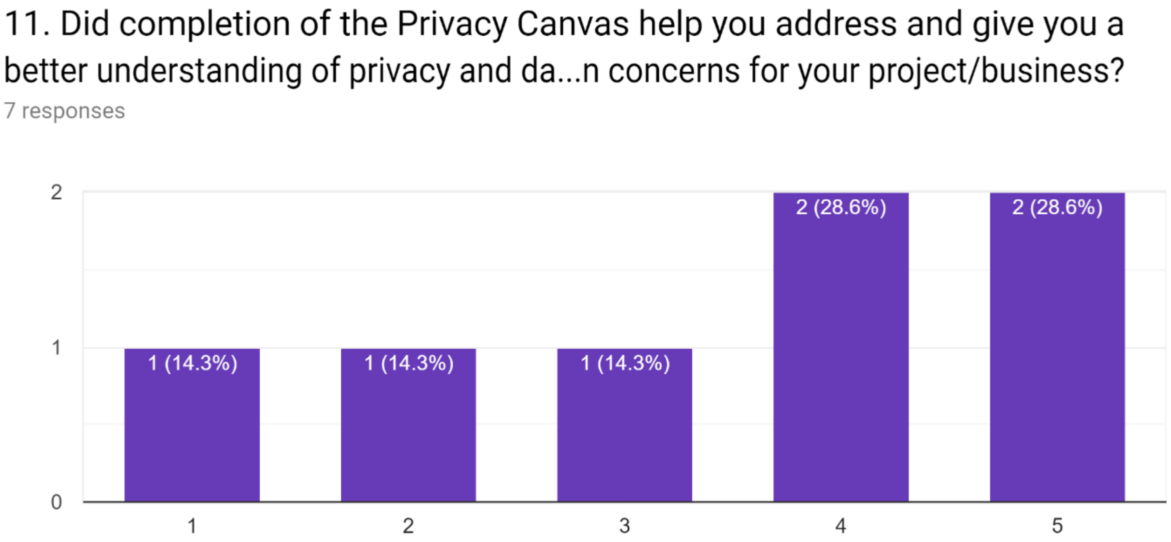
7 responses



10. I needed to learn a lot of things before I could get going with this system.

7 responses



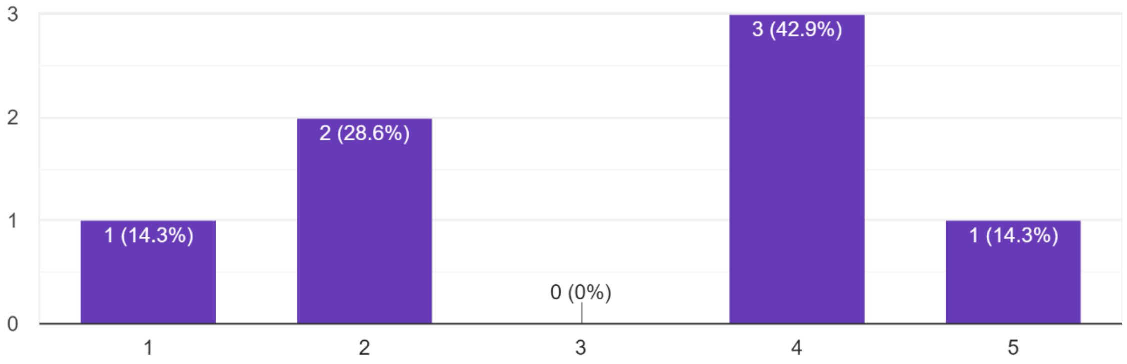


11. Did completion of the Privacy Canvas help you address and give you a better understanding of privacy and da...n concerns for your project/business?

7 responses

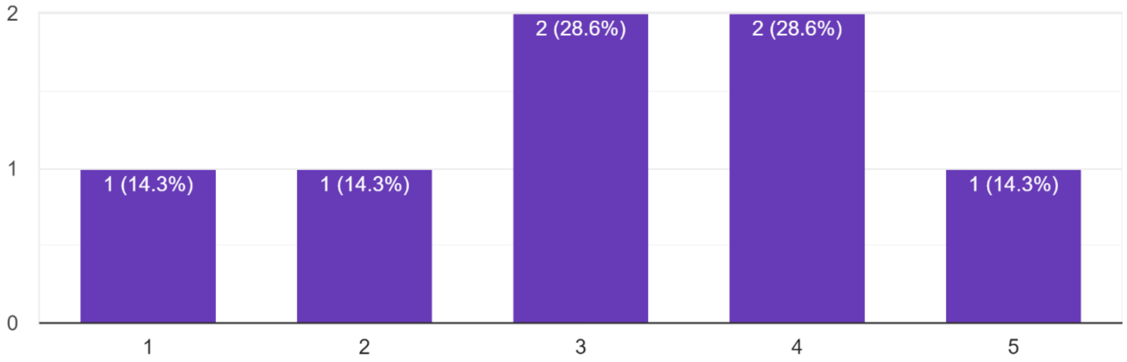
12. Do you think that it is helpful to complete a Privacy Canvas alongside a Business Model Canvas?

7 responses



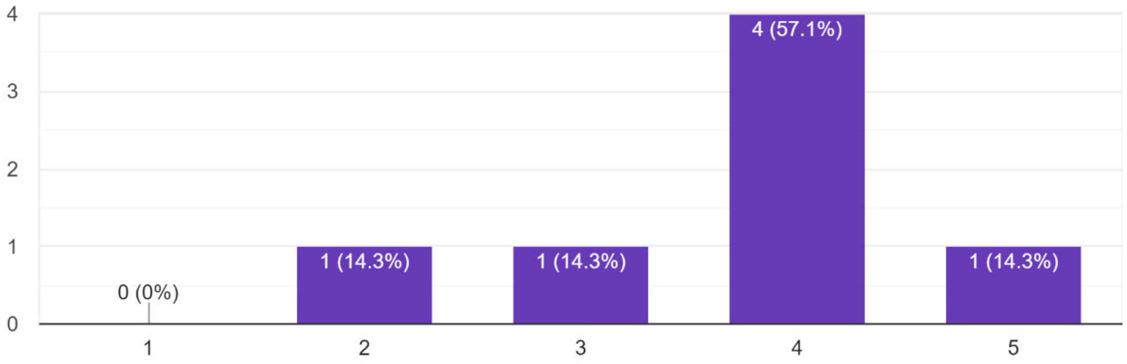
13. The privacy and data protection concern for my project/business were not applicable to the Privacy Canvas?

7 responses



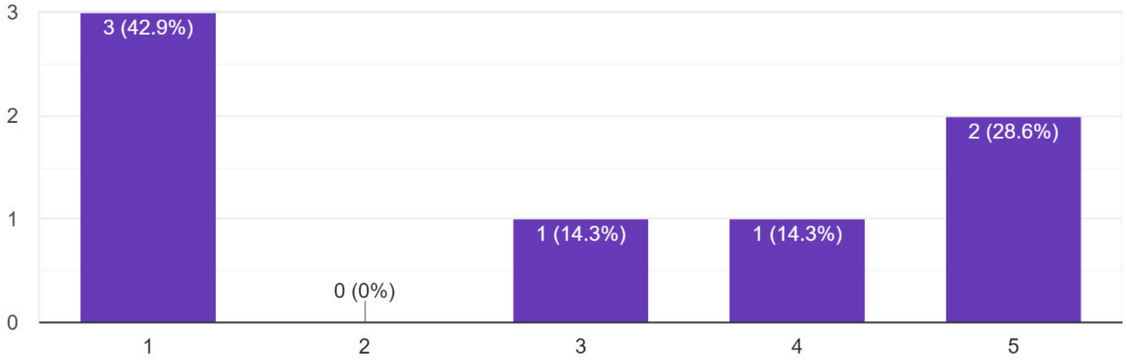
14. The Privacy Canvas helped identify privacy or data concerns that were not previously thought about.

7 responses



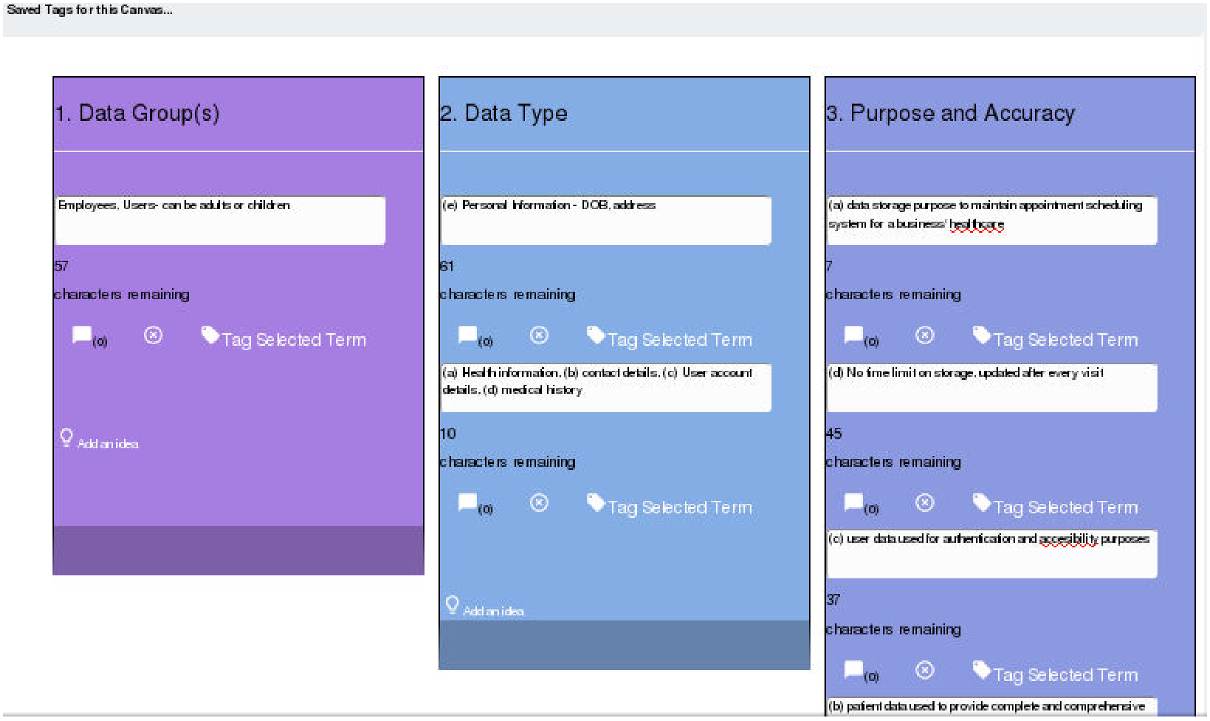
15. The Privacy Canvas would be a useful tool in the project/business innovation process?

7 responses



Appendix 4: Privacy Canvases

Canvas 1



Saved Tags for this Canvas...

1. Data Group(s)

Employees, Users- can be adults or children

57

characters remaining

2. Data Type

(e) Personal Information - DOB, address

61

characters remaining

(a) Health information, (b) contact details, (c) User account details, (d) medical history

10

characters remaining

3. Purpose and Accuracy

(a) data storage purpose to maintain appointment scheduling system for a business/ healthcare

7

characters remaining

(d) No time limit on storage, updated after every visit

45

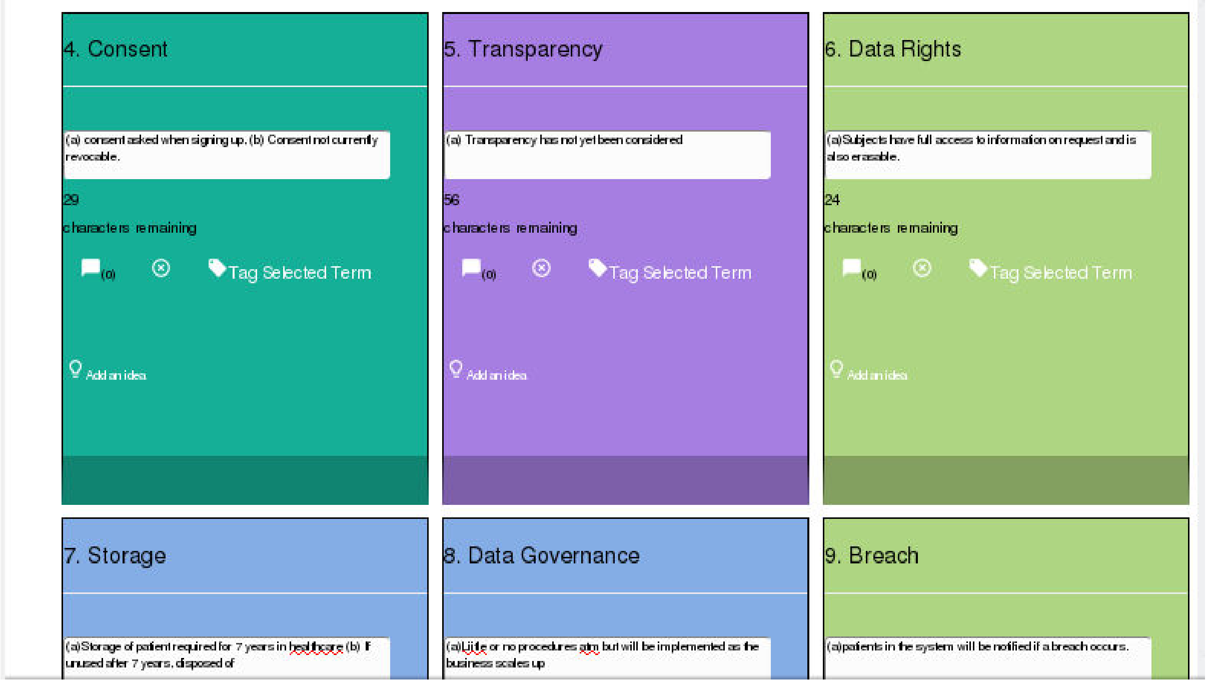
characters remaining

(c) user data used for authentication and accesibility purposes

37

characters remaining

(b) patient data used to provide complete and comprehensive



4. Consent

(a) consent asked when signing up, (b) Consent not currently revocable.

29

characters remaining

5. Transparency

(a) Transparency has not yet been considered

56

characters remaining

6. Data Rights

(a)Subjects have full access to information on request and is also erasable.

24

characters remaining

7. Storage

(a)Storage of patient required for 7 years in healthcare (b) If unused after 7 years, disposed of

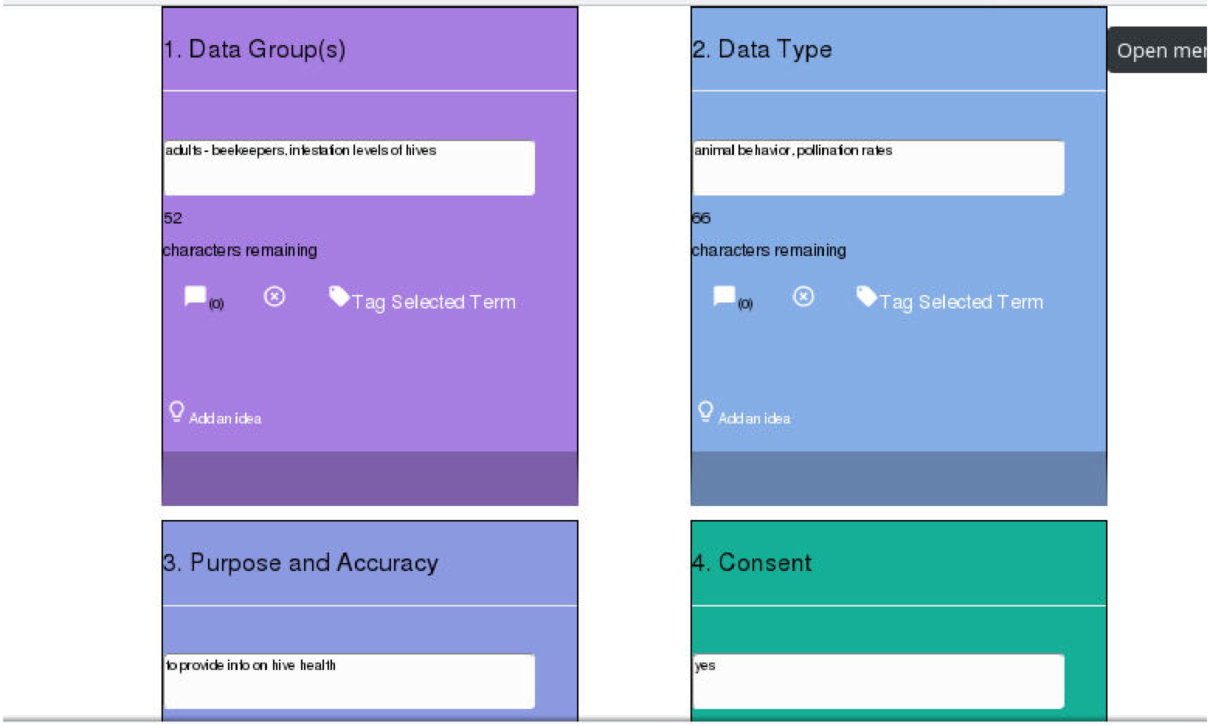
8. Data Governance

(a)Liitle or no procedures atm but will be implemented as the business scales up

9. Breach

(a)patients in the system will be notified if a breach occurs.

Canvas 2



1. Data Group(s)

adults - beekeepers, infestation levels of hives

52

characters remaining

2. Data Type

animal behavior, pollination rates

66

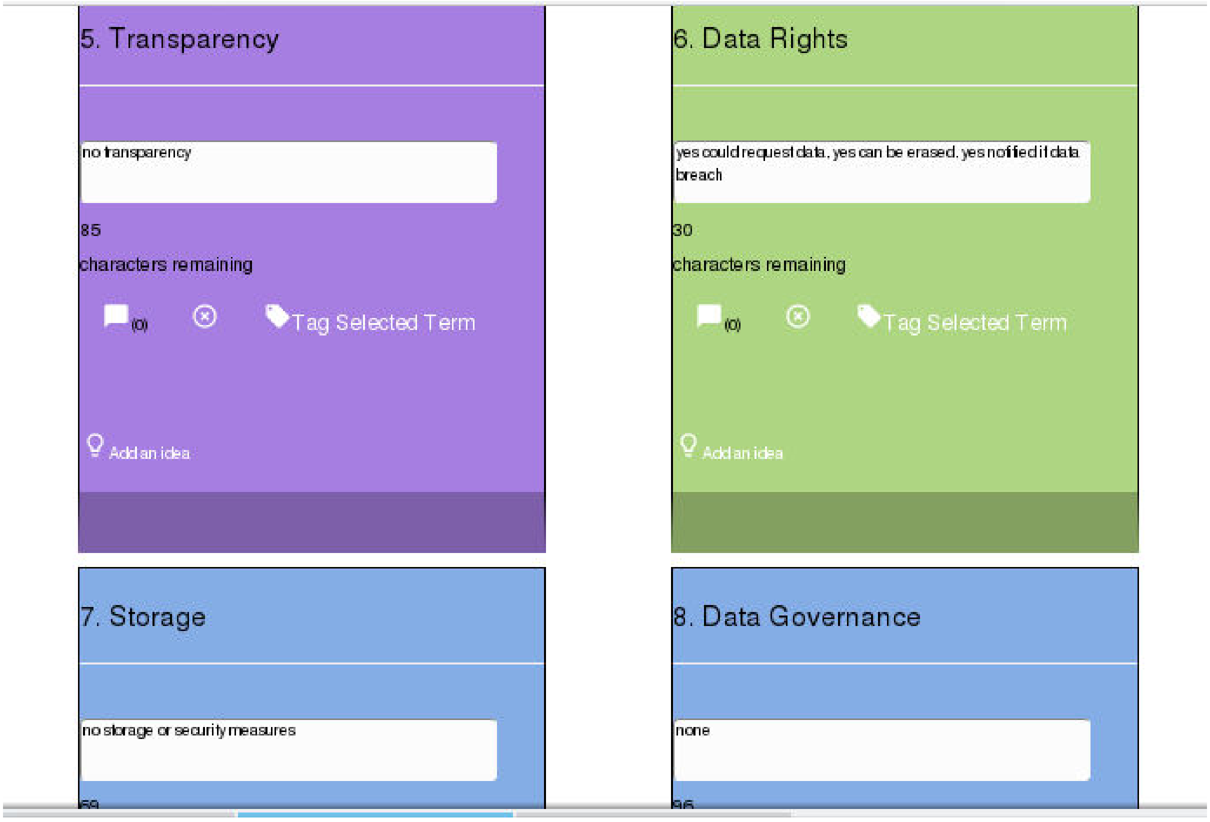
characters remaining

3. Purpose and Accuracy

to provide info on hive health

4. Consent

yes



5. Transparency

no transparency

85

characters remaining

6. Data Rights

yes could request data, yes can be erased, yes notified if data breach

30

characters remaining

7. Storage

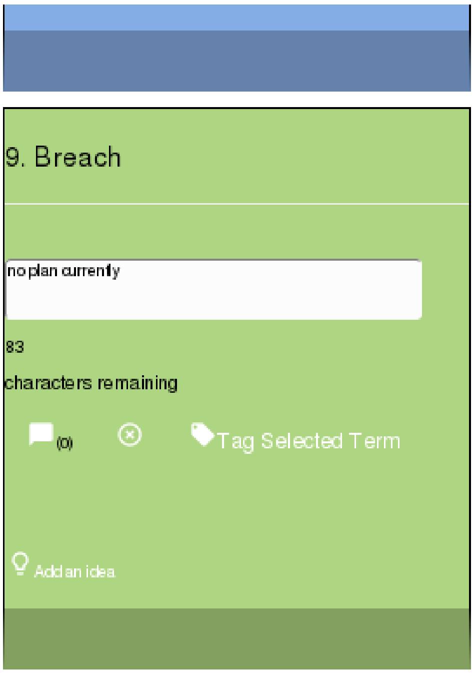
no storage or security measures

69

8. Data Governance

none

96

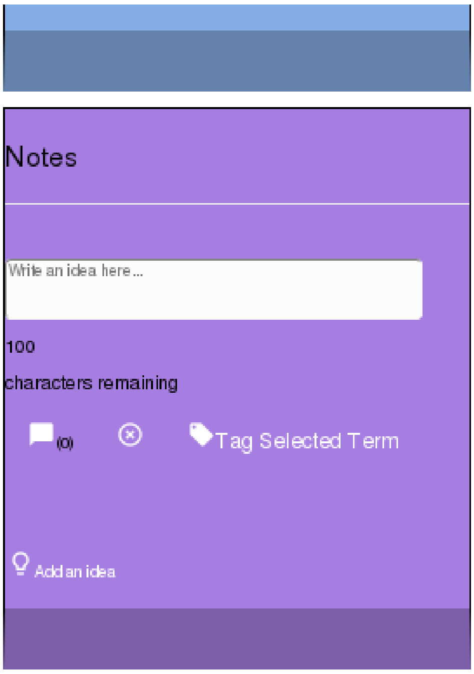


9. Breach

no plan currently

83

characters remaining



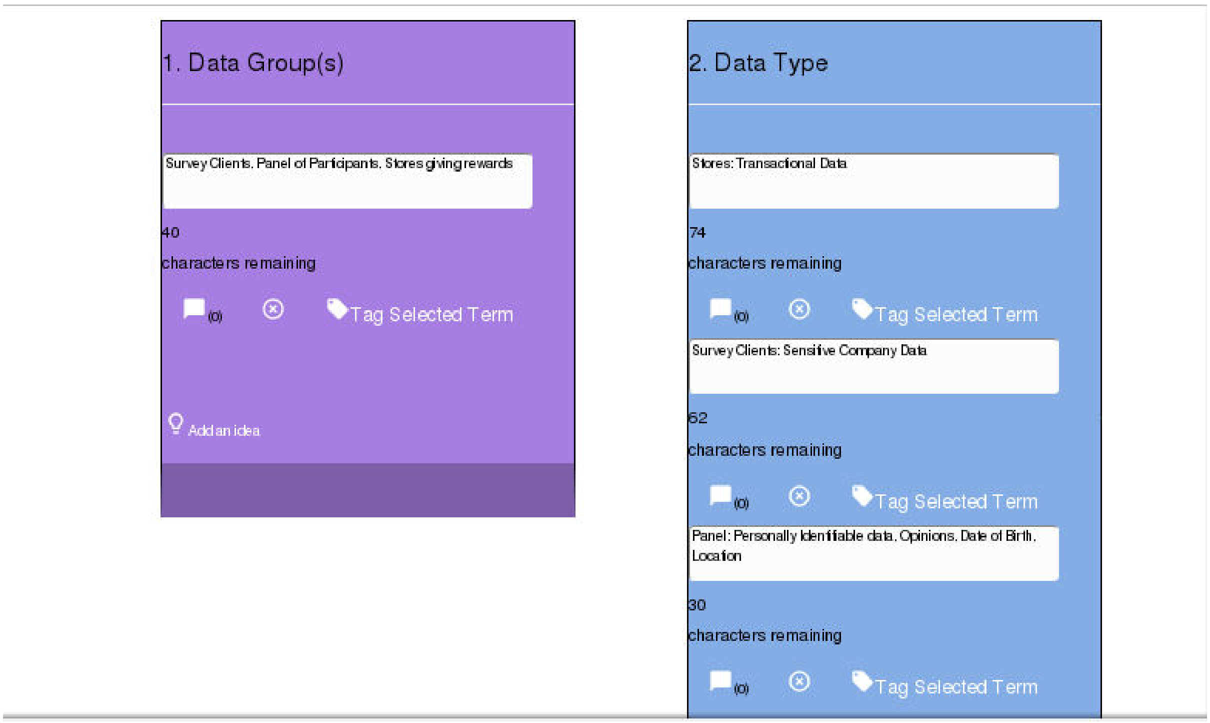
Notes

Write an idea here...

100

characters remaining

Canvas 3



1. Data Group(s)

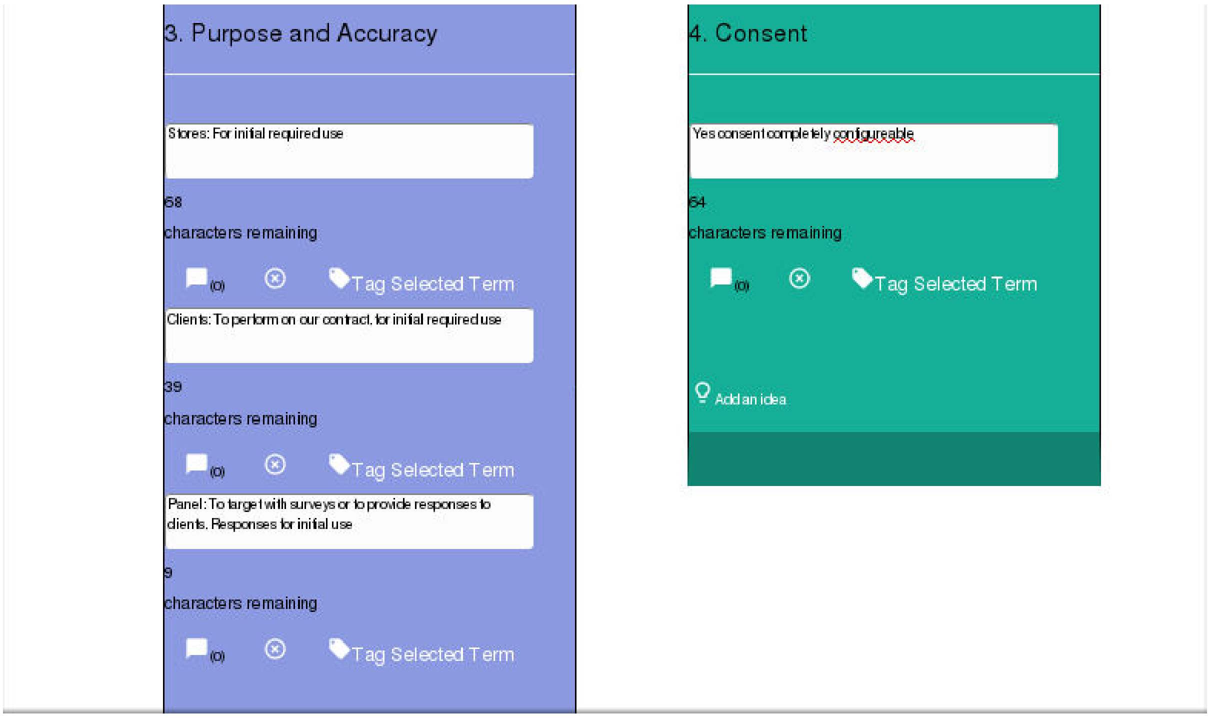
Survey Clients. Panel of Participants. Stores giving rewards

2. Data Type

Stores: Transactional Data

Survey Clients: Sensitive Company Data

Panel: Personally Identifiable data. Opinions. Date of Birth. Location



3. Purpose and Accuracy

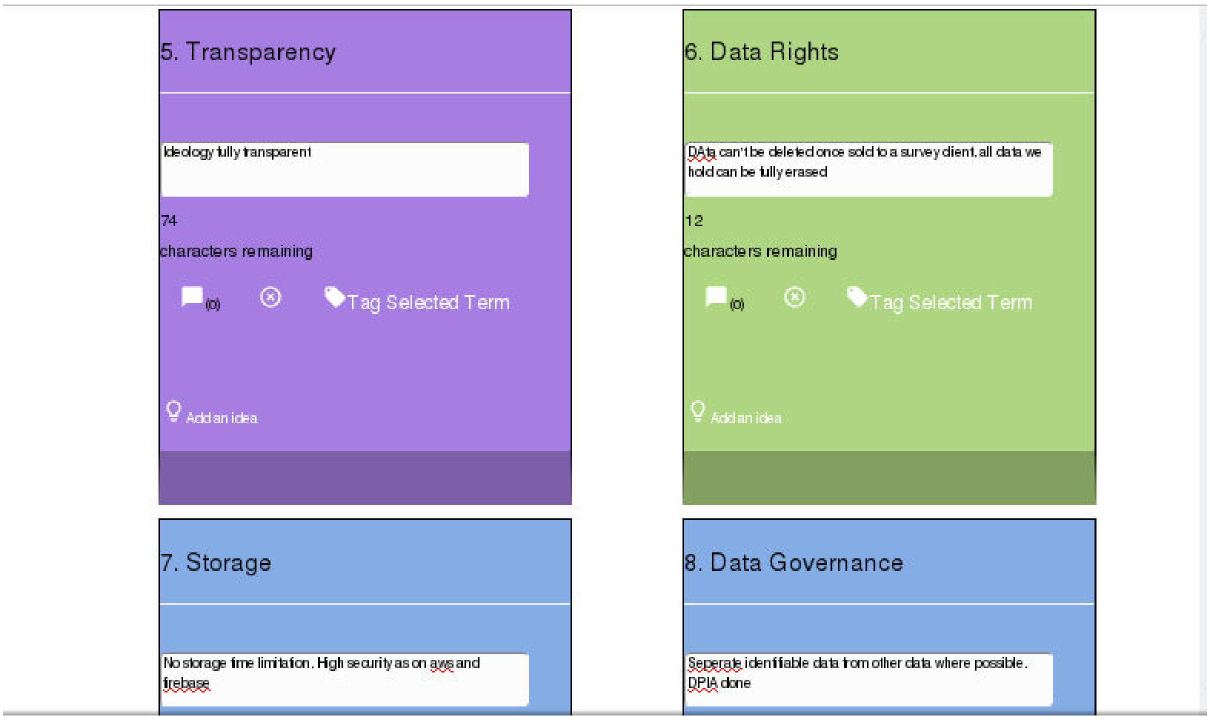
Stores: For initial required use

Clients: To perform on our contract, for initial required use

Panel: To target with surveys or to provide responses to clients. Responses for initial use

4. Consent

Yes consent completely configureable



5. Transparency

Ideology fully transparent

74

characters remaining

6. Data Rights

DAta can't be deleted once sold to a survey client, all data we hold can be fully erased

12

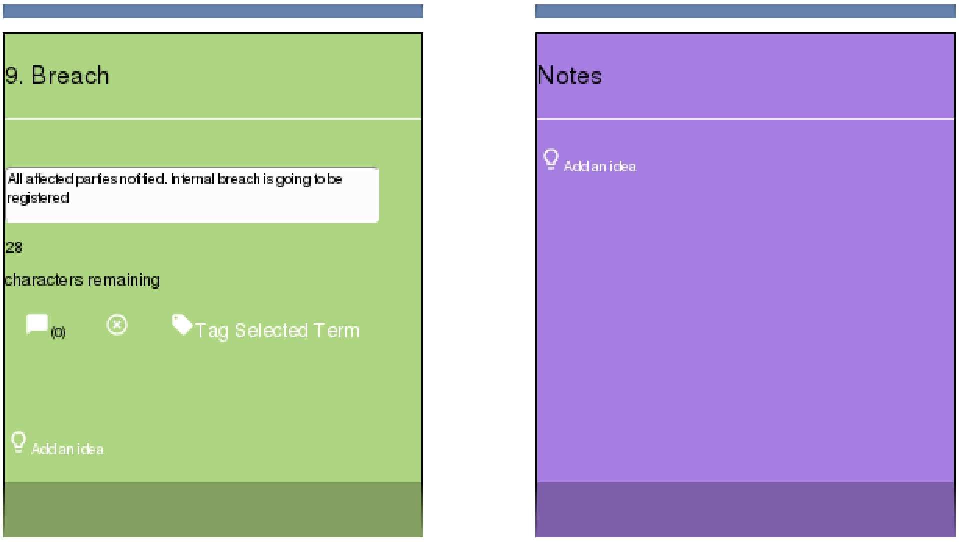
characters remaining

7. Storage

No storage time limitation. High security as on aws and firebase

8. Data Governance

Seperate identifiable data from other data where possible. DPIA done



9. Breach

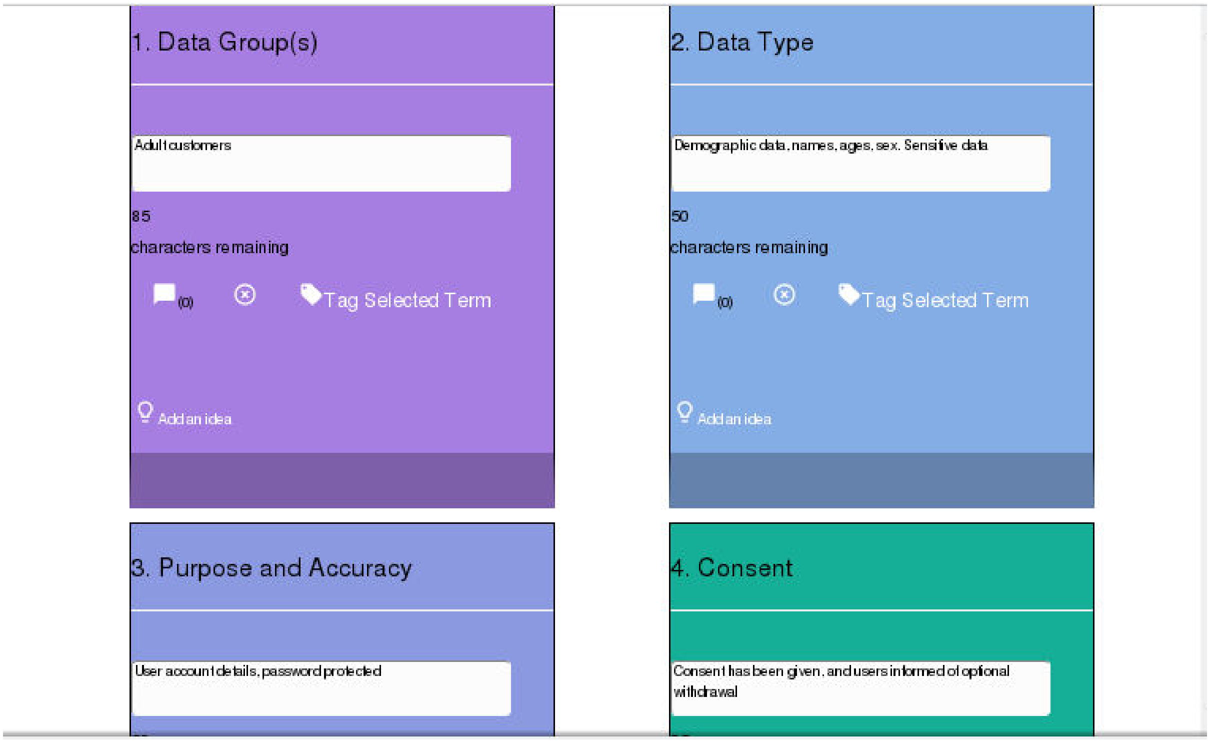
All affected parties notified. Internal breach is going to be registered

28

characters remaining

Notes

Canvas 4



1. Data Group(s)

Adult customers

85

characters remaining

2. Data Type

Demographic data, names, ages, sex. Sensitive data

50

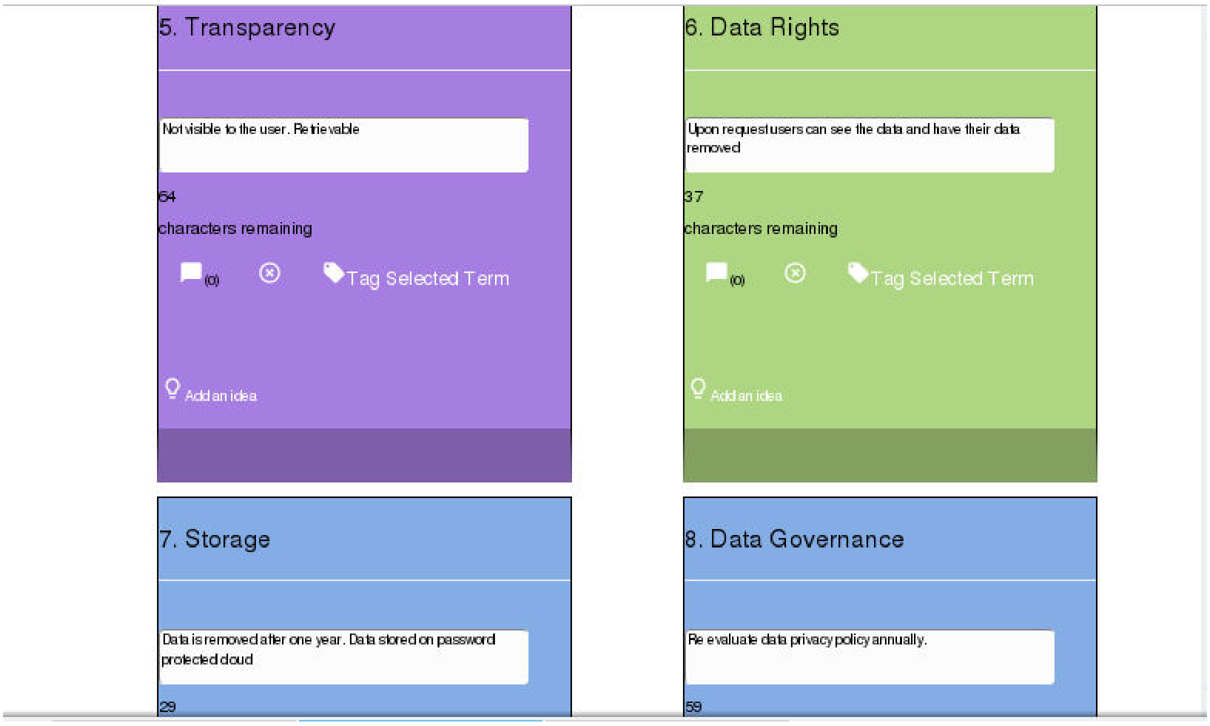
characters remaining

3. Purpose and Accuracy

User account details, password protected

4. Consent

Consent has been given, and users informed of optional withdrawal



5. Transparency

Not visible to the user. Retrievable

64

characters remaining

6. Data Rights

Upon request users can see the data and have their data removed

37

characters remaining

7. Storage

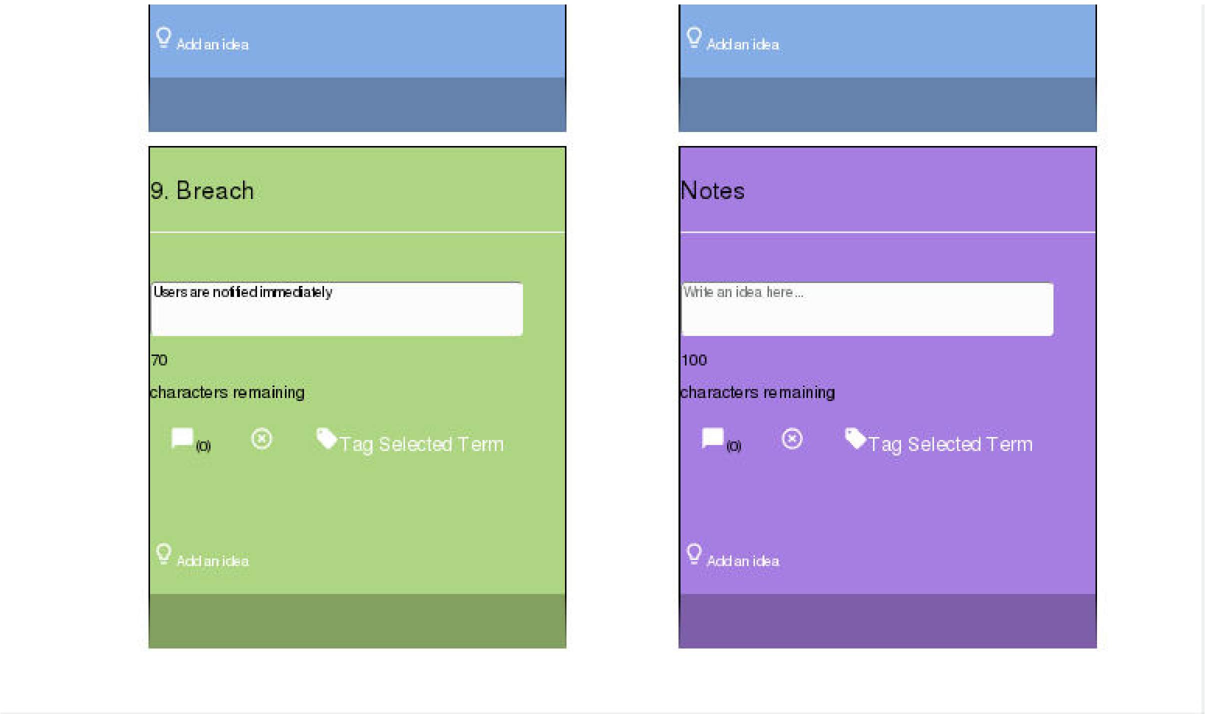
Data is removed after one year. Data stored on password protected cloud

29

8. Data Governance

Re evaluate data privacy policy annually.

59



9. Breach

Users are notified immediately

70

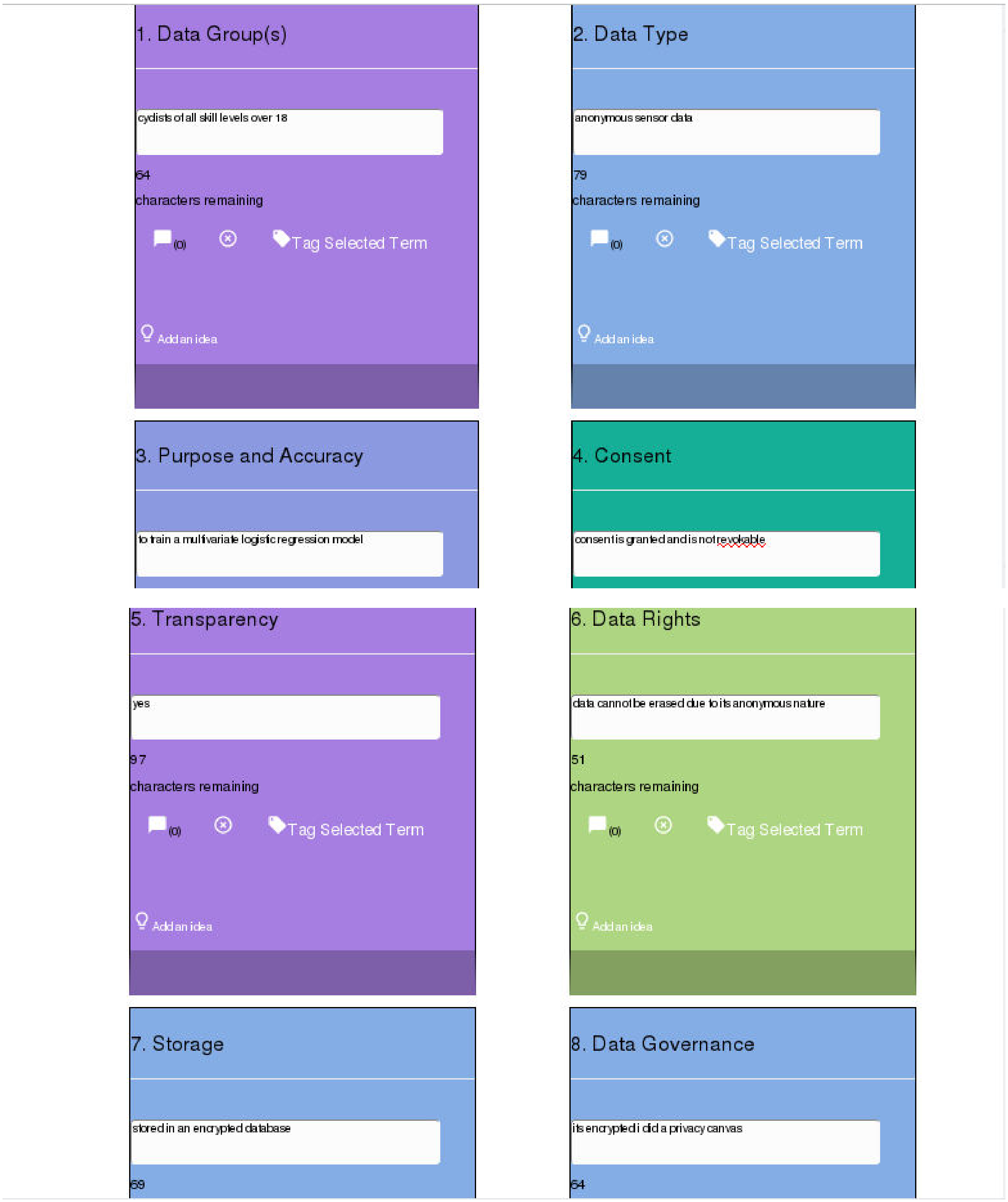
characters remaining

Notes

100

characters remaining

Canvas 5



1. Data Group(s)

cyclists of all skill levels over 18

64

characters remaining

2. Data Type

anonymous sensor data

79

characters remaining

3. Purpose and Accuracy

to train a multivariate logistic regression model

4. Consent

consent is granted and is not revokable

5. Transparency

yes

97

characters remaining

6. Data Rights

data cannot be erased due to its anonymous nature

51

characters remaining

7. Storage

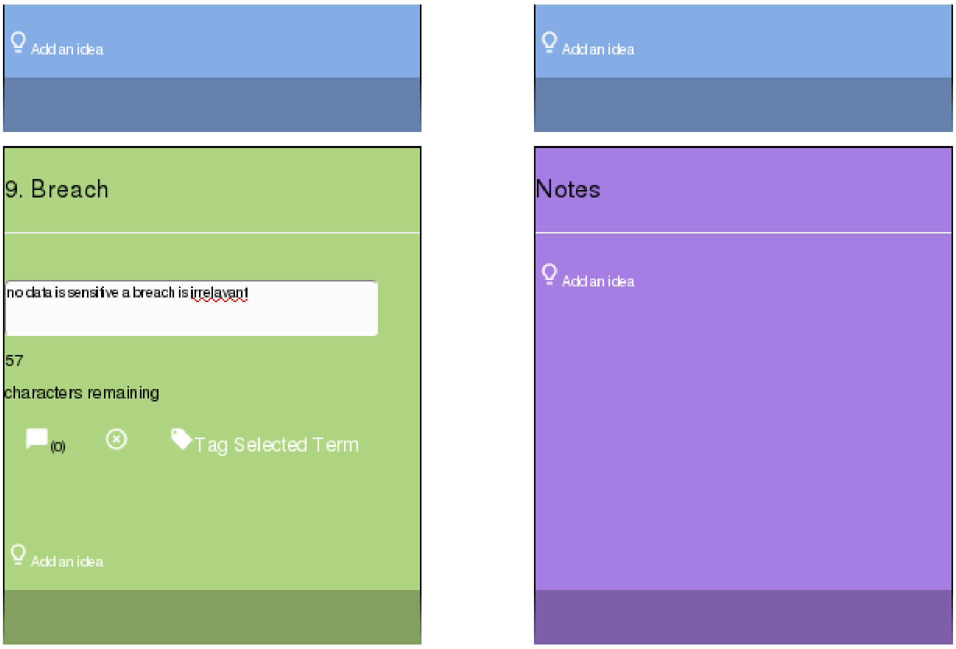
stored in an encrypted database

69

8. Data Governance

its encrypted i did a privacy canvas

64



9. Breach

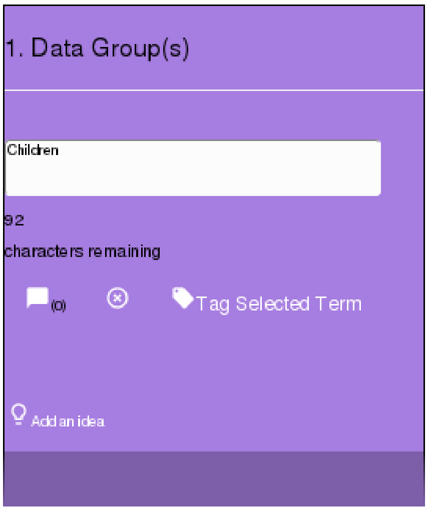
no data is sensitive a breach is irrelavant

57

characters remaining

Notes

Canvas 6

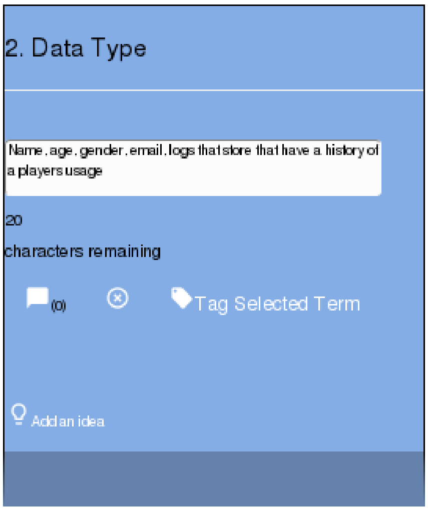


1. Data Group(s)

Children

92

characters remaining

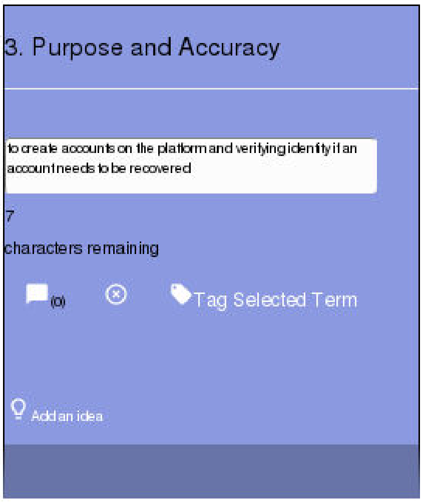


2. Data Type

Name . age . gender . email . logs that store that have a history of a players usage

20

characters remaining

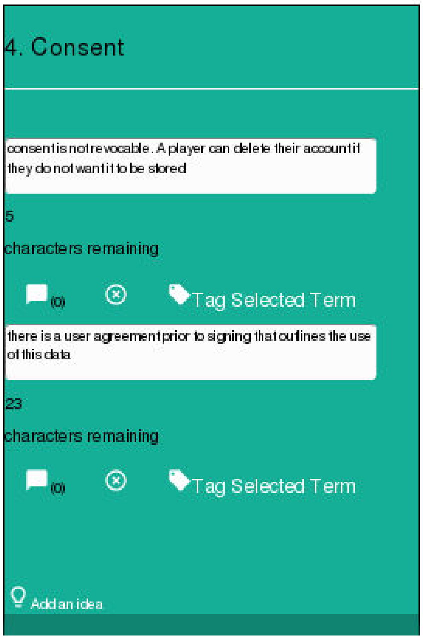


3. Purpose and Accuracy

to create accounts on the platform and verifying identity if an account needs to be recovered

7

characters remaining



4. Consent

consent is not revocable . A player can delete their account if they do not want it to be stored

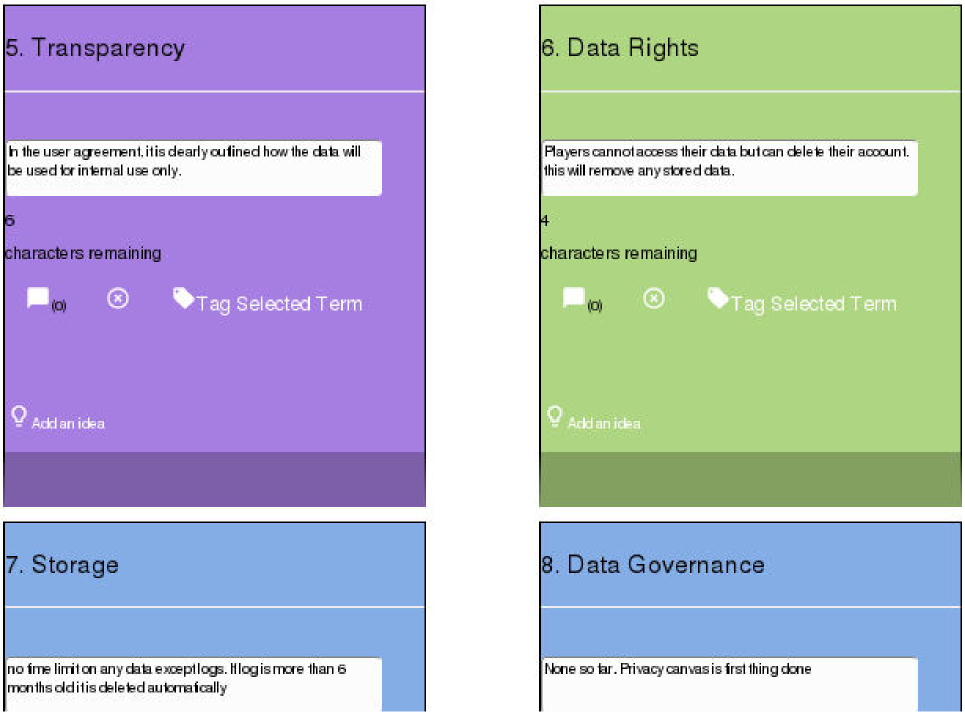
5

characters remaining

there is a user agreement prior to signing that outlines the use of this data

23

characters remaining



5. Transparency

In the user agreement, it is clearly outlined how the data will be used for internal use only.

6

characters remaining

6. Data Rights

Players cannot access their data but can delete their account. this will remove any stored data.

4

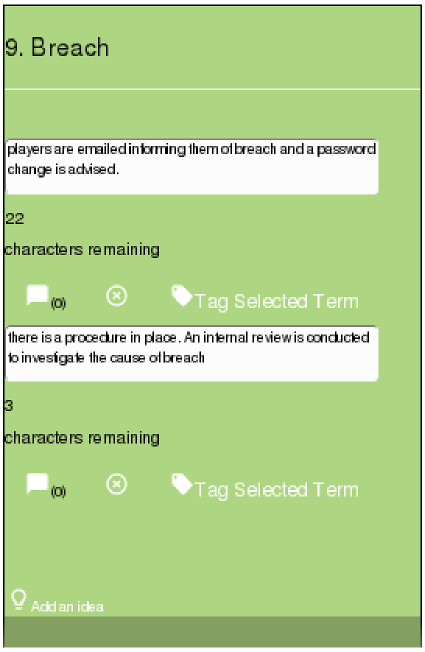
characters remaining

7. Storage

no time limit on any data except logs. If log is more than 6 months old it is deleted automatically

8. Data Governance

None so far. Privacy canvas is first thing done



9. Breach

players are emailed informing them of breach and a password change is advised.

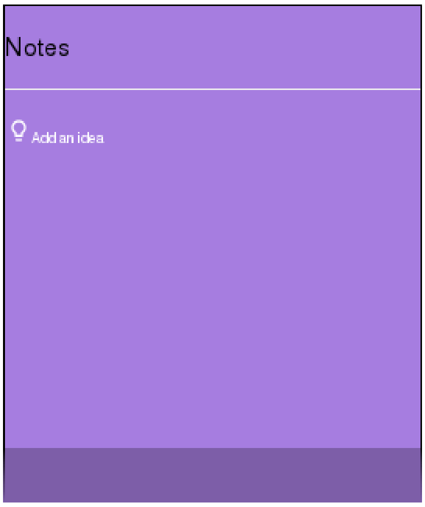
22

characters remaining

there is a procedure in place. An internal review is conducted to investigate the cause of breach

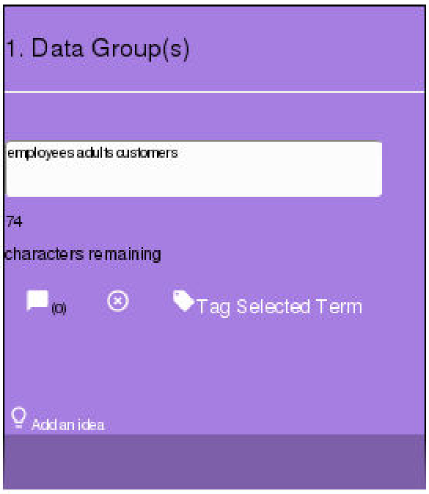
3

characters remaining



Notes

Canvas 7

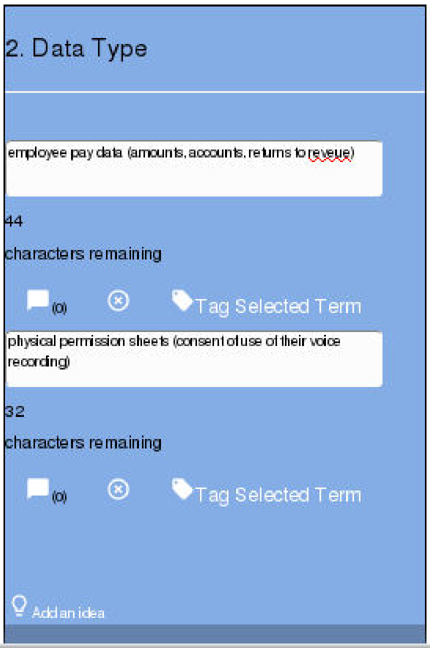


1. Data Group(s)

employees adults customers

74

characters remaining



2. Data Type

employee pay data (amounts, accounts, returns to reveue)

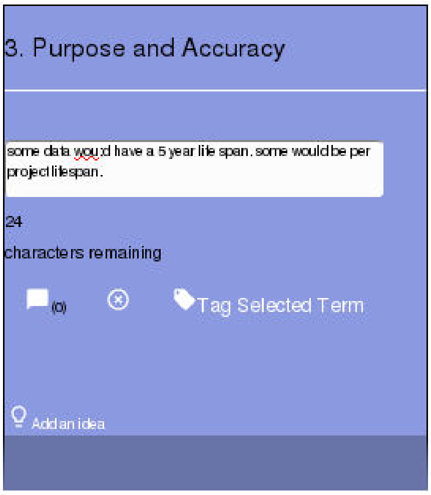
44

characters remaining

physical permission sheets (consent of use of their voice recording)

32

characters remaining

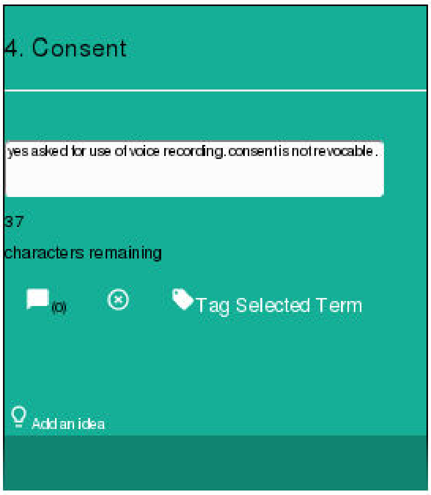


3. Purpose and Accuracy

some data woud have a 5 year life span. some would be per project lifespan.

24

characters remaining

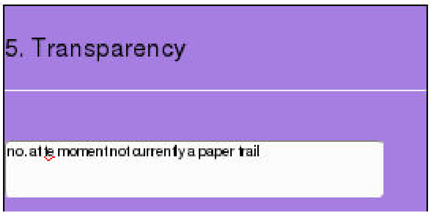


4. Consent

yes asked for use of voice recording. consent is not revocable.

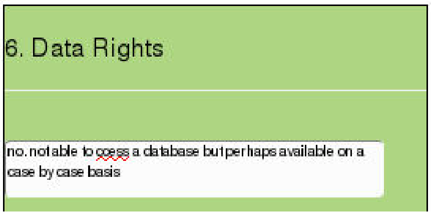
37

characters remaining



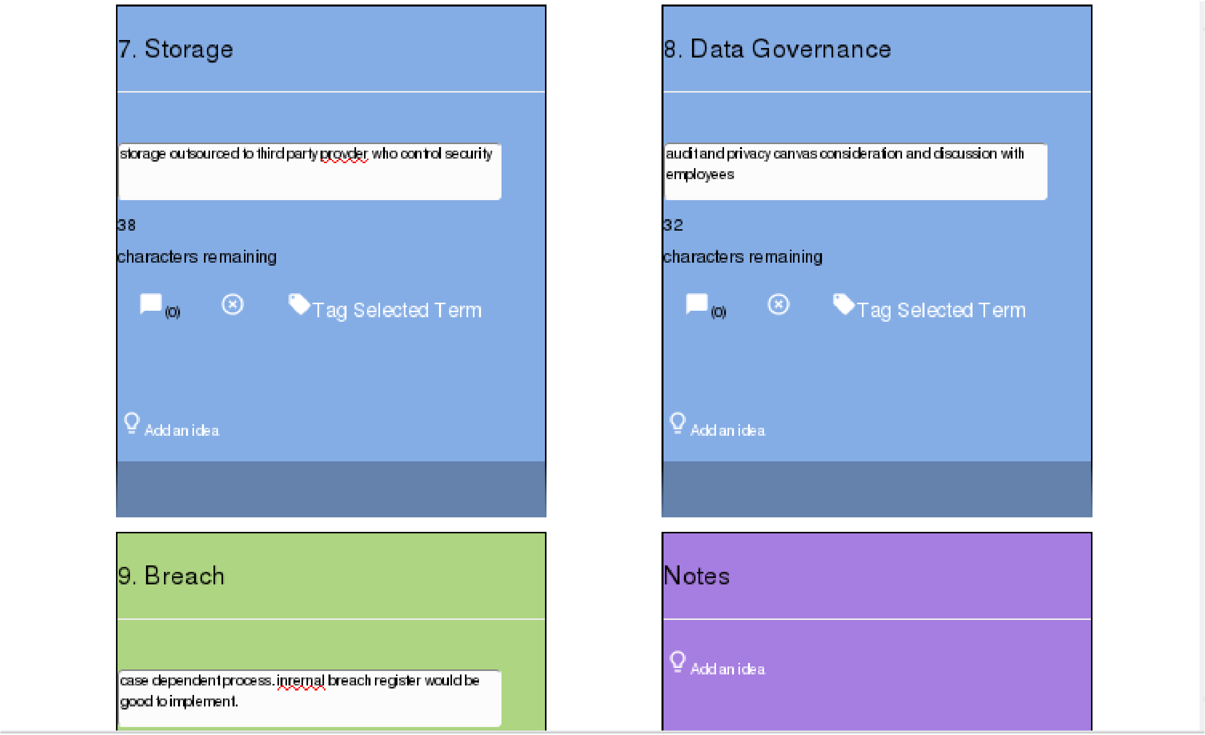
5. Transparency

no. at je moment not currently a paper trail



6. Data Rights

no. not able to ccess a database but perhaps available on a case by case basis



7. Storage

storage outsourced to third party provder who control security

38

characters remaining

8. Data Governance

audit and privacy canvas consideration and discussion with employees

32

characters remaining

9. Breach

case dependent process. inrernal breach register would be good to implement.

Notes

Bibliography

PETs controls matrix - A systematic approach for assessing online and mobile privacy tools. (2019). [online] Available at: https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools [Accessed 28 Mar. 2019].

Itgovernance.co.uk. (2019). *GDPR Penalties and Fines | IT Governance UK*. [online] Available at: https://www.itgovernance.co.uk/dpa-and-gdpr-penalties [Accessed 28 Mar. 2019].

Osterwalder, A., & Pigneur, Y. (2010). Business Model Generation. Hoboken, NJ: Wiley.

Lewis, D., Reijers, W., & Pandit, H. (2018). Discussing Ethical Impacts in Research and Innovation: The Ethics Canvas. IFIP TC9 Human Choice and Computers Conference (in press).

Boardman, R., Mullock, J. and Mole, A. (2017). [online] Twobirds.com. Available at: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en [Accessed 30 Mar. 2019].

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y. and Bourka, A. (2016). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. *ENISA*. [online] Available at: https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools [Accessed 1 Apr. 2019].

Ethicscanvas.org. (2017). *The Ethics Canvas*. [online] Available at: https://www.ethicscanvas.org/ [Accessed 4 Apr. 2019].

General Data Protection Regulation (GDPR). (2016). *Art. 35 GDPR – Data protection impact assessment | General Data Protection Regulation (GDPR)*. [online] Available at: https://gdpr-info.eu/art-35-gdpr/ [Accessed 7 Apr. 2019].

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H. and Rost, M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. *Privacy Technologies and Policy*.

The Eight Principles of Data Protection | Data Protection Commission. (2019). *The Eight Principles of Data Protection | Data Protection Commission*. [online] Available at: https://www.dataprotection.ie/en/individuals/eight-principles-data-protection [Accessed 9 Apr. 2019].

Additional materials

A CD is attached to this report containing the code used for the virtual Privacy Canvas implementation.