

## **A Consent and Privacy Management Framework**

Petteri Kalaoja

Master's Thesis  
Degree Programme in  
Leading Business Transformation  
2022



<b>Author</b> Petteri Kalaoja	
<b>Degree Programme</b> Leading Business Transformation, Master's Degree	
<b>Thesis Title</b> A Consent and Privacy Management Framework	<b>Number of pages + appendix pages</b> 56 + 47
<p>The change drivers in customer behaviour, tightening privacy regulation around the globe and evolving privacy technology is changing how people value and give consent to use their data. This has both short and long-term impacts, especially for businesses that have been used to utilising consumer data very freely.</p> <p>This thesis investigates different factors that must be considered when approaching such a large and complex environment of change drivers. The work includes a categorisation of themes and relevant topics where an organisation can choose the correct elements when building an iterative privacy strategy. The research also analyses new privacy-related technology needed to comply with the regulation.</p> <p>Research findings from the questionnaire and interviews gained insight into how people value their privacy and how they compare this against how they act in practice. The conclusion is that a majority of people are concerned about how their personal data is used, and they want to be in control of that, but their actions are contradictory. People expect companies to apply transparency, fairness and a customer-first approach when designing the consent process, no matter if the user is declining or giving consent. These findings align with other similar studies. Another finding was that users experience consent fatigue when they are forced to react to consent banners almost on any service they access, mainly because most of these banners are designed differently. Even though legislation directs how consent must be acquired, there are no standards currently that would make the consent process quick and user-friendly. An outcome of the study was customer-centric prototypes of consent banners that build trust in users.</p> <p>The outcome of the thesis presents a framework to build and manage consent and privacy in a complex and rapidly changing environment. It applies a customer-centric approach to design services that are based on trust and transparency.</p>	
<b>Keywords:</b> Consent Management, privacy, ePrivacy, PrivacyTech, transparency, customer data, regulation, privacy paradox	

# Table of contents

<i>Abbreviations and terms</i> .....	1
<b>1 Introduction</b> .....	<b>2</b>
1.1 <i>Objectives</i> .....	3
1.2 <i>Research questions</i> .....	4
1.3 <i>Scope</i> .....	5
<b>2 What are the change drivers around consent and data privacy?</b> .....	<b>6</b>
2.1 <i>Privacy history</i> .....	6
2.1.1 <i>Analogical</i> .....	6
2.1.2 <i>Digital</i> .....	7
2.2 <i>Key drivers for change in privacy management</i> .....	7
2.3 <i>Ethical and transparent data</i> .....	8
2.3.1 <i>The privacy challenge</i> .....	8
2.3.2 <i>Corporate data responsibility</i> .....	10
2.3.3 <i>Complexity with interconnected data</i> .....	10
2.3.4 <i>Data as a human right</i> .....	11
2.3.5 <i>The privacy paradox</i> .....	11
2.4 <i>Data governance and privacy focused frameworks</i> .....	12
2.5 <i>Transparent consent design</i> .....	13
2.5.1 <i>Deceptive design</i> .....	13
2.6 <i>Data and privacy initiatives in the EU</i> .....	14
2.6.1 <i>The need for regulation</i> .....	14
2.7 <i>Regulation</i> .....	14
2.7.1 <i>GDRP - General Data Protection Regulation</i> .....	15
2.7.2 <i>ePrivacy directive and regulation</i> .....	15
2.7.3 <i>DSA – Digital Services Act</i> .....	15
2.7.4 <i>DMA – Digital Markets Act</i> .....	16
2.8 <i>Technology</i> .....	16
2.8.1 <i>A description of relevant technology</i> .....	16
2.8.2 <i>The rise of privacy technology</i> .....	20
2.8.3 <i>A practical approach to Consent Management</i> .....	20
2.9 <i>Theory conclusion</i> .....	20
<b>3 Research plan</b> .....	<b>22</b>
3.1 <i>Methodology and approach</i> .....	22
3.1.1 <i>Constructive Research and design science research</i> .....	23
3.1.2 <i>Comparison and differences</i> .....	23
3.2 <i>Approach</i> .....	23

3.3	<i>Data collection and development process</i>	23
4	<i>Consent and privacy management framework</i>	25
4.1	<i>Privacy and consent toolkit</i>	26
4.1.1	<i>Legal, regulation and security</i>	27
4.1.2	<i>Technology &amp; data</i>	28
4.1.3	<i>Design, UX &amp; UI</i>	30
4.1.4	<i>Trust and ethics</i>	31
4.1.5	<i>Insight and trends</i>	32
4.1.6	<i>Business, processes and strategy</i>	32
	<i>Business impact assessment</i>	34
4.2	<i>Technology architecture</i>	34
4.2.1	<i>Customer controlled data</i>	35
4.2.2	<i>Digital identity and Consent Management</i>	35
4.2.3	<i>Unified customer data omni-channel orchestration and activation</i>	36
4.2.4	<i>Technology architecture – Customer Data &amp; PrivacyTech</i>	36
4.3	<i>Consent design &amp; research</i>	38
4.3.1	<i>Service design and the Double Diamond process</i>	39
4.3.2	<i>The research process</i>	39
4.3.3	<i>Quantitative questionnaire</i>	40
4.3.4	<i>Findings</i>	40
4.3.5	<i>Conclusions</i>	42
4.3.6	<i>Qualitative research and design thinking process</i>	42
4.3.7	<i>Interviews</i>	43
4.3.8	<i>Wireframes and prototypes</i>	44
4.3.9	<i>Findings</i>	45
4.3.10	<i>Conclusions</i>	46
5	<i>Evaluation of research</i>	48
6	<i>Conclusion</i>	50
	<i>References</i>	52
	<i>Appendices</i>	57
	<i>Appendix 1: Questionnaire</i>	57
	<i>Appendix 2: Mindmap</i>	68
	<i>Appendix 3: Consent and privacy toolkit</i>	69
	<i>Appendix 4: Interviews</i>	70
	<i>Appendix 5: Prototyping</i>	92

## Abbreviations and terms

AdTech	Advertising Technology
CDP	Customer Data Platform
CIAM	Customer Identity Access Management
CIPP	Certified Information Privacy Professional
CJO	Customer Journey Orchestration
CMP	Consent Management Platform
CRA	Constructive Research Approach
CRM	Customer Relationship Management
DMA	Digital Markets Act
DPO	Data Protection Officer
DSA	Digital Services Act
DSR	Design Science Research
IAB	The Interactive Advertising Bureau
ISMS	Information Security Management Systems
MAP	Marketing Automation Platform
MarTech	Marketing Technology
PbD	Privacy by Design
PET	Privacy Enhancing Technologies
PII	Personally Identifiable Information
PIMS	Privacy Information Management Systems
RegTech	Regulatory Technology
SSO	Single sign-on
TCF	Transparency and Consent Framework
UI	User Interface
UX	User Experience

# 1 Introduction

The importance and business impact of digital channels are growing strongly, as are the ever-increasing touch points where customers interact in various ways with companies and organisations. This change has been amplified by the changes in consumer behaviour after Covid-19.

Companies are investing or at least planning to invest in relevant technology that makes it possible to collect customer data and make that data actionable to provide personalised and relevant services aimed at the customers. Examples of this type of technology are traditionally Marketing Automation Platforms (MAP) and Customer Relationship Management (CRM) software. New technology and concepts are available on the market that makes it even easier to connect customer data from various back-end systems and customer touchpoints. This data can then be grouped into segments, and personalised content can be activated in different channels. A popular example of this kind of new technology is Customer Data Platforms (CDP).

To understand customer behaviour and serve them better in all the different channels and touchpoints, the use of customer data is becoming more important and necessary to provide a good customer experience and hence run a sustainably profitable business.

Customer expectations are growing regarding their personal data, and they expect that companies must give back something in exchange for the data in a valuable way, e.g., in terms of meaningful and personalised services, products and content that the customers want to use. However, several obstructions might prevent customers from giving companies permission to use their customer data because of several different factors. A huge driver of change is constantly tightening legislation that is rapidly changing how companies and organisations can utilise personal customer data. There is also a change in customer behaviour where they are becoming more aware of privacy issues concerning their data. Big technology players such as Google, Meta, Amazon and Apple are reacting by self-regulating themselves, mostly due to the tightening regulations around the world, which is necessary for them to keep up with the changing privacy landscape. Also, technology such as web browsers with cookie and ad-blockers have gained popularity already for years and is already a standard feature in many browsers. Besides worldwide legislative actions, the near approaching end of the 3rd party cookie usage drives companies to focus more on 1st party data to offer personalised services and offerings to their customers. In practice, this means a shift in focus towards using and leaning more on data collected from companies' own channels and straight from the customers instead of relying on data from third party advertising providers.

Despite all the changes in the personal data environment, consumers do not seem to care nor especially understand what they are signing up for when they agree to the terms and conditions of companies that want to use their data. All of that is changing due to the change drivers mentioned in the previous chapter. Since companies will depend more on 1st party consumer data in the near future, they have to ensure the means how to get permission to use personal data. This requires a more transparent way of designing how consent information is displayed and explained in a short, concise, and especially trustworthy way.

This thesis aims to research the different factors needed to tackle these challenges and provide a plan and framework to help companies understand the different needs and build their privacy data and technology-related roadmap.

The result of this thesis is to provide a framework around privacy and consent to help customers and companies to understand how to build their privacy-related data and technology roadmap.

## **1.1 Objectives**

At Dagmar, we are helping our clients to solve various needs around digital business. Due to the changes mentioned earlier, we have noticed that the clients are confronted with a new, complex and rapidly changing environment around customer data where they need help navigating. It has become clear that in such a challenging environment, there is a strong need to understand different interconnected elements that must be addressed and taken into careful consideration to ensure short-term and long-term business objectives.

The objective of this research is to investigate the emerging digital consent and privacy domain and the different elements that are a part of it and to understand where we have come from and what the status is today, and where we are going in the near future and how to prepare for that, especially in a fast-changing environment. We are looking into the different drivers behind the change, such as regulation, technology and change in consumer behaviour.

The research aims to determine and understand what the customers think about consent and privacy. In addition, different designs, layouts, and ways of presenting the consent to the user will be studied. An evaluation of tools and technology will be part of the research to understand the technology needed to execute customer data and consent management in the different multichannel touch points. Technology is essential in handling and presenting transparently to the customers what for and how their data is used.

This field is very complex and is evolving at a very rapid pace. Instead of entirely focusing on one snapshot topic around consent and privacy, which quite likely would be partly outdated within a few years, the research aims to understand and find the factors that are significant for the long-term planning of a future-proof consent and privacy approach. It is essential to understand what is changing in this domain and constantly monitor and react to those changes.

Another objective of the research is to give insight into customer behaviour regarding customers giving consent to use their data. To achieve this, we must understand how customers need to decide whether to give consent or not. Besides understanding customer behaviour and how it changes, we must also understand the regulations directing what is allowed and what is not. Also, the technology and tools must be evaluated to be future-proof. The environment around customer data is currently changing a lot. Therefore, we must understand towards which direction these different topics are going in the near future and try to make a future-proof plan.

The objective is also to look deeper into the different drivers that encourage customers to give consent, such as transparency, trustworthiness, brand image and trusted certifications when customers consider giving consent to use their data.

Besides consumers, this is a topic that significantly impacts the business and mainly the marketing and sales departments. Many other stakeholders are involved, such as the data & AI team, customer experience team and IT. If the customers give consent to use their personal data, marketing and sales can target and personalise content and offers based on that information, making targeted content more relevant for the customer. This brings savings in ad spending when the marketing costs are aimed at customers who have given their consent, their preferences are known, and those that do not fit the target group can be excluded. This consent-based customer data can be used in different departments to gain customer insight when developing new products. It also supports companies' long-term aim of providing the best customer experience in different customer touchpoints.

The purpose is to give any organisation an understanding of what concepts are needed and which tools to use when building a sustainable consent and privacy process.

## **1.2 Research questions**

With the research questions, the objective is to build a management framework for the needed elements to handle a modern privacy and consent strategy and understand customer behaviour when they give consent to companies to use their personal data. This should form insight into visually designing trustworthy consent management layouts from



the customer's perspective. Also, a suggestion for relevant technology and architecture to execute this is an objective.

- What are the required elements needed when implementing an iterative and long-term consent and privacy strategy?
- How do users value their privacy, and how do they behave when confronted with consent in web services?
- How should a consent banner be designed to build user trust and follow the demand of regulation?
- What technologies and what kind of architecture is required to achieve this?

### **1.3 Scope**

The scope and framing of this work were carefully evaluated to meet the current needs of Dagmar and its clients. The consent management and privacy field are developing rapidly without a clear understanding of how the future will turn out. There are still many elements around consent management and privacy that no one knows how they will form within the next few years. From that context, it is currently more helpful to look into what elements play an essential part in the whole and try categorising these into a meaningful framework. In other words, instead of focusing on one subject, the purpose is to understand the big picture opening up for businesses. To support the current and most urgent needs, a questionnaire, including interviews, will be conducted to understand how consent should be acquired today and in the near future.

An implementation of the technology is not a part of the thesis, only a high-level recommendation based on research in the current technological capability with a focus on consent management and privacy technology. It should also be a natural fit for most companies' current architecture.

Data security-related issues are not a part of this thesis. Even though data security is very closely related to ePrivacy, it is also a topic of its own and usually more of an IT topic than a topic for the business side, which is the main focus of this work. Data security is too large to be handled in this thesis and is therefore only mentioned but not covered.

In this work, when discussing regulation, we will focus mainly on EU privacy laws and regulations.

## **2 What are the change drivers around consent and data privacy?**

Behind all the governmental-driven privacy regulation that is going on globally and the changes in consumer behaviour and expectations, the main reason why we have come to these changes is because of privacy-related issues and concerns people have. Besides that, people around the world have seen what can happen if your personal digital data is used for intrusive purposes. It can be misused to target people with false content, as happened in the US elections in 2016. In authoritarian countries, it can be used to control people and to know details about people's personal lives that should not be anybody's business. Unnecessary data collected by companies is also a security risk if it might be leaked. These are big drivers of why people want to control what data they want to share and with whom.

Consumers are increasingly worried about the consequences of what might happen if critical data were stolen and used in a criminal manner, e.g., identity theft and even blackmail. We are also present online and communicating via online channels with digital profiles; if these are compromised, people risk losing their reputations and financial risks in case of fraud. Therefore, as consumers, we are more worried and aware of what data companies and organisations need to collect from them to provide their services. The question companies have to answer is what data is absolutely necessary to provide a specific product or service?

It is an iterative circle of various drivers pushing for these changes; the change in customer behaviour pushes for changes in regulation which pushes for changes in technology.

### **2.1 Privacy history**

To understand that privacy is not anything new but has, in fact, been around for hundreds of years from a legal perspective, I think it is relevant and interesting to have a quick look at the history of privacy to see how quickly it has developed and gotten very complicated within the past few years with digitalisation.

#### **2.1.1 Analogical**

- 1361 England's Justices of the Peace Act criminalizes "peeping Toms" and eavesdroppers.<sup>4</sup>
- 1792 US Congress passes a law enforcing the privacy of letters.
- 1858 Development of Privacy laws in France.
- 1890 US lawyers Samuel D. Warren and Louis Brandeis publish 'The Right to Privacy in the Harvard Law Review, prompting recognition of privacy as a legal right

- 1948 UN Declaration of Human Rights establishes the right to privacy. (Klasovec Kingsmill & Barday, 2021)
- In 1950, the right to privacy was part of the Human Rights European Convention on, that declares, “Everyone has the right to respect for his private and family life, his home and his correspondence.” (*What Is GDPR, the EU’s New Data Protection Law?* - *GDPR.Eu*, n.d.)

### **2.1.2 Digital**

- 1994 Netscape releases a browser that makes online tracking possible for the first time.
- 1995 European Union adopts the Data Protection Directive.
- 2000 US and EU signs the Safe Harbour agreement allowing data transfer of European citizens’ data to the US.
- 2015 European Court of Justice declares Safe Harbour is not a proper way of transferring data between Europe and the US.
- 2016 The EU enacts the General Data Protection Regulation (GDPR), which is the most significant change in data protection laws in over 20 years. It is applied across the EU with a single set of rules and stricter penalties.
- On May 25<sup>th</sup> 2018, after a two year transition period the GDPR goes live. (Klasovec Kingsmill & Barday, 2021)

## **2.2 Key drivers for change in privacy management**

The megatrends that affect privacy and consent management are in close relation to digitalisation, the pandemic, changes in consumer behaviour and consumer empowerment.

There are several drivers behind the paradigm shift in terms of digital privacy and the rights to our own data. The two strongest drivers are regulation and change in consumer behaviour. These are forces that drive each other. EU has set the standard in digital rights where the GDPR is perhaps the most well-known initiative, which has inspired similar initiatives in over 100 countries (*Cisco-Consumer-Privacy-Survey-2022*, n.d.).

Privacy-focused individuals and organisations have been driving projects to enhance user privacy. Early examples of these are browser add-ons to block out trackers and cookies. Later different browsers, such as Mozilla Firefox, have taken a completely privacy-focused approach and are blocking tracking technology by default. This has forced the big technology players, usually referred to as GAMA (Google, Amazon, Meta, Apple), to acknowledge this in their own approach to meet the rising demands of evolving regulations and expectations of consumers.

Several studies indicate that the trend in privacy issues leans strongly towards consumers wanting transparency from companies and brands. (*#BrandsGetReal: Social Media & the Evolution of Transparency* | Sprout Social, n.d.)

Why is the topic of our privacy in terms of data on the agenda right now? Privacy laws have been around for a long time, the earliest for hundreds of years (Klasovec Kingsmill & Barday, 2021). However, it is only recently that privacy laws have extended to the digital world (Turrecha, n.d.).

## **2.3 Ethical and transparent data**

Consumers are demanding more privacy, transparency, and control over their own data. Regulators all over the world are setting stricter laws to meet these demands that are based on values such as trust and transparency. Ethics and transparency are examples of a sustainable data strategy. This is a phenomenon growing worldwide and something that is taken with great seriousness in the EU and Finland. Sitra has stated fair data as one of its four strategy cornerstones. Especially in the area where individuals should own their own data.

“At the individual level, the right to one’s own data is considered to be a fundamental right in the digital era.” (*Fair Data Economy - Sitra*, n.d.)

However, both the EU and Sitra are making a call for competitive business opportunities as well within the boundaries of fair data economy but the emphasis being on data sovereignty. (Sitra, n.d.)

### **2.3.1 The privacy challenge**

Our personal and intimate information is getting increasingly digitalised and spread out to different parties and systems in a way that we can’t control ourselves.

On the other hand, there are business needs that drive how to optimise business results and profitability. This is optimised by utilising ever more efficient technology to combine data from a variety of sources and automating that for maximum outcome. Now, with the advent of regulatory and consumer behaviour changes, companies have to consider how to find a balance in maximising profit but to keep up with the regulatory changes as well as how to react to customers demanding that their data should be sustainably in a fair, transparent and trustworthy way.

Currently, there are different players lobbying for various agendas on how strictly personal data can be utilised. There are big GAMA technology companies such as Google, Amazon,

Meta and Apple looking out to safeguard their own business interests. The European Union have imposed legislation trying to control its dominant position in digital ecosystems.

There are also various global and local organisations representing companies, advertisers and agencies arguing that current legislation is too strict and it is killing business opportunities for many companies because they cannot use the customer data anymore in a meaningful way. IAB is an example of an organisation lobbying against stricter regulation on how customer data can be used. IAB has developed a framework, TCF 2.0, that would solve issues related to the use of customer data, especially when it comes to the use of third-party and first-party cookie data. There are constantly coming up new reports where research is trying to prove that businesses and consumers actually benefit from fewer restrictions on how customer data can be used (Howard Beales & Stivers, 2022).

On the other end, you have organisations like Noyb (None Of Your Business) and privacy activists, where Max Schrems is maybe the most well-known. Max Schrems has successfully argued for privacy regulation and driven cases in EU courts, pushing for stricter control of personal data and how it can be used.

In a way, you could say two counterparts are colliding with opposite views. On the other side, there is the wish to utilise all kinds of data to maximise business profit versus regulating and controlling what data can be used from the legal aspect and moral aspects of consumers. Then you have the consumer somewhere squeezed in there between, learning how to react and function in an ever-complex digital world. The fourth player in the equation is the government responsible for the legislation and regulation for everyone's benefit.

The European Union is a perfect example of a regulator trying to find some middle ground from all the different views with a European Data Strategy that holds many digital initiatives. When it comes to respecting individual privacy values, the focus is on European values, but at the same time, the EU is making efforts to create digital opportunities for businesses. (*A European Strategy for Data | Shaping Europe's Digital Future*, n.d.; *EU Data Initiatives in Context*, n.d.)

Consumers are becoming more aware and concerned about how their private data is used. According to an IBM study, 81% of global users are concerned about how companies use their data (*IBM Study: C-Suite Leaders Who Value Trust in Data Are Positioned to Outperform Peers - Nov 12, 2019*, 2019). Even though such a vast majority of consumers are concerned about their data, according to many studies, they still give it away by impatiently confirming anything just to get quick access to content. This phenomenon is best known as the privacy paradox (*Why It's So Hard for Users to Control Their Data*, n.d.).

One interesting topic is how people see and value their personal data. What data can be seen as commonly available data that might not need any permission from other parties – is there any data of that kind? What is highly confidential data – such as sexual orientation, political views etc.? Obviously, there are some common norms, but as in life, in general, different people have different views on this. The interesting question is how the view on personal data change in the years will to come. Will it be seen as an intimate issue? In what kind of scenarios can what kind of data be utilised? Should there be laws to govern some kind of data, or can the individual decide and override common legal perceptions and give away their data as they see the best fit? What will be the common standards in how and what data is acceptable to use? E.g., usually, you do not ask other people sensitive questions, nor do you not give them out.

### **2.3.2 Corporate data responsibility**

According to a study made by KPMG, it shows that business leaders share a very different view on how data and privacy issues. 95% of the leaders state that their organisations have strong data protection processes in place, and up to 98% state that privacy is an organisational priority. The employees have a very different view on this. 44% of full-time employees said that their data protection training could be more helpful, and 40% found the data privacy training not useful. With part-time employees, the numbers are even lower with 30% for the respective category. (*Corporate Data Responsibility - Bridging the Consumer Trust Gap*, 2021)

In order to manage data privacy and security it will become imperative to build solid data supply chains where transparent data management is high on the strategic agenda in organisations. (Orson & Stein, 2020)

### **2.3.3 Complexity with interconnected data**

Today still, one of the biggest obstacles to combining various data sources is the mismatch between different systems and the need for common structured rules on how to do this. To tackle this problem and find new possibilities for data use in various fields EU has started an initiative called The European Gaia-X project. (*Gaia-X Finland - Sitra*, n.d.) Furthermore its goals are to bring different stakeholders closer to one another by providing frameworks for data policies and rules and open innovation ecosystem. (*Home - Gaia-X: A Federated Secure Data Infrastructure*, n.d.)

As we know, the amount of data is growing at an incredible speed and like Sitra's President Jyrki Katainen said: "Data is the world's fastest growing resource." (Katainen, 2022).

Besides the vast amount of growing data available, many other pieces build on the data ecosystem's complexity, making it very difficult for even professionals to understand all the different relations to make everything work, let alone the individual. However, attitudes change from unawareness to awareness regarding who should control and benefit from personal data. According to a study made by Visa, up to 68% of customers believe that companies benefit from the personal data the consumers have given them. In the same study, 76% of consumers say that they want to take control over their own data. (Bella, 2021)

#### **2.3.4 Data as a human right**

The discussion of who should own the rights to their own data is not new, but for some reason, it has not been very high on the agenda of the average consumer. Data as a human right was already mentioned at the World Economic Forum back in 2012, stating that data should, in a bigger picture, be put to work for the greater good of humankind with an ethical framework in place (Green, 2012). In a study by KPMG from 2020 it states that 87% of consumers think privacy is a human right (Orson & Stein, 2020).

In another study, it is proposed that data should be a labour in the future where the user data should propose as a means of serving the benefit of the one who is generating the data in forms of payment in the change of access to data. It is proposed that some form of data labour unions could be a force of giving control to the user with a “minimum data wage” as well as means of data striking as well as improving the quality of the data. (Arrieta Ibarra et al., 2018).

There are parallels to be drawn to previous phases of the industrial revolution. The change towards people would oversee their own data has been compared to the rise of labour rights in the late 1800s and early 1900s when citizens' felt their rights were exploited by large corporations (Pentland & Hardjono, 2020). All over the world, governments issued laws to protect the rights of citizens and regulate the companies.

#### **2.3.5 The privacy paradox**

The term privacy paradox was first used in a study made in 2001 by Barry Brown for HP (Brown, 2001). This is exemplified when consumers online say that their intentions are privacy-focused, but their behaviour is contrary (Stouffer, n.d.).

Another close example is when consumers do not want to share their data with companies but, at the same time, expect personalised services. Despite several studies, there are no clear conclusions why people expect that their privacy should be respected, but still, many hands out their data on quite light incentives. (Gerber et al., 2018)

People do care about their privacy, but it is due to several factors that it is not always implemented in real-life behaviour. In a fast-paced digital world, it is not easy to make qualified decisions about your privacy, especially when it takes time and is quite a complex environment. People are also inclined to grab easy and quick incentives instead of thinking long-term and considering how their data will be used or even misused. This is just natural human-biased behaviour that has been researched in several studies. (Leslie K. John, 2018)

Another example is the illusion of control, where people think that when presented with an option to control some of the data they are sharing and to opt-out of how they are tracked on the web gives them a false feeling of security (Leslie K. John, 2018).

## **2.4 Data governance and privacy focused frameworks**

Data governance is usually mentioned as a solution in connection with data privacy issues. However, data governance as a topic is extensive and includes data security, data quality, data lifecycle handling, master data and privacy as well if implemented correctly. However, the privacy aspect seems to fall short and is often a bit overlooked or sidestepped in the data governance process. The debate around privacy is heating up, and it is a topic that is growing fast and in complexity. Therefore, privacy frameworks are much needed to supplement the data governance process. As an example, this could be compared to the ISO certification 27001 for Information Security Management Systems and the extension ISO 27701 for Privacy Information Management Systems, where the latter focuses more in detail on privacy instead of data security.

IAB Europe has introduced their own TFC 2.0 framework from a regulations and technology perspective. Its purpose is to solve the roles of regulation, technology, and different stakeholders such as the first party (i.e., publisher) and third party (i.e., advertisers). The technology used here is the CMP. Currently, the TCF. 2.0 has been ruled as non-GDPR compliant by the Belgian Data Protection Authority, which places TCF 2.0 in a place of uncertainty.

Privacy by Design, also known as Privacy by Default, means, in short, that privacy should be built into the technology. It is an approach to data protection that encourages companies to design their systems and processes to ensure that the highest level of privacy is achieved by making sure that personal data is automatically protected in different IT systems and business processes. If a user does not do anything, their privacy remains intact. Privacy by Design consists of seven different foundational principles, which are:

1. Proactive not Reactive; Preventative not Remedial



2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality — Positive-Sum, not Zero-Sum
5. End-to-End Security — Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

(Cavoukian, n.d.)

Other well-known, widely used and referenced frameworks are the NIST Privacy Framework and the OECD Privacy Framework.

## **2.5 Transparent consent design**

When planning and designing, how to achieve the point is not to trick users into giving consent by making designs that are deceptive. The way to get consent in the future is to earn the trust of the users. This is done by being clear and honest about what the user is giving consent to and making it clear and easy. The design should be clear and simple and explain shortly why the company needs the data and what is the return and value for the customer when doing so. The first step and the minimum are to follow the guidelines of the regulation. The next step is to create a design and policy that goes beyond the lowest level of necessary banner design with the required elements. This gives the user an additional feeling of trust.

### **2.5.1 Deceptive design**

Deceptive design or dark patterns means that users are misled into giving consent and tricked into performing actions they would not do otherwise. Even though many users find the cookie consent banners in the EU annoying and state that these are making the internet unusable by applying “regulatory bureaucracy”. The point the lawmakers are making is that approving or declining cookies should be made easy and simple. One of the main problems is that many websites deliberately apply these so-called dark pattern designs where the user is tricked into giving consent by making the whole cookie consent process more annoying for the user. Only the accept all cookies has been made easy enough. Quite often, the reject cookies option is hidden behind too many clicks and might even be missing altogether. According to Max Schrems, only 3% of users want to give consent, but up to 90% can be influenced by deceptive design to accept all cookies. (*Deceptive Design - User Interfaces Crafted to Trick You*, n.d.; Lomas, 2022)

## **2.6 Data and privacy initiatives in the EU**

There are various privacy initiatives around the world, but we will have a look at some of the EU initiatives since they are quite often forerunner initiatives when it comes to creating new business opportunities and fair usage of data.

One such colossal initiative is the European strategy for data, where the concept of data spaces plays a significant role. The idea behind this is to create data spaces for different sectors such as health, agriculture, manufacturing, energy, mobility, financial, public administration, skills and so forth. The data would be standardised in these sectors for better data quality and data flows to ensure better business opportunities. An essential factor is to follow and respect European rules, governance standards and values for the fair use of data. (*Common European Data Spaces – Real-Time Linked Dataspaces*, n.d.; *Staff Working Document on Data Spaces | Shaping Europe's Digital Future*, 2022)

### **2.6.1 The need for regulation**

Companies and organisations have been slow to adapt to privacy guidelines. Therefore, authorities and governments have started to impose stricter regulations on data use. However, in many EU countries, the authority responsible for privacy data-related regulation does not have the resources to follow and enforce that the rules are followed, and they remain unsolved as the pile of complaints keeps growing. (*Cookies: I Looked at 50 Well-Known Websites and Most Are Gathering Our Data Illegally*, n.d.)

## **2.7 Regulation**

There are currently privacy laws applied in over 130 countries worldwide (*Cisco-Consumer-Privacy-Survey-2022*, n.d.). This means that privacy laws are eventually becoming a standard for personal data processing, and people all over the world are becoming used to these standards. The laws will dictate how companies and other data processors must apply to handle their data accordingly. The change driven by these privacy laws will also guide people using services and eventually be more demanding when it comes to data privacy-related issues and behaviour.

Gartner is predicting that by the end of 2023, up to 75% of the global population will be covered by a privacy law that protects personal data (Panetta, 2021).

EU has been at the forefront for years and a thought leader by example when it comes to personal data privacy topics and is committed to doing so by building trust with legal certainty. In this work, when discussing legal aspects and regulations, the focus is mainly on EU privacy laws and regulations.

### **2.7.1 GDRP - General Data Protection Regulation**

The GDPR is presumably the most well-known privacy law in the world and one of the first of its kind. It finally came into effect on May 25th 2018, after a lot of commotion and years of preparation. In fact, it took more than four years of debate before being approved by the European Parliament and Council in April 2016. (Burgess, 2022) The usual two-year period for preparation and implementation was given to the member states.

The GDPR replaced the European Data Protection Directive, which was stated in 1995 and had become outdated during the 20 years of development in digital and especially how personal data can be used. (*What Is GDPR, the EU's New Data Protection Law? - GDPR.Eu*, n.d.) The GDPR is a directive which means that all member states have to apply the directive as such without any deviations.

### **2.7.2 ePrivacy directive and regulation**

The ePrivacy directive was the driving rule in EU privacy-related issues in 2002. A directive is not a piece of legislation that enforces all the member states to apply it as such, but it is more of a guideline that can be implemented to fit the needs of each member country.

The ePrivacy regulation was meant to stand in action alongside the GDRP and support it. But it has been delayed time after time due to various reasons. It is not known yet at the time of writing this thesis when it will be finally released. The estimate is that the earliest will be in 2023.

The difference between the regulation and the directive is that a regulation must be implanted as such by all the EU member states, as was the case with the GDPR.

This situation has caused a lot of irritation and different interpretations of how ePrivacy should be applied. For instance, in Finland, it took long before the proper authority, Traficom (Finnish Transport and Communications Agency), was mandated to take responsibility for implementing guidelines on how to interpret the ePrivacy directive for cookies and data. The guide has taken quite a strict approach on how to implement the directive and perhaps even to take a stricter approach in anticipation of the upcoming ePrivacy regulations.

### **2.7.3 DSA – Digital Services Act**

The purpose of the Digital Services Act is to give the online user a more trusted online environment with transparency and better protection when interacting with digital services and regulate how these players can operate. It consists of a long list of actions and obligations, such as better protecting minors on different platforms and a ban on profiling children based on people's political, ethnic or sexual orientation. The obligations also

include flagging and monitoring illegal content and putting measurements in place to fight disinformation. The list goes on by giving more transparency into what terms and conditions apply to different services, making it easier for users to challenge platforms in regard to their content and banning the use of dark patterns to trick users into giving consent. (*Questions and Answers: Digital Services Act, 2022*)

The DSA entered into force on 16 November 2022 and will start to apply after a 15-month transition period on 17 February 2024 (*The Digital Services Act Package | Shaping Europe's Digital Future, n.d.*).

#### **2.7.4 DMA – Digital Markets Act**

The purpose of the Digital Markets Act is to apply new rules for platforms that are considered gatekeepers due to their substantial size in the market. The package will cover all European Union's digital services, including social media, online marketplaces, and other online platforms. One of the purposes is to hinder these platforms from applying unfair conditions for both businesses and consumers alike. The DMA is a vital part of the European digital strategy to make Europe more competitive in the digital age. (*Digital Markets Act: Ensuring Fair and Open Digital Markets, 2022*)

The DMA entered into force on 1 November 2022 and will be applicable after a six-month-long transition period on 2 May 2023 (*The Digital Services Act Package | Shaping Europe's Digital Future, n.d.*).

### **2.8 Technology**

Technology is becoming more vital and necessary to handle and control different aspects of privacy and consent. There are emerging new technology for privacy, consent and regulation, which has to be planned and fitted to work together with other technology the organisations possess. This varies from newer marketing-related technology, which usually is connected with customer touchpoints but also back-end technology which can quite often consist of old legacy technology in companies and can, in worst scenarios, build bottlenecks and hinder an effective and functioning technology architecture stack.

#### **2.8.1 A description of relevant technology**

A new breed of technology is building up next to, or maybe even on top of, traditional MarTech and AdTech if you look at it from an architectural point of view. Because of the often-mentioned change drivers, the privacy landscape is evolving at a great pace, and it is getting more complex the whole time. Utilising technology and especially privacy-related

technology is a must in order to comply with and execute the mandatory processes required by regulation.

## **Cookies**

The internet has been dependent on cookies for various purposes, and it still is and will be so in the future. Even though cookies have nowadays a somewhat shady reputation, most websites and digital services are dependent on cookies to function correctly. Cookies per se are not bad, and it is more how they have been misused, mostly in terms of privacy-related issues.

It is generally the third-party cookies that have a shady reputation that is going to slowly disappear. 3rd party cookies are a means to connect information between different websites or digital channels. Back in the early days, no one had any control or information on how these were tracking consumer data and behaviour. Now that the third-party cookies are disappearing, the switch will turn towards 1st part cookies on other identifiers.

Without cookies, web services cannot function, and they are, in fact, essential for many features to work correctly. Many of the web services we use require cookies, and shopping baskets in web shops are an excellent example of this. When third-party cookies disappear sometime around 2024, as it seems now, all cookies will not disappear. Instead, we will be using more first-party cookies in the. The difference is that first-party cookies are stored on the server of the website someone visits and are therefore considered more trustworthy than third-party cookies, which come from other services, as the name itself states.

However, in regard to acquiring consent, the same rules and regulation applies as for third-party cookies, and consent has to ask for first-party cookies and the user can decline them just like third-party cookies.

## **Consent Management Platform (CMP)**

The Customer Management Platform is maybe the most well-known and used tool today in terms of acquiring and controlling consent. Typically, the CMP is the first encounter a user has with a company. This is where the user selects how a company can use tracking technology, usually cookies.

Depending on the technology provider, the CMPs can vary slightly in the functionality they provide. But basically, the CMPs are consent and consent banners that most of us face when we go to a website, web service or digital application. The primary purpose is to obtain legal consent to use and process customer-related data. With a CMP, it is possible to apply it to follow the regulations that are applicable in different countries. In the EU, legal

regulations set rather strict guidelines on how this consent should be achieved. This is usually data based on cookies and tracking technology.

### **Centralised consent management**

There is a new emerging technology called Privacy and Preference Centers which work as an extension and in unison with consent banners. These tools allow users to choose more in detail what information they want to share with a company. Both tools have overlapping functionality but have some distinctly different features that are good to be aware of when implementing this technology and functionality. Quite often, these are implemented with overlapping functionality. For the customer, there should be only one interface where they can access and control their information. In addition, these tools can give insight into how people are willing to share data which can be interesting information from a business perspective. Privacy Centers are usually more formal than Preference Centers because of the type of data they handle.

### **Privacy Centers**

A Privacy Center is meant to serve more from a regulatory perspective and take privacy-related legislation into consideration. With a Privacy Center, companies can control that privacy regulation-related policies are always up to date and applied to all channels simultaneously. If a company has business in various countries with different privacy regulations, these can be applied and controlled separately.

A Privacy Center is a source of truth in how and when consent was given. A Privacy Center shows consumers that the company takes privacy seriously and is a trusted partner. It can be a serious competitive advantage and build on a positive brand image. It also has operational benefits when manual and time-consuming processes can be automated so that customers can access their information themselves.

Customers can use a Privacy Center to exercise their privacy rights. In the case of GDPR, people can ask to be forgotten and get their data removed, transfer their data somewhere else and access their information, to mention a few of these rights. (*What Are Privacy Centers and Should You Have One? - Privacy Policies, 2022; What Is a Privacy Center & Why Does It Matter? - Securiti, n.d.*)

### **Preference Centers**

A Preference Center is more aimed at the business side, especially with marketing communication. Here customers can choose the preferred frequency they want to receive messages from a company, whether it is monthly, once per week or even daily, whatever

the preference might be. In a Preference Center, customers can also decide from which channels they want to receive information. These are usually email, push messages, text messages and phone calls. Customers can also give more detailed preference information such as clothing size, favourite cities to travel to or preferred movie genre, to name a few examples. The GDPR is necessary to consider because, by default, consumers have to actively opt-in for any communication or preferences. (*What Is a Preference Center & Why Is It Important?* - Securiti, n.d.)

## **Identity Management Platforms**

As we are moving away from the use of third-party cookies and entering the era of first-party data, it will become imperative for companies to make it easy for customers and prospects to sign in and sign-up for services in a way that the user would prefer. Typical tools and solutions to achieve this technically are Customer Identity Access Management (CIAM) and Single Sign-on (SSO). (Parker, 2022)

## **Digital ID solutions**

In the world of digital identification, there are a lot of things happening right now, and there are many initiatives going on around the world. There are governmental, commercial, and non-commercial initiatives that are actively being developed to handle various forms of digital identification. This is a fast-growing trend since it is estimated that by 2024 over 5 billion people worldwide will have a digital ID in their use (*Digital Identities in 2022 | DW Observatory*, n.d.). In the EU, there is the European Digital Identity, which is meant to be a digital wallet for all citizens, residents, and businesses in Europe (*European Digital Identity | European Commission*, n.d.). Currently, there seem to be too many digital ID initiatives that it will be difficult to know what to use when to use them and in which context. However, this is a positive development and will surely be centralised eventually.

## **Customer Data Platform (CDP)**

Customer Data Platforms have been the buzzword on the marketing technology scene for a few years now and are slowly but finally getting wide acceptance and adaptation in companies as the tool that combines customer data from various sources into a single view of the customer and activates it in a personalised way in an omnichannel environment. As the CDPs develop, so do their functionalities, and there is overlapping functionality with other established marketing technology tools. (What Is a CDP? - CDP Institute, n.d.; What Is a Customer Data Platform (CDP) and Why Do Marketers Need One? 2022)

The paradox here is that now when it is easier than ever for marketers to implement and use so-called out-of-the-box tools for unifying personal customer data, it is more difficult to activate this data because of privacy-related regulations and consumer behaviour.

In order to manage how a CDP can be used to its full potential, proper consent management will be extremely important and practically a mandatory element when executing use cases in different touchpoints.

### **2.8.2 The rise of privacy technology**

PrivacyTech landscape is a relatively new technology category that is still developing rapidly. Some would argue that it is a subcategory of MarTech, which it, to some extent, also is, especially when it comes to tools that are used at the customer touchpoints, such as a CMP or a Preference Center. However, technology such as Privacy Centers, identity management or Privacy Enhancing Technologies (PETs) is at the borderline of enterprise technology. In the big picture, privacy technology is about strengthening the privacy of the individual users of any organisation that is using personal data privacy (Barday & Klasovec Kingsmill, 2021).

### **2.8.3 A practical approach to Consent Management**

The regulation gives strict guidelines on how consent must be asked from users if there is tracking technology on the website or application. Organisations must solve the issue by finding the right balance between business drivers and needs versus how they are using consumer data when achieving business goals. (Klasovec Kingsmill & Barday, 2021)

Companies also must have solid processes for how they handle data and privacy from various perspectives. Until recently, users didn't really have a say when it came to how a company could utilise their data. Now they have a choice. Some might still give permission to use their data as usual, while others will certainly decline or at least be more aware and cautious about what data they are sharing. This means that use cases companies have been using will not work as they used to for the ones who are declining cookies as a means of targeting and personalisation. For those, companies will have to come up with new use cases to reach them; this requires a look into new business processes.

## **2.9 Theory conclusion**

While technology has made it possible to collect data from various sources and track consumers through many channels and touchpoints in intrusive ways, technology is also the solution to restrict this and gives all parties involved in collecting and storing customer data the means to control it in a sustainable way. The legislation, such as the GDPR, was



the trigger, but paragraphs cannot bring the hands-on solution; in this case, the right kind of technology is needed.

It is quite an interesting paradigm that there is now building up a new technology category around privacy and regulation that is meant as a counter-measurement purpose to tackle the technology that made intrusive data collection easy. Hopefully, this new technology is a supplement or, even better, a corrective and iterative way to bring transparency and sustainability to the way data was collected and used earlier without that many possibilities from consumers to have a say in how their data was utilised. As it seems now, this new technology could even replace the old intrusive tracking technology. This is hopefully also the starting point for a more significant take on how to utilise personal data beyond the marketing purpose scope. We don't want any authoritarian governmental use of our personal data, even though in that context, different and more personal and even intrusive data and information is needed, it should always be transparent, and the subject of the personal data should always know who, when and how data about them was used and in which context. How this is implemented is, of course, up to all of us and do we want to support the data democratisation process?

There is not just one single framework or process for an organisation to use and follow when preparing for the upcoming changes around various privacy topics (Auty & de La Lama, 2022). Due to the vast number of tools and technology, frameworks, local and global legislation and many other related changing variables, organisations need to have insight into various topics wherefrom to start building their own consent and privacy playbook that is an agile and iterative consent and privacy strategy that is future proof.

### **3 Research plan**

There does not seem to be a lot of academic research that covers the same aspects as in this research. The aspect where regulation and technology are meeting the customer in the context of consent and privacy, seems to be such a new and fast changing topic that the research is often from highly specific and focused areas around it.

However, the topic is gaining a lot of interest due to the adjacent changes and is getting more coverage in articles on different sources on the web that are specialised in the topic from different angles. Large consultation agencies such as Gartner, KPMG, EY etc., are covering this topic from different angles. Sitra is an organisation that is researching this topic from a fair data economy perspective (*Testbed for Fair Data Economy – Ihan.Fi - Sitra*, n.d.). Harvard Business Review is writing about this topic from various points of view but also from a designing for transparency and trust perspective when using customer data (Morey et al., 2015).

In my research, I am utilising academic research papers to get solid insight into the different basic concepts and deepen those views with in-depth research in expert areas and form my own conclusion to match the research questions and meet the expectations of the work.

#### **3.1 Methodology and approach**

Service design and design thinking are gaining ground in the corporate world. Many organisations are turning to service design methods when establishing a customer-centric culture in all kinds of business fields. Service design is a customer-centric approach to focus on understanding the customer's needs. There are several approaches in the service design process; some of the most well known are: Moritz's six stages of service design (Miettinen & Koivisto, 2009) the double diamond from the UK Design Council (Koivisto et al., 2019) and Stickdorn and Schneider's discover, define, develop, deliver (Peng & Tran, n.d.) to name the most well-known ones. These process phases include techniques like interviewing, observing, co-creating, generating ideas and narrowing those ideas down to ones that are going to be prototyped and then iterated over again. Divergent and convergent thinking is used in different stages when finding and defining, developing and producing results and findings (Thoring & Müller, 2011). Both quantitative and qualitative methods are used, but the latter seems to be used more often.

Business design is another design thinking method that is used more frequently in connection with service design projects to ensure that profitable business models are in focus when designing services (Koivisto et al., 2019).

### **3.1.1 Constructive Research and design science research**

Constructive research approach (CRA) often referenced as design science research (DSR) are quite similar and comparable in the approach (Pirainen & Gonzalez, 2014) and very often referenced as synonyms for the same research method (Dresch et al., 2015).

Both CRA and DSR methods are well suited for research in domains such as engineering, technology, business, and economics-related fields (vom Brocke et al., 2020). This approach suits well the nature of applied research we are supposed to conduct for companies as applied science students.

### **3.1.2 Comparison and differences**

Service design, design thinking, and design science research have similar ideological phases in understanding the problem from a user point of view and even using the same type of methods of gaining insight. Based on the findings, a solution is developed. While service design is generally considered more creative and human-centric, design science research is more focused on developing and delivering a solution, usually with a technology focus.

## **3.2 Approach**

As for the methods used in the thesis, service design and design science research because they complement each other very well (Teixeira et al., 2019). Service design is perfect for understanding customer needs and matching that with business requirements. I wanted to use the human-centric approach to gain a deep understanding from a customer point of view. This was conducted with a quantitative questionnaire and qualitative interviews. This was important for the foundation of the thesis work since it is paramount to understand customer behaviour when they are confronted with a consent banner and how to consider how they want to share their data with companies.

I approached the complexity of the work by drawing a mind map to understand the different elements and their relations. This helped me to understand what to include and exclude from the work. A detailed picture can be found in Appendix 2.

## **3.3 Data collection and development process**

To gather data and insight, I used both quantitative and qualitative methods. I started with the quantitative part by conducting a questionnaire for Dagmar's personnel. The reason for this method was to get a larger set of comparable data to understand the user's view on consent and privacy. Based on the findings from the quantitative phase, I got an insight into

certain focus areas that I examined deeper in the qualitative part with in-person interviews and prototyping. For the service design and design thinking phase, I used qualitative methods such as interviewing to gain a deeper understanding. Based on these findings from the interviews, I made wireframe prototypes that I tested with additional iterative interviews.

As for the technology architecture solution, I used constructive research methods to research in technology literature, whitepapers and other sources, as well as my own expertise working with marketing technology for over 15 years.

## **4 Consent and privacy management framework**

The framework consists of three entities: the privacy and consent toolkit, the consent design and testing and the technology architecture.

The purpose of the framework is to create methods, to list and explain tools that are needed to understand the complexity of digital consent and privacy-related issues and prepare for short- and long-term actions, to be future-proof as well as quick and reactive.

Its use is meant to give the tools and concepts for any organisation to plan for the right elements to handle their approach in a complex environment with a strong focus on consent and ePrivacy. Companies, especially the business and legal stakeholders, benefit more from a less technological approach to understanding what the change drivers behind privacy are.

The ePrivacy and consent toolkit is the largest in terms of complexity and content in this. It is a listing of different and essential know-how areas to take into consideration when evaluating what ePrivacy and consent-related topics are necessary for an organisation. It is important to recognise that the topics from these know-how areas are under constant change as the environment is changing around consent and privacy.

The consent design and testing focus on a topic that is often overlooked. Most companies and organisations implement an out-of-the-box consent mechanism that is provided by the technology provider. They might make minor brand colour adjustments and tweaks to comply with local privacy laws. It is still rare that any organisation is really considering how to design a consent banner that communicates what, why and how the data is used. This can be the deal breaker when a visitor decides if they trust the company to give extended permission to use their data. A/B testing is an extended feature to perform in order to understand and be certain what kind of a banner converts the best.

Without technology, consent management cannot be handled. Therefore, privacy technology must be implemented into the architecture stack, which can easily be quite complex with various data sources, back-end and front-end technology and many customer touchpoints to take into consideration. This technology is also relatively new and usually demands skills and business understanding beyond traditional IT needs.

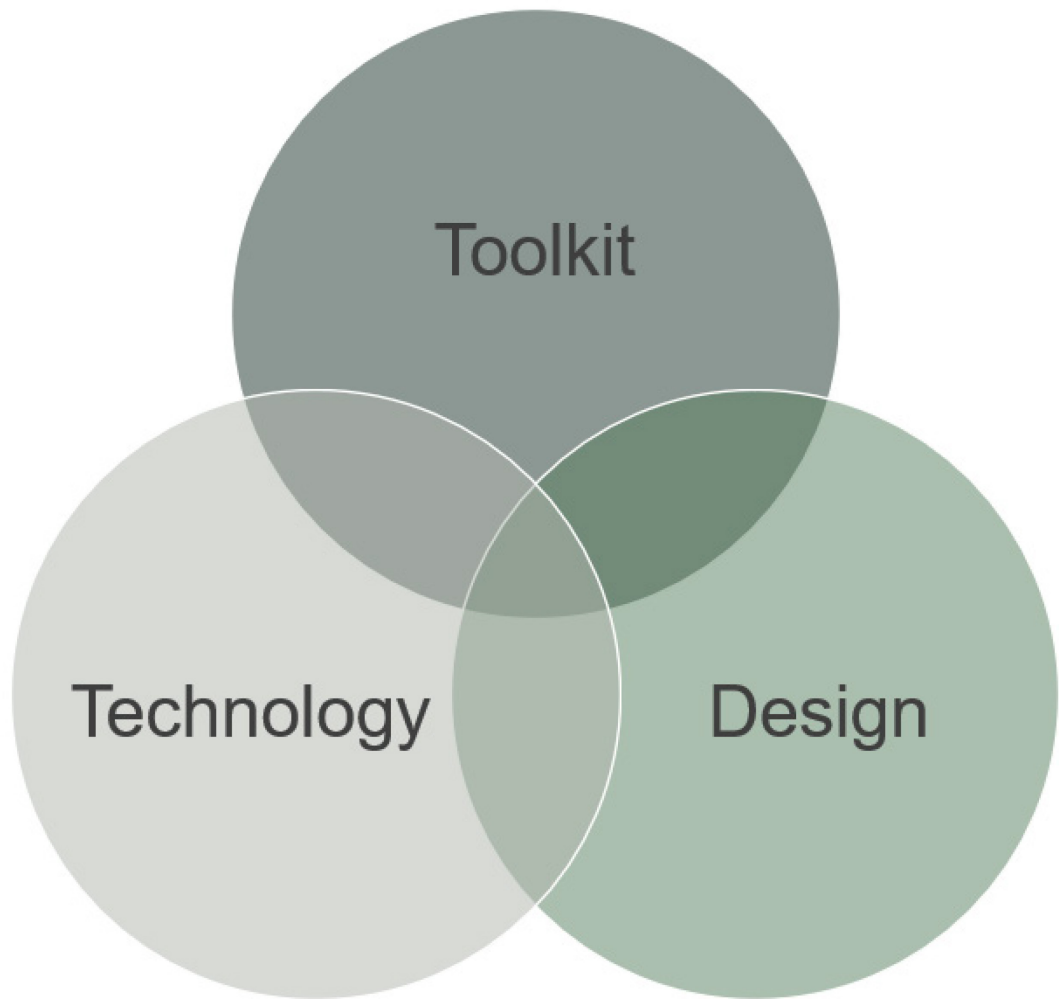


Figure 1. Consent and privacy management framework.

#### **4.1 Privacy and consent toolkit**

The purpose of the privacy and consent toolkit is to frame relevant topics into areas that are applicable when planning for a long-lasting and future-proof strategy. These topics enable an iterative approach in a very fast-changing environment with a lot of different factors to take into consideration. It is not meant that all the topics have to be addressed at once but chosen and selected based on the needs at the moment.

There are five different categories: legal and regulation, trends and insight, technology and data, ethics, values and design and business and processes.

Topic	Legal & Regulation	Trends & insight	Tech & Data	Design, UI & UX	Ethics & Values	Business, Processes & Strategy
Why is this important	It is important to understand what new privacy laws and regulations obligates companies to do. The consequences can be substantial fines or reputational damage and consumer mistrust.	This is a very complex environment that is evolving very fast and there are many different factors to take into consideration. Changes can mean very time consuming, expensive and complicated processes to implement. The sooner you know, the better you can plan and be reactive.	Without technology consent and privacy cannot be handled.	Design plays an important part in how consent has to be acquired by law but also how design can be implemented in a way of creating trust and optimising a positive consent rate.	Consumers are demanding for more privacy, transparency and control over their own data. Regulators all over the world are setting stricter laws to meet these demands that are based and values such as trust and transparency.	All of these changes are changing fast in a very complex environment. It brings new rules and new ways of executing business cases that used to work before but will impact heavily many traditional business cases.
Context (examples)	<ul style="list-style-type: none"> <li>Regulation – what has to be executed and has to be in place (eg. GDPR, cookie compliance)</li> <li>The most important drivers. (Sanctions, reputation damage)</li> </ul>	<ul style="list-style-type: none"> <li>Change in consumer behaviour</li> <li>Technology landscape changes (Cookie depreciation)</li> <li>Privacy First approach</li> <li>Insight -&gt; actions</li> </ul>	<ul style="list-style-type: none"> <li>Tech needed to handle all of this (CMP, preference centers, CDP, server side)</li> <li>Support in selection of tech</li> <li>Tech implementation</li> <li>Audits</li> <li>Threat assessments</li> </ul>	<ul style="list-style-type: none"> <li>Fair design principles</li> <li>Tone of voice in communication</li> <li>A/B-testing</li> </ul>	<ul style="list-style-type: none"> <li>A sustainable approach to using data transparently</li> <li>Fair design principles</li> <li>Tone of voice in communication</li> <li>Utilisation of brand values</li> </ul>	<ul style="list-style-type: none"> <li>Iterative privacy processes (for different units)</li> <li>Skills (in-house / external)</li> <li>New business opportunities (e.g. preference center tools as personalisation enablers -&gt; better personalisation -&gt; Less op-outs)</li> <li>Automation</li> <li>Risk mitigation</li> <li>Customer journey planning for data collection</li> <li>Audit</li> </ul>
Elements	<ul style="list-style-type: none"> <li>Privacy regulation &amp; law <ul style="list-style-type: none"> <li>World</li> <li>EU</li> <li>Local/ country</li> </ul> </li> <li>Threat modelling</li> <li>Schrems II</li> </ul>	<ul style="list-style-type: none"> <li>Consumer behaviour</li> <li>Privacy regulation &amp; law</li> <li>Technology</li> <li>Unexpected change drivers</li> <li>EU initiatives <ul style="list-style-type: none"> <li>Data spaces etc</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Privacy technology <ul style="list-style-type: none"> <li>CMP, Privacy &amp; preference centers</li> <li>RegTech</li> </ul> </li> <li>Other relevant technology <ul style="list-style-type: none"> <li>CDP</li> <li>ID solutions</li> <li>Threat modelling</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Customer experience</li> <li>Privacy First approach</li> <li>Trusted design</li> <li>Privacy Communication strategy</li> <li>Trusted design</li> <li>Privacy-by-design</li> </ul>	<ul style="list-style-type: none"> <li>Values: transparency &amp; trust</li> <li>Brand values</li> <li>Customer experience</li> <li>Privacy frameworks</li> <li>Privacy First approach</li> </ul>	<ul style="list-style-type: none"> <li>Certificates <ul style="list-style-type: none"> <li>ISO standards</li> <li>CIPP-certificates</li> </ul> </li> <li>Business case strategy / evaluation</li> <li>Privacy frameworks</li> <li>Privacy strategy</li> <li>Data strategy</li> <li>Threat modelling</li> <li>Privacy audit</li> <li>Privacy-by-design</li> <li>A/B testing &amp; optimising</li> <li>Follow-ups with key stakeholders</li> </ul>

Figure 2. Consent and privacy toolkit. Appendix 3

#### 4.1.1 Legal, regulation and security

Understanding the wide impacts of different ePrivacy legislation is vital for any organisation. This is, however, quite tricky because it involves not only legal topics but as well deep understanding of technology and how digital marketing is functioning.

However, the law and regulation are where everything starts, and this is something everyone must comply with. Failing to do so might have dire consequences and impact in terms of hefty fines and risk of reputation damage.

Even though data security is not a part of this thesis, it is a classification that is closely related to this category, especially from the Schrems II ruling point of view. Many organisations operating in the EU must evaluate carefully how different partners and technology providers handle their data in terms of where the data is handled, the server locations, who are the possible subprocessors etc. Privacy-related threat assessments can be daunting operations, and they are becoming common for many European organisations, especially since many of the large technology companies operate outside of the EU/ETA area.

Certificates are important when finding guidelines on what to follow and how to implement procedures and showcasing expertise on an individual and organisational level.

On the organisational level, the two main ISO certifications related to data security and privacy are 27001 and 27701. ISO 27001 is more focused on Information Security

Management Systems (ISMS) that deal with data security than a traditional IT approach. ISO 27701 has more of an emphasis on privacy and Privacy Information Management Systems (PIMS) that supports and deepens the ISO 27001 standard. ISO 27701 gives companies and organisations a framework with building blocks and additional guidelines on how to handle Personally Identifiable Information (PII) data by applying best practices. Other closely related ISO certificates are ISO 27018 and ISO 29151. Their focus is on public clouds acting as data processors and how to protect sensitive customer data. (*What Is ISO 27701? How Is It Different from ISO 27001? - Polymer, 2021*)

Regarding certificates showcasing personal skills and knowledge, the Certified Information Privacy Professional (CIPP) is one of the most well-known and respected privacy certificates available. The International Association of Privacy Professionals (IAPP) organisation offers standardised certifications for privacy professionals. There are many different certifications that IAPP offers. As mentioned, the most well-known is the CIPP certification with a focus on a specific region: Asia (CIPP/A), Canada (CIPP/C), Europe (CIPP/E), U.S. private-sector (CIPP/US) and U.S. Government (CIPP/G). Brazil (CDPO/BR) and France (CDPO/FR) have their own specific certifications. In addition to these certifications, there are two more to take in case there is a need to specialise in privacy management and privacy technology. Certified Information Privacy Manager (CIPP/M) is aimed at professionals who can implement and lead privacy programs in organisations. The Certified Information Privacy Technologist (CIPP/T) certification, as the name states, is more from a technology point of view with a focus on data, infrastructure, software and cybersecurity. (*International Association of Privacy Professionals, n.d.*)

#### **4.1.2 Technology & data**

Marketing-related technology, also known as MarTech, has grown almost exponentially over the past few years. The guru of MarTech, Scott Brinker, has compiled a MarTech Landscape map of different MarTech-related tools since 2015. The number of listed tools has grown from 2011 with, circa 150 to almost 10 000 tools in 2022, with a growth of 6521% over 11 years (Brinker, 2022). This does not even cover all the tools on the market; I have noticed that there are several tools developed in the Nordic market that are not listed on Scott Brinker's MarTech Landscape. This Landscape map of MarTech tools is getting so bloated that despite being divided into several subcategories, it is almost impossible to get a grip on the offering that is available in different technology categories. These types of lists are not that useful anymore since it is almost impossible to use them to find relevant tools and technology. They serve as more of a measurement to understand and follow the rapid development of MarTech. This might be one of the reasons the different subcategories now have passionate people creating similar landscapes for a specific genre. For instance,



Privacy Tech is growing so rapidly that it already has over 1000 different recognised tools on its list that are maintained on [privacylandscape.alias.dev](https://privacylandscape.alias.dev) by Mehdi Medjaoui. There are probably other PrivacyTech-related lists maintained by other people as well, but for sure, it is a quickly emerging field in technology.

In the EU and many other countries around the globe, it is mandatory for anyone using cookies or other similar tracking mechanisms to have a Consent Management Platform (CMP) in place. A CMP is also known as a consent banner or a consent banner. It is a tool that is used to categorise, control and give users a choice to select which cookies they give consent to be used. There is a plenitude of CMP providers on the market that offer basic features to manage cookies.

The next step after implementing a CMP is to consider implementing a centralised consent management approach. This is usually called the single source of truth of a customer. This approach and tools have slightly different definitions depending on the company providing the technology. The two most common tools to consider are a Privacy Center and a Preference Center. Usually, they are slightly different by definition. In addition, a Customer Data Platform (CDP) is usually needed to collect, unify and activate the customer data.

Let us start by looking into Preference Centers. A Preference Center is a place where customers can see and manage their preferences straight from an interface themselves. These preferences changes depending on the company and the business they are in. Typical examples are marketing-related preferences such as from which channels, how often and what kind of marketing and sales communication customer wants to receive. These channels are typically email, push messages from mobile apps, SMS messages and telephone calls. Besides communication preferences, customer data preferences can be adjusted from the Preference Center. This is usually so-called zero-party data that enriches customer information. As an example, this can be the shoe size, the favourite colour, a preferred seat on an aeroplane and so on. Quite often in companies, this data resides in a CRM or a custom-built solution.

The definition of a Privacy Center often refers to a tool aimed more from a compliance point of view to handle privacy policy-related issues. With a Privacy Center, a company can control regulation-related communication to their customers with effective legislation depending on where around the world they are doing business in. A Privacy Center is the source where consent information is stored, and it serves as a repository for any party to control this information.

Some of the most significant benefits of centralised consent management are that it provides transparency for the customer, which usually means that they are more willing to

share data with companies. Another benefit is that many processes related to consent management can be automated and externalised for the customers to do the job. By utilising centralised consent management processes throughout its channels, a company ensures that all consent is always up to date and the customer receives messages when and where they so wish.

Even though privacy technology is a sub-category with its own tools, it still is quite a complex environment since the data that is processed often resides in many back-end and front-end systems and tools an organisation is using. Quite often, there is old legacy technology in place that is siloed and difficult to connect, as well as siloed data sources scattered all around the organisation.

#### **4.1.3 Design, UX & UI**

It is essential and, in many aspects, mandatory to apply legal and regulatory guidelines to design when it comes to how consent can be acquired. Today, we mainly talk about Consent Management Platforms (CMP) or consent banners as a more common term. For instance, in the EU and in Finland, the guidance is quite strictly telling how a consent banner should be designed, where it should be located on a website, what elements it must have and how it should function.

A cookie consent banner is usually the first thing a visitor, customer or prospect sees when encountering and interacting with a company. Therefore, it has a huge impact on how this is presented to the visitor and what kind of impression it gives. There are many elements to take into consideration and required to make it work. Some of them are visual, and some are not; they are more related to the tone of voice and feeling.

Transparency is a growing trend in everything related to privacy and personal data. This is especially important for the consent banner. The questions an organisation must answer and solve are, does the consent banner give the impression that the company can be trusted to handle the data in a trustworthy way? Does it comply with the regulation? Are the terms and ways of handling data explained and understandably?

What must be considered with the placement of the consent banner? Does it restrict the use of a site before a visitor has accepted, declined or made changes to cookie consent? Consider the implications of these choices and make what the regulation says about this. For instance, in Finland, the authority in the matter, Traficom, has clearly stated that a consent banner cannot block the use of a website even if the visitor has not made any changes to the settings. In practice, this means that the banner must be placed at the bottom of the page. Things to consider are what are the right design measures and communication

that maximise the amount of consent. Will most of the users decline consent if they are forced to decide before entering a website, or would more visitors be willing to give consent if it is not forced on them?

Another important aspect to remember is that there has to be an equal possibility to accept or decline with buttons for respective actions. Also, the placement and colouring of the buttons play an important role in how visitors give consent. Test and play with the colours, do not just stick to your brand colours but try out colours which are usually combined with consent, such as traffic light colours green and red.

What are the options to state trust with the text on a consent banner? What is the tone of voice that fits your customers to gain trust? How can the text and explanation be simplified? Evaluate what the value of the brand is and how the logo should be displayed. Can images build a feeling of sympathy and trust? Are there any certificates that could be used to indicate trust and transparency?

### **A/B test everything**

All of the previous thoughts, tips, ideas and open questions have to be A/B tested to see what works best for your company and customers. It should be an iterative and ongoing process to make sure that the consent is always maximised.

#### **4.1.4 Trust and ethics**

The debate about ethics and values around personal data is a growing topic that is on the agenda of many stakeholders and is a matter that is gaining traction all over the world. It is certain that there is no way of going back to the way companies could use personal consumer data basically any way they wished. Trust and transparency are values that upon trust is going to be built on and the way for companies to earn the trust to use some data in the future.

The questions to ask are, what is the company policy on data ethics? How do you build a trusting relationship with the customers, and how does a company communicate and especially show with actions that they also walk the talk? When it comes to something intimate such as personal data and the willingness to share this, trust will be one of the most important factors for any company.

#### **4.1.5 Insight and trends**

Gathering insight and trend-watching might first sound as insignificant. However, there are many quite complicated topics related to privacy, such as regulation and technology, as well as keeping up with changes in customer behaviour. It is precisely the nature of the complexity of the subject which makes it important to follow up and get an understanding of what is happening within privacy from various aspects and points of view. By getting the latest information and understanding early on the upcoming trends and insights, an organisation can make plans accordingly to respond to these upcoming changes. When it comes to technology, the processes can be quite extensive and, in many cases, take months or even years to complete. The same impact is applicable to any legislative changes. Monitoring changes in consumer behaviour helps a company to understand what is bubbling under and react to those changes in due time.

All of these changes can have a considerable impact on current business use cases that are dependent on present technology and processes.

#### **4.1.6 Business, processes and strategy**

Under business, processes and strategy, there are many elements from the other toolkit areas that closely touch.

The privacy-related processes companies must set up and follow around regulation, changes in user behaviour, development of privacy technology and the needed skills in the organisation to successfully manage all of this.

Risk management is one of the most important factors when it comes to customer data. There are different topics under risk management to take into consideration. Due to the nature of the thesis, the focus here is on privacy, not data security, which is an adjacent and important topic, but too large to be included as a part of this thesis or framework. It is also easier for many organisations to approach the topic of consent and privacy more from a business needs perspective than an IT perspective, where data security usually falls on.

#### **Regulation**

Companies must understand how and where they do business and what regulations they have to apply locally. For European companies being compliant with the Shrems II ruling is important and something to carefully evaluate when selecting any technology where Personally Identifiable Information (PII) data is being used. The risk lies in that the data must not be in any danger of being accessed by foreign and especially US surveillance authorities. Other countries have similar privacy legislation to take into consideration if a

company is present in another market, but the regulation is still different and therefore, the same processes, especially when it comes to consent, cannot be applied globally. A lot of regulation around the world and in the EU is developing all the time, and it is developing at a fast pace which requires constant monitoring.

Besides needing the right kind of knowledge to understand the regulation, this is where technology can help to maintain this process. Privacy Centers are tools aimed at organisations to control and apply these regulations and help organisations to choose which privacy regulations to follow and apply locally for visitors. Also, proof of consent can be shown from these tools showing when users have approved or declined consent. These processes should be applied transparently so that users can access their information from an interface showing all their history.

This is a process that has to be mandated for someone to follow regularly. The scene for this is getting more complex the whole time, and not following the regulation can have serious business impacts in terms of high penalties and public damage to the reputation of the company. The latter is often something that companies cannot control themselves once something is out in the media channels – no matter if it is true or not.

Usually, this is something that belongs to the compliance and legal teams. A typical position to lead this is a Data Protection Officer (DPO).

### **Marketing technology, architecture customer touchpoints**

As we know, technology is developing at an incremental speed and especially in the field of marketing technology (MarTech). Privacy technology can be categorised as a subfield of MarTech, and it is also growing very fast at the moment. Customer data is everywhere, and the amount of this is growing significantly. On top of this, there is a multitude of customer touchpoint channels where customer data is handled.

When the technology and customer data sources are growing the whole time, also the complexity and the risks are growing at the same pace. This requires a deep understanding of technology, data and marketing channels in order to ensure that customer data is handled with the right privacy regulations and principles. Every time a new technology, data source or channel is taken into use, it must be ensured by the DPO or equivalent position that the privacy issues are taken into consideration.

### **Privacy skills and education**

People in an organisation should get obligatory basic education about privacy. In addition, there are many certificates that can be applied to ensure that an organisation is compliant

with privacy from different perspectives. There are ISO certificates, such as ISO 27701, and there are certifications for the personnel to take. The IAPP certifications are amongst the most well-known and respected. They have several focus areas for different needs, such as privacy processes in an organisation or privacy technology.

### Business impact assessment

Besides privacy and security-related processes, as well as a technology-focused approach to privacy, in an organisation, quite often a forgotten aspect is the business impact it might impose. Since customer data cannot be used as it was allowed before due to tightening regulations, change in customer behaviour and security risks, it will have an impact on a lot of use cases. This might have a negative impact on revenue if there is not a wide enough understanding in all parts of the organisation about this. Here it is crucial all stakeholders from marketing, sales, IT, legal, compliance and upper management understand the big picture and how these issues affect each other and, in the end, the business use cases. It will require a new kind of approach and, in some cases, even a new set up of use cases to be built since the old way of doing things is not just possible anymore from a legal or fairness aspect.

### 4.2 Technology architecture

The technology around marketing is evolving very rapidly. A subsection of MarTech is privacy technology, which is a rather new category and evolving very fast as well. To understand the needs and requirements of privacy-related technology, it is important to understand some concepts around this and what drives the need for different technology needs.

I developed a conceptual framework around topics that is good to understand before starting to evaluate and implementing the necessary technology.

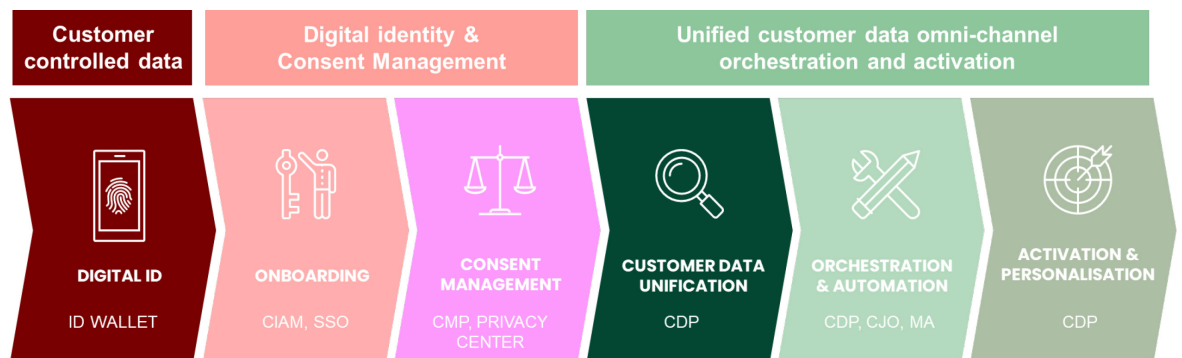


Figure 3. Conceptual framework

The framework consists of three main categories divided into six subcategories. The main categories are: Customer controlled data, Digital identity and Consent Management and Unified customer data omnichannel orchestration and activation.

#### **4.2.1 Customer controlled data**

Customer-controlled data is a category for solutions where the customer will manage their own data in different systems, usually called Digital IDs or Digital Wallets. There are many different initiatives around this topic. Some are state and government initiatives such as the EU-wide EUiD. Many states have their own initiatives that are quite new, and in many countries, these are on their way. In addition to the government initiatives, there are many private initiatives that are either up and running or about to start.

The idea is that a regular person gets their digital ID, where they can store their data and then decide whom to share it with. For instance, specific data has to be shared with governmental authorities, such as tax-related information. Then there is personal data, such as address information which can be shared with companies when needed or commercially orientated data, such as preferences where the consumer has the choice to decide with whom to share this information.

This is a relatively new concept and still evolving, and, in my opinion, it will take some years before it is a reality for consumers and companies. However, it is an interesting and important aspect to keep an eye on.

#### **4.2.2 Digital identity and Consent Management**

Under Digital identity and Consent Management, there are two areas: Onboarding and Consent Management.

Onboarding will be an important factor in the near future when there have to be several options to get customers to sign up for services. This is due to the fact that after the third-party data is going to eventually disappears, companies have to focus on first-party data, which is data where the customer is known and identified somehow. It is optional in every situation to use strong identification methods such as sign-up with banking logins. Only some people want to sign in with their Facebook or Google accounts but something else they might already use and prefer to use.

Consent Management is the process where a consumer uses tools like a CMP or a Privacy Center and a Preference Center to control what kind of consent they will give to companies. These are tools that companies control, but the customers have an interface where they can make individual choices.

### 4.2.3 Unified customer data omni-channel orchestration and activation

It is a paradox that now there is so-called out-of-the-box technology that is available for all companies to use when it comes to collecting customer data from various sources. This is a tool called a Customer Data Platform (CDP). It is built for marketers so that they can build audiences and segments using data from various sources, such as back-end systems and from different customer touchpoints. This data can then be activated in real-time to show personalised content to consumers. The paradox lies within that even though it is easier than ever to unify customer data, at the same time, it is getting harder than ever to get permission to use it.

However, once the consent has been received as described in the previous phases with the help of a CDP, the data can be transformed into meaningful insight, and customers can receive relevant and personalised information along the customer journey.

Important tools and processes alongside a CDP are automation and customer journey orchestration. These features overlap with different MarTech tools from different vendors, and it is essential to find the right fit for the MarTech stack to function optimally.

### 4.2.4 Technology architecture – Customer Data & PrivacyTech

A CDP is the centralised hub where all the customer data gets connected for different use cases and purposes.

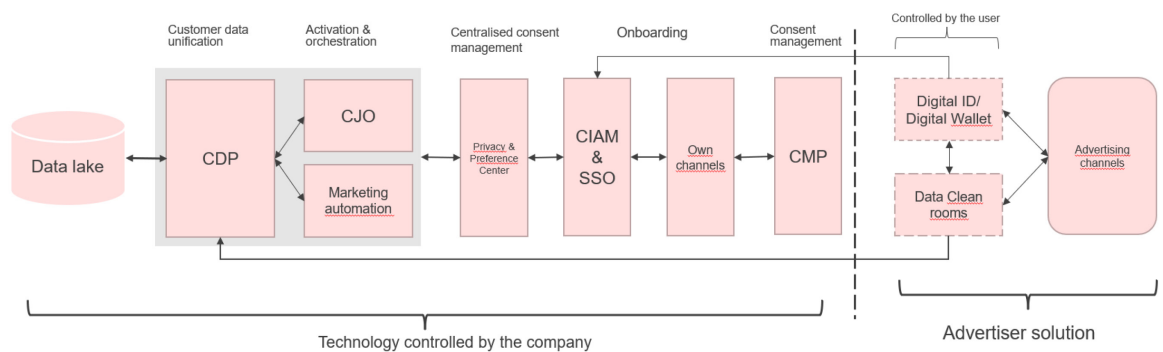


Figure 4. Privacy technology architecture

#### Onboarding

The technologies used here are meant for sign-up and sign-in processes depending on the stage where the customer is at. The most well-known technologies are Customer Interface Access Management (CIAM) and Single Sign-On (SSO).

#### Consent Management



Consent management is a newer technology category where there is happening quite a lot of development currently, especially with Privacy Centers and Preference Centers. Consent Management Platforms (CMP) or more familiarly known as cookie consent banners are the most well-known and adopted of this technology.

### **Data lake**

Data lakes or data warehouses represent here the various back-end data sources a company has. Usually, applications are CRMs, ERPs and other data systems either on-premises or as SaaS implementations in the cloud. It is not that unusual that rogue excel-sheets are used in companies to handle data. Therefore, a comprehensive data strategy is recommended for the data needs.

### **Customer data unification**

A CDP is nowadays the go-to tool for unifying customer data into meaningful entities. CDP type of functionality has been done and can be done with custom solutions utilising technology such as Snowflake. The problem usually with custom solutions is very heavy development and maintenance costs, whereas, with so-called out-of-the-box solutions such as CDPs, the technology is developed for this specific purpose and can be taken into use faster and is usually more affordable. CDPs today come with a wide variety of ready-made APIs for easy connection to other tools and technology.

There are plenty of different CDPs on the market today, which brings a huge variety into the functionality of the CDP tools and overlapping features with other marketing technology that can already be in use in companies.

### **Activation and orchestration**

Marketing automation is typically the tool that most companies already have, at least for email marketing automation. Customer Journey Orchestration (CJO) is another quite new MarTech abbreviation to learn. It is a tool made to create journeys through different channels based on predetermined triggers and activities based on use cases. A typical marketing approach for this use is the Next Best Action (NBA) use case scenarios.

But, as mentioned before, this is technology is overlapping strongly and is doing so the more the different technology companies are developing their tools and platforms.

### **Own channels**

Own channels are the traditional channels companies have such as web sites and services, mobile applications, chats and customer service. In other words, channels where the company has control themselves how to run and develop them.

### **Digital ID's and Digital Wallets**

Digital IDs and Digital Wallets are being actively developed from various starting points. There are governmental, private, and commercial initiatives, and only time will tell which ones are going to succeed and gain traction. It will most likely be a combination of what consumers want to use and which tools are technically the easiest to implement.

### **Data Clean Rooms and Advertising solutions**

From the advertiser side, a solution to tackle the disappearance of the third-party cookie is Data Clean Rooms. This is also quite new technology, but some of these types of solutions are already up and running. The Data Clean Rooms works as a hub where segmented first-party customer data from a company gets connected to audience data from the advertiser side. The data which is connected in the Data Clean Room should be anonymous, and the advertiser will not know the identity of the person targeted.

### **4.3 Consent design & research**

This is one of the three parts in the Consent and Privacy framework concept. It will be more and more important to consider how consent is presented and asked from the consumers. The regulation tightens its grip on how consent must be acquired, and it is easier than ever to decline companies to use your data. This is where the design comes into the picture in all of its forms. By utilising service design and a customer-centric approach to solve things, it could be possible to enhance the possibility that more consumers would give consent and, thus, better operational opportunities for companies. Factors and outcomes from the design process understand what the consumers see things and what they would prefer. Based on this understanding, the layout of the consent banner can be optimised to see what converts the best. How should the text explaining the use of data be written, and what other factors should be considered, such as the brand image or different types of certificates? It is essential to remind that it is, in many cases, forbidden to use deceptive design methods to trick the user into giving consent. This is also not a customer-centric approach that builds trust between the company and the consumer in the long run and can backfire, resulting in the consumers going over to a competitor who has a transparent and trustworthy attitude towards how privacy should be handled.

It is quite obvious that the process of giving consent today is not user-friendly and is frustrating the user even though the idea behind it is good and for the users' benefit. It is also a difficult process for the companies to handle and is affecting marketing and business efforts.

#### **4.3.1 Service design and the Double Diamond process**

For the research phase, I decided to use the Double Diamond process. In service design, the double diamond is a widely used process to visually display the four different design phases. The first diamond consists of the discovery and defined phases. The first phase is the discovery phase, where the aim is to understand what the problem is by speaking and interviewing people. The second phase is about defining the collected insight into a new view and perspective on the topic. The second diamond consists of the development and delivery phases. The development phase is about finding inspiration and different and new views about the topic at hand. The fourth and last part in the double diamond is the delivery phase is about testing different solutions and prototypes to find improved solutions that work.

#### **4.3.2 The research process**

When it comes to ePrivacy and consent, today, the first encounter in most cases is the consent banner on a website where a user is stopped and has to make a selection of what kind of consent to give before entering the website. Even though it might sound like a simple thing, it is actually quite a complex issue. There is a multitude of tools available that use cookies that require categorisation. There are worldwide over 100 different privacy laws that are somehow guiding how to do this; the most well-known is the EU GDPR and the ePrivacy directive, and the upcoming ePrivacy regulation. In the EU, each member state can apply their own interpretations of the ePrivacy directive. In addition to this, there are many ways how to design a consent banner with buttons, colours, text and position on a website, just to mention a few variables. More detailed explanations of privacy policies have to be squeezed in somewhere.

All of this makes the design process of cookie consent quite hard to control, and the UI and UX design is often forgotten.

In my thesis work, I am going to focus on how to optimise the cookie consent but with fairness and transparency principles taken into consideration. To point out is to create designs that build trust in users instead of utilising dark pattern design where the user is usually tricked into making selections that grant the website owner as many rights as possible.

In my work, the main focus is on the EU regulation and interpretations of the Finnish authority in the matter of Traficom (The Finnish Transport and Communications Agency). It is considered that Traficom has generally made stricter interpretations than, on average, in Europe. Therefore, it is more interesting to reflect on the work against how to apply the design work in a more difficult environment. The result will be easier to implement with use cases and lighter interpretations of cookie regulatory.

### **4.3.3 Quantitative questionnaire**

The purpose of the qualitative phase was to get a deeper insight into basic issues when dealing with sharing customer data and especially in the context of using cookie consent banners. This was conducted as a questionnaire with 24 questions (Appendix 1).

The questionnaire was aimed at the personnel at Dagmar. It was discussed if there is a risk of bias because Dagmar is a digital agency where it is presumed that more people are, in general, aware of cookies, data and what is happening around this topic. However, after thinking about it and discussing this idea with other thesis stakeholders for a while, I considered that it could be beneficial for the research if the people were more aware of the topic. This is based on the assumption that the vast majority of regular consumers are not aware of the topic yet. Because of this, the questionnaire would give the study more usable answers on base assumptions. Also, this most likely allowed the take to be smaller to get usable results for the study and especially what is needed for the quantitative phase.

### **4.3.4 Findings**

All the visual graphs and analysis of the questionnaire are in Appendix 1.

#### **Background**

The questionnaire was sent out to the whole personnel of Dagmar. Out of 255 who received the questionnaire 56 answered which gives a response rate of 22 % out of the total amount. For a questionnaire of this kind of complexity and without any personal incentives this can be considered as a good result. The respondents were in four age groups between 18-54, out of those 60% were female and 38% male and 2% chose not to say.

#### **People want to control their data but are lazy in taking actions**

71% of respondents have some kind of an idea what cookies are used for and 27% understands more in detail what cookies are used for. In total only 2% of the respondents did not have any kind of an idea what cookies are used for. People want to have more control over their data, but they are not prepared to make choices every time with consent banners as they are displayed today. About 10% always adjust or declines cookie settings.

Up to 67% adjust cookies sometimes and up to 24% never adjust anything but gives consent to all cookies. 26% would like to but find it too time consuming. **87% believes that themselves should control their own data.** 13% would trust authorities and governments. 0% would trust companies to control their data. 76% of the respondents believe is necessary to set boundaries how personal data can be used. 16% believe that the current regulation in the EU is enough. 6% think there should be less regulation on personal data. 2% do not understand what their data right are.

### **Poor consent design makes users consider if a web site is untrustworthy**

71% of users have stopped from using a website because of a poorly designed consent banner but 56% have entered a website because of a misleading or untrustworthy consent banner. If a website doesn't have a consent banner 73% would consider it suspicious but 47% would continue using the website. 33% would use a website without a cookie banner and 67% would use a website without a consent banner if it is a brand they trust.

### **Personalisation trackers should be based on explicit consent**

40% would approve to be tracked on a website with analytics cookies and 27% if it would be completely anonymous. 24% states that they don't fully understand how their data would be used. People tend to be stricter when it comes to personalisation because only 20% would not mind but 40% would be ok only if they have given explicit consent to be targeted. 31% would like to know how from the company how their data would be used for personalisation. Only around 7% would never give consent to analytics or personalisation cookies.

### **Brand trust is an important factor when users are willing to share data**

Only 13% would never give consent if they would not know how their data would be used. 26% would always give consent. 62% could consider giving consent if they would trust the company or the brand. 40% are moderately concerned how companies are using their personal data. 40% are a little bit concerned and 13% are not concerned at all. Only 7% are very concerned. 84% of the respondents only trust that some companies are using their data responsibly. 9% trusts that their data is always safe and 7% never trust that their data is safe. **A well-known brand would be the largest driver for users to trust companies, 73% would give consent.** 67% would trust a company if it would be as easy to decline consent as it is easy to give consent. Transparency in informing about how the data is used was also highly rated up to 60%. The type of industry plays a significant role where users would trust to give their consent. Banking & insurance was trusted up to 77%, public services up to 58% and health up to 31%. Fashion had the lowest trust rate with 2%.

## **Meaningful insight and personalisation from user data increases consent willingness**

80% of users would give consent if the data would be used to create meaningful insight and get 78% to get personalised services. Monetary benefits weren't as important but still valued up to 64%. 11% would not be concerned and would share the data freely. It was quite clear that user wants to have control over their data themselves with 85% of the respondents.

## **Consent banner can be a hinder when entering a web site**

26% of the respondents think that is not easy to continue to a website without giving consent to all cookies. 60% say that it is difficult sometimes and 14% thinks it is always easy. 51% of users believe they can sometimes use a website without giving consent to cookies, 25% say that they can use a website without making any cookie selections. 24% say that they cannot use a website without making choices. 34% of users continue to a website even though they could not decline non-necessary cookies, 13% would never use a website where they could not decline cookies and 53% would use such a website sometimes.

### **4.3.5 Conclusions**

It is quite clear that people want to have control over their own data, and they wish that there is also strong support from governmental legislation to drive the change. People do not really trust companies to handle their personal data. Banking and financial institutions and public services were trusted as data operators.

As in many studies before, that data shows here as well that there is a slight paradox in what people say and what they do in practice. Even though people want to have control over their data, they still tend to give companies access to it quite freely. However, the trend seems to be that people are more aware of how their data is used, although they are fatigued to make the needed effort every time, they have to react to a consent banner.

### **4.3.6 Qualitative research and design thinking process**

Based on the findings in the qualitative questionnaire and insight gained through theory and findings through experience with real customer work, I used the double diamond from the design thinking process to approach the problem and created prototypes to find out what kind of factors would give the user to give consent when using a consent banner.

In design thinking, the double diamond is a widely used process to display the four different design phases visually. The first phase is the problem discovery phase which consisted of the interviews where I framed and explained the purpose of the phase and showed over 20 different consent banner designs to the interviewees. In the second problem definition

phase, I analysed the findings from the interviews and created a list of conclusions. In the third solution discovery phase, I created prototype wireframes based on the conclusions. In the second and third phases, I summarised the findings from the interviews and made conclusions to receive compromised end results. In the fourth concept validation phase, I shoved the prototype wireframes to the interviewees again and asked for their validation again. These prototypes are the ones that would go to implementation with proper brand design elements.

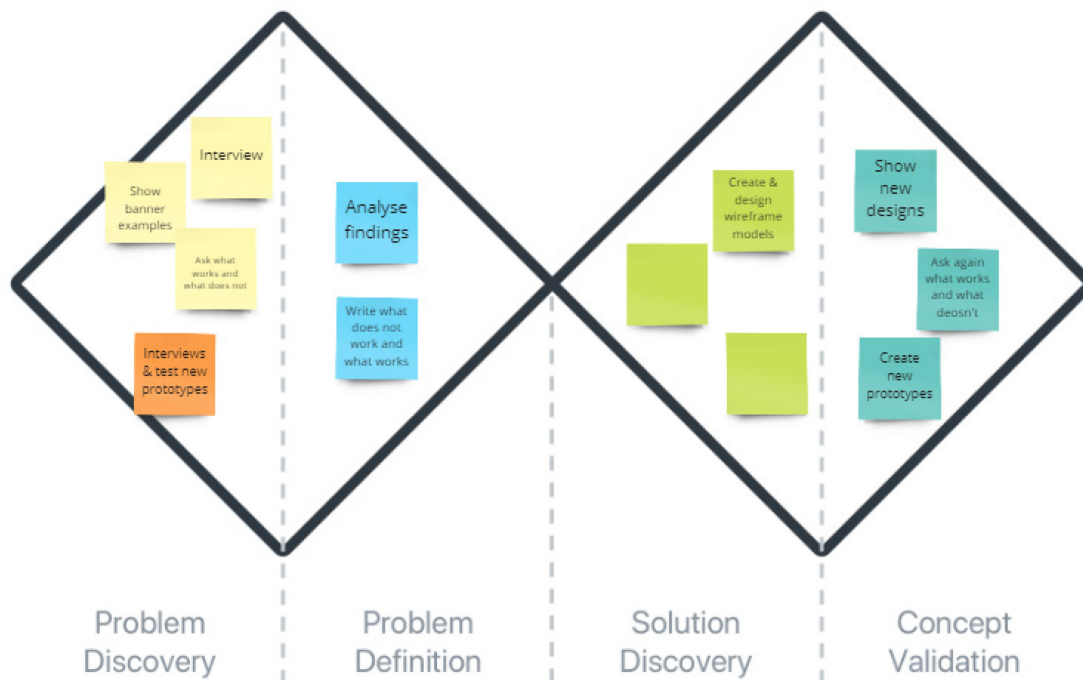


Figure 5. A Miro board screen print from the design process.

#### 4.3.7 Interviews

I conducted five separate interviews all together and four interviews with people who also participated in the questionnaire. One interview I conducted with a person who did not participate in the questionnaire but had an understanding of the consent topic. This was because I wanted to compare and validate the interview results with a so-called external variable. In the end, it did not have much deviance from the other interviewees who participated in the questionnaire from Dagmar. The interviewees had various views and levels of knowledge on the topic. The questionnaire, they said that it forced them to consider their own behaviour when confronting consent banners. However, they said that it still has not changed their behaviour much with how they interact with consent banners today.

The interviews lasted from approximately 45 to 60 minutes each. There were two women and three men who participated. The interviewees' age category was from 20 – 54 years.

For the first phase of the interviews, I showed them over 20 different consent banners (Appendix 4) and asked them to spontaneously tell what they thought about them. I gave them some thoughts in advance to consider in front of each banner; they were topics such as does the consent banner create trust, whether it is quick and easy to understand, whether it is functional, and how they would interact with the consent banner. In the latter part of the interview, I showed them examples where the focus was on evaluating the effect of colouring, images, and headlines in consent banner design.

During the interviews, I took notes and made a conclusion after the interview. It was based on this material; I created several prototype wireframes for the next phase of the concept validation.

The interview process I displayed in Appendix 4.

#### **4.3.8 Wireframes and prototypes**

The wireframes and prototypes are meant to serve as a starting point when creating new consent banner designs based on evaluated and tested research and understanding. Based on the findings from the interviews with consent banner examples, I created a set of 11 wireframe prototypes. I showed these to three interviewees, two of whom had participated in all the previous phases. One interviewee didn't participate in the previous phase because I again wanted to validate an unbiased view of the designs.

All the prototypes had common elements, which somehow came up more frequently in the first round of interviews. In the designs, I played with slightly different variations. Some had text fields presenting detailed information about what a certain selection means, some had different styling of selection elements, and some had images. All of the prototype designs are in the Appendix 5.



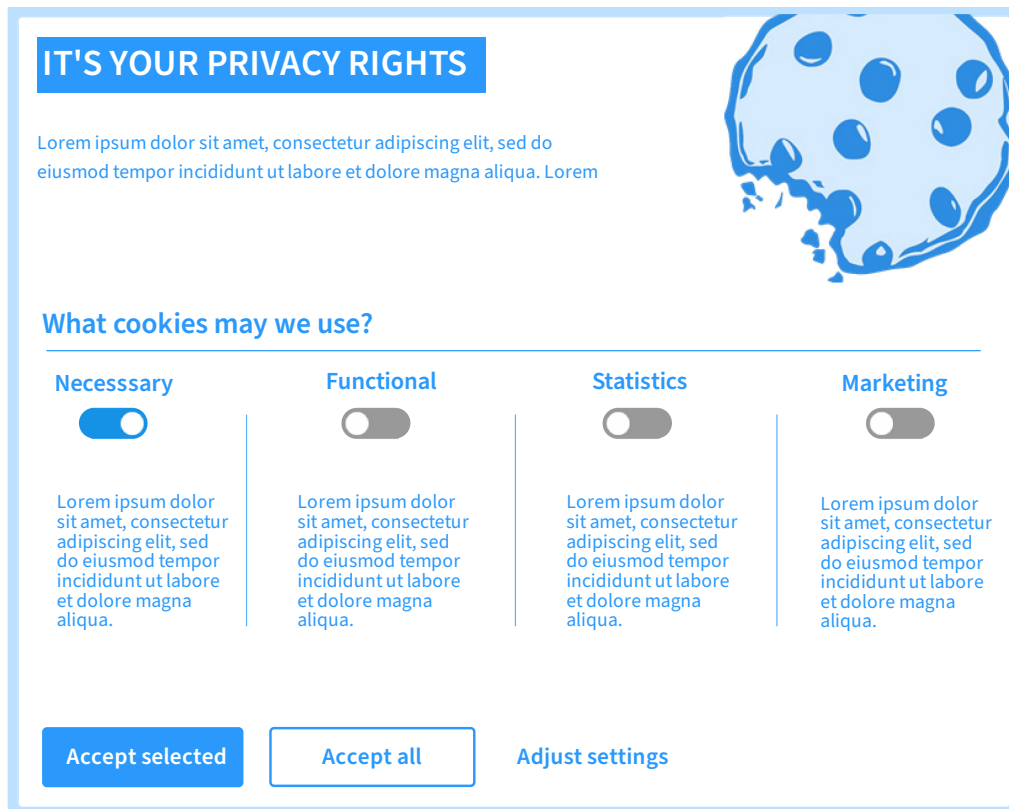


Figure 6. Consent banner from iteration round one

#### 4.3.9 Findings

Based on the feedback of the prototype designs, I created in the next phase four new wireframe models of consent banners with various options. Maybe one of the biggest findings affecting the design was in relation to the Finnish authority Traficom's guidelines, where the consent banner should not prevent a user from using a website even though they have not made any selections. In practice, this means that the consent banner has to be placed at the bottom of a website. Otherwise, the comments were with minor detail changes, e.g. the pictures were changed for a logo to create more trust. It came out in both the first phase interview and prototype session that, in general images are endorsed to be used because it shows that the company has put some thought and effort into the banner. A brand logo was considered something to be trusted.

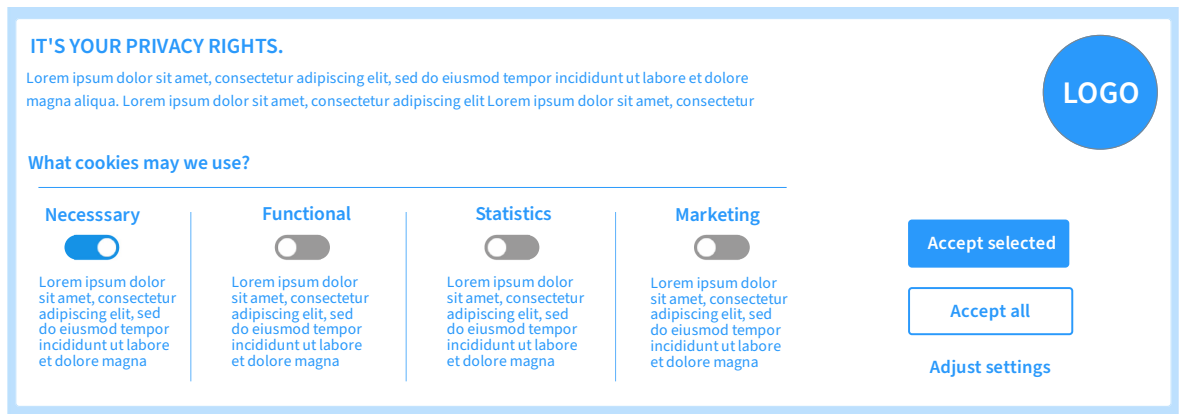


Figure 7. Consent banner from second iteration round

#### 4.3.10 Conclusions

The results of the questionnaire and interviews show quite clearly the same trends as from several other studies that people do wish and expect that their privacy will be respected and the users themselves would have control over their data. However, currently, it is too cumbersome and time-consuming to do this repeatedly when visiting a website or a digital service.

Even though some of the respondents from the questionnaire and the interviews said that they are not happy with making consent selections every time they visit a website and find this annoying and even intrusive, companies have to follow regulation that forces them to implement a consent mechanism. One large problem is that these consent banners and the mechanisms they use vary from one execution to the other and make it, therefore, difficult for users to adopt a common way of reacting to them. Instead, users have to stop too often and consider how to make choices and changes to consent and privacy settings. What is lacking is a common standard. Because of this, users are fatigued, and the majority are just proceeding with giving consent. Before we get to a state where there could be a standard applied to how consent is designed, the regulation should be stricter in stating that the default consent that is emphasised should be the selection where a user can decline all consent except for the necessary. This is, of course, not what the businesses want, but when it comes to evaluating the importance of the privacy rights of the individual or the rights of all the companies getting open hands in utilising personal data, the emphasis must be set on behalf of the individual user.

Another conclusion is that the consent design process has to be an iterative process that is most preferably under constant A/B testing. This is mainly due to the fact that there are many factors affecting what has to be taken into consideration in the consent touchpoint. As mentioned so often, these are changes in regulation, user behaviour and changes in technology. Also, making too drastic changes in how to ask for consent from users could

lead to confusion and affect the consent process negatively. Even though there are not all too common and clear standards on how consent is supposed to be acquired, it usually still follows a certain type of similar pattern.

In the service design interview phase, it was quite a clear message from all the respondents that even though all of them don't care that much about their privacy consent preferences and just want to continue as quickly and easily to the website, they still prefer a transparent way of displaying the different consent buttons because it builds trust. This means, in practise, that it is not indifferent from a user perspective how consent is designed and presented. It showcases that even though the customers might approve of all consent cookies consent, they still prefer that companies design and display the consent in a way that provides a sense of trust.

## 5 Evaluation of research

The outcome of this work consists of three elements. The consent and privacy toolkit is a collection of different topics and elements recognised needed to run a successful consent and privacy strategy at any company. The second element is an explanation of the most relevant tools and a technology architecture focused on privacy technology and how that is related to current technology in companies. The third element consists of research where customer opinions are evaluated through a questionnaire and a design phase with in-depth interviews and prototypes of a consent banner.

In my thesis work, I tried to answer a real need we have discovered at Dagmar when working with clients. We have seen the clients struggle with all the topics covered in this thesis. The issues covered in the thesis are very complex and hard to understand, and it is not easy to connect all the dots and draw the big picture, even for a seasoned expert.

When I have been discussing my thesis work at Dagmar, it has been seen as important and valuable, especially for the changes coming up within the next one to three years. We have recognised many new opportunities and services Dagmar can start supporting its clients with, both short and long-term.

I answered the research questions quite well, especially with the questionnaire in the quantitative phase. Also, the interview phase with prototyping brought valuable insight into how a consent banner should be designed with the realities of today, especially in the double diamond process itself. I am sure this will prove to be an essential experience and skill now that companies want to validate and customise their consent banners to stand out from the competition and make consent design into a competitive advantage.

The consent and privacy toolkit was a huge undertaking, and it was quite difficult to narrow it down so it would not become too bloated with topics no one could possibly cover. However, it was seen as valuable at Dagmar to have an understanding of what kind of themes and topics there are and especially how they are interconnected. The toolkit is the part of the thesis work that will require more consideration on how to help companies to pick out the themes and topics that are relevant to them.

I was sometimes struggling with the thought that the thesis topic was too large, but I was reminded that this is a topic that has a real need and should somehow be addressed or at least tried to be investigated if it can be done to this extent.

The thesis work is firmly based on a real need, feedback, and experience from client work; therefore, I am confident that many of the elements can be used and further developed when offering consent, privacy design and technology-related work for clients.

As mentioned so often, the topic of the work is new and quite complex, and therefore it took much work to keep a red line through the work so it would bloat up into something too large and intangible in the end. The theory part was perhaps the easiest in the work. Even though the research phase with the questionnaire, with all of its preparation, analysis, interviews and prototyping, was very time-consuming, it was the part which gave me the most satisfaction and learning. It was great to see that customer-centric approaches bring valuable insight, and this can be taken into something tangible to be developed further and iterated eventually into a real product or a service.

## 6 Conclusion

The concept of personal digital data is very complex and has many aspects to consider. Data is something intangible, it does not have any clear country borders, and in the end, it is quite a new concept to most of us.

Most people want to have control over their own data instead of letting companies decide how their data is used. However, the behaviour is often in contradiction to what people say. This type of behaviour is called the privacy paradox.

People are experiencing consent fatigue because of the process, which in the EU is based on regulation, and it is necessary to give consent almost every time one enters a web service of some kind. In most cases, consent is asked in a way that is different each time and requires the user to stop for a moment to consider what choices to make. As we know, the digital user today does not want to stop and take any extra time at all for any additional hindrances before entering a website or a service. No wonder the majority are taking the most effortless approach when granting consent, especially since many companies are not giving the user an easy and straightforward way to object to non-necessary cookies. On top of the consent, users often have to push through long conditions and terms documents. I argue that consent fatigue is one major factor in the privacy paradox.

It is necessary to impose regulations on how our data can be used and who owns it. However, it seems that the regulation is not enough to make the change happen in our behaviour with consent. We need technology to make it easy to adjust consent only once in a centralised data repository where people control what data access, they give to different data receivers. For this kind of consent sharing across platforms and technology to work, we need universal standards. Otherwise, we will be in a consent mess situation. There is a real need for universal consent, but it seems that this is still years away from getting realised. There are too many different laws around the world, and many of these laws are still being constructed as we have seen in the EU that these can take a long before they are validated and set into execution. Privacy technology is still new and developing at a fast speed. Most of the digital ID and digital wallet solutions are still being built up, and there are too many different solutions around. None has yet taken a clear place as a winner.

The largest players on the market, such as Meta, Google, Microsoft, Amazon, and Apple, who have almost a monopoly situation on our data, are not willing to let go of their business opportunities easily since their business models rely heavily on user data. Fighting this monopoly status is one of the most important arguments for heavy regulation of personal data on behalf of the user.

## **Corporate data responsibility and sustainability**

Besides traditional sustainability programs where sustainability is monitored from more traditional fields such as supply chains, companies must consider adding sustainable data programs to their sustainability repertoire to show consumers that they do take privacy-related issues seriously.

### **The future**

The topics to consider in the future in regard to privacy issues is new emerging technology such as blockchain technology, IoT, AI-powered algorithms, facial recognition, virtual reality, still social media and healthcare-related technology.

My own opinion, with the current facts at hand, is that this is the beginning of the next step in the evolution of the internet in regard to customer data. I would argue that this is a part of web 3.0, where blockchain is becoming a crucial part of securing and validating the information on the internet. The same is going to eventually happen with individuals' private data. Eventually, we users can control and decide when, how and with whom we want to share our data. Companies have to come up with and develop services that are interesting and beneficial enough so that customers are willing to share their data. I believe that the digital IDs, digital wallets and data vaults which customers can use to connect with different services and share the data that people find relevant sharing will be the sustainable way to go. The end goal should be transparent and equal for all parties involved. There will be a time of transformation where especially advertisers and some companies will struggle, but in the long run, this will create new business opportunities for the old businesses and open new innovative businesses.

### **Closing words**

I believe that we, the users, should be able to decide about our own data, who can use it, and how and where it can be used. There are, of course, exceptions, for instance, with governmental instances where we all need to share specific data, such as tax-related information, but even the authorities should not need to know everything about us. A lot of the data is our private and personal data and ours to share if we want to. I also believe that it should be made more accessible for us consumers to share data with companies that should also be able to drive profitable business. The consent management process has to be solved to be less intrusive with common standards. It should be a balanced act between the functionality of a service and the fair use of only relevant data.

## References

- A European Strategy for data | Shaping Europe's digital future.* (n.d.). Retrieved 27 November 2022, from <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>
- Arrieta Ibarra, I., Goff, L., Jiménez Hernández, D., Lanier, J., & Weyl, E. G. (2018, February 21). *Should we treat data as labor? Let's open up the discussion.* <https://www.brookings.edu/blog/techtank/2018/02/21/should-we-treat-data-as-labor-lets-open-up-the-discussion/>
- Auty, C., & de La Lama, A. (2022, January 26). *2023 here we come: How to prepare your privacy program.* <https://iapp.org/news/a/2023-here-we-come-how-to-prepare-your-privacy-program/>
- Barday, K., & Klasovec Kingsmill, S. (2021). *Privacy technology: What's next? The evolution of data-privacy technology in the age of automation.*
- Bella, K. (2021, December 15). *How to overcome mistrust of data | World Economic Forum.* <https://www.weforum.org/agenda/2021/12/how-to-overcome-mistrust-of-data/>
- #BrandsGetReal: Social media & the evolution of transparency | Sprout Social.* (n.d.). Retrieved 19 October 2022, from <https://sproutsocial.com/insights/data/social-media-transparency/>
- Brown, B. (2001). *Studying the Internet Experience.*
- Burgess, M. (2022). *What is GDPR? The summary guide to GDPR compliance in the UK | WIRED UK.* <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>
- Cavoukian, A. (n.d.). *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices.*
- cisco-consumer-privacy-survey-2022.* (n.d.).
- Common European Data Spaces – Real-time Linked Dataspaces.* (n.d.). Retrieved 16 November 2022, from <http://dataspaces.info/common-european-data-spaces/#page-content>
- Cookies: I looked at 50 well-known websites and most are gathering our data illegally.* (n.d.). Retrieved 23 October 2022, from <https://theconversation.com/cookies-i-looked-at-50-well-known-websites-and-most-are-gathering-our-data-illegally-176203>



- Corporate data responsibility - Bridging the consumer trust gap.* (2021).
- Deceptive Design - user interfaces crafted to trick you.* (n.d.). Retrieved 27 November 2022, from <https://www.deceptive.design/>
- Digital identities in 2022 | DW Observatory.* (n.d.). Retrieved 26 November 2022, from <https://dig.watch/topics/digital-identities>
- Digital Markets Act: Ensuring fair and open digital markets.* (2022, October 31). [https://ec.europa.eu/commission/presscorner/detail/en/QANDA\\_20\\_2349](https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349)
- Dresch, A., Lacerda, D. P., & Antunes Jr, J. A. V. (2015). *Design Science Research*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-07374-3>
- EU Data Initiatives in Context.* (n.d.).
- European Digital Identity | European Commission.* (n.d.). Retrieved 26 November 2022, from [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en)
- Fair Data Economy - Sitra.* (n.d.). Retrieved 20 October 2022, from <https://www.sitra.fi/en/themes/fair-data-economy/#what-is-it-about>
- Gaia-X Finland - Sitra.* (n.d.). Retrieved 20 October 2022, from <https://www.sitra.fi/en/topics/gaia-x-finland/>
- Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, 226–261. <https://doi.org/10.1016/J.COSE.2018.04.002>
- Green, S. (2012, December 10). *Data as a human right | World Economic Forum.* <https://www.weforum.org/agenda/2012/12/data-as-a-human-right/>
- Home - Gaia-X: A Federated Secure Data Infrastructure.* (n.d.). Retrieved 20 October 2022, from <https://gaia-x.eu/>
- Howard Beales, J., & Stivers, A. (2022). *An Information Economy Without Data.*
- IBM Study: C-Suite Leaders Who Value Trust in Data are Positioned to Outperform Peers - Nov 12, 2019.* (2019, November 12). <https://newsroom.ibm.com/2019-11-12-IBM-Study-C-Suite-Leaders-Who-Value-Trust-in-Data-are-Positioned-to-Outperform-Peers>

- International Association of Privacy Professionals*. (n.d.). Retrieved 23 October 2022, from <https://iapp.org/>
- Katainen, J. (2022, July 21). *The fair data economy of the future is here – How do we seize the opportunities today?* - Sitra. <https://www.sitra.fi/en/articles/the-fair-data-economy-of-the-future-is-here-how-do-we-seize-the-opportunities-today/>
- Klasovec Kingsmill, S., & Barday, K. (2021). *Privacy technology: What's next? The evolution of data-privacy technology in the age of automation*. <https://home.kpmg/xx/en/home/insights/2021/05/privacy-technology-whats-next.html>
- Koivisto, M., Säynäjäkangas, J., & Forsberg, S. (2019). *Palvelumuotoilun bisneskirja*. Alma Talent.
- Leslie K. John. (2018, September 18). *Uninformed Consent*. Harvard Business Review. <https://hbr.org/2018/09/uninformed-consent>
- Lomas, N. (2022, January 10). *Cookie consent tools are being used to undermine EU privacy rules, study suggests* | TechCrunch. <https://techcrunch.com/2020/01/10/cookie-consent-tools-are-being-used-to-undermine-eu-privacy-rules-study-suggests/>
- Miettinen, S., & Koivisto, M. (2009). *Designing Services with Innovative Methods*. Kuopio Academy of Design.
- Morey, T., Forbath, T., & Schoop, A. (2015, May). *Customer Data: Designing for Transparency and Trust*. <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>
- Orson, L., & Stein, S. (2020). *The new imperative for corporate data responsibility*.
- Panetta, K. (2021, October 21). *Gartner - The Top 8 Cybersecurity Predictions for 2021-2022*. <https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022>
- Parker, P. (2022, June 1). *What is identity resolution and how are platforms adapting to privacy changes?* | MarTech. <https://martech.org/what-is-identity-resolution-and-how-are-platforms-adapting-to-privacy-changes/>
- Peng, F., & Tran, N. (n.d.). *Service design thinking for social good Fashion Communication View project Cross Cultural Design for Healthy Ageing View project*. <https://www.researchgate.net/publication/342735975>

- Pentland, A., & Hardjono, T. (2020). *Building the New Economy*. PubPub. <https://doi.org/10.21428/ba67f642.0499afe0>
- Piirainen, K. A., & Gonzalez, R. A. (2014). *Constructive Synergy in Design Science Research: A Comparative Analysis of Design Science Research and the Constructive Research Approach*. <https://www.researchgate.net/publication/262198751>
- Questions and Answers: Digital Services Act*. (2022, November 14). [https://ec.europa.eu/commission/presscorner/detail/en/QANDA\\_20\\_2348](https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348)
- Sitra. (n.d.). *PRINCIPLES-BASED FRAMEWORKS AND TOOLS FOR FAIR DATA ECONOMY*.
- Staff working document on data spaces | Shaping Europe's digital future*. (2022, February 23). <https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces>
- Stouffer, C. (n.d.). *The privacy paradox: How much privacy are we willing to give up online? | Norton*. Retrieved 13 October 2022, from <https://us.norton.com/blog/privacy/how-much-privacy-we-give-up#>
- Teixeira, J. G., Patrício, L., & Tuunanen, T. (2019). Advancing service design research with design science research. *Journal of Service Management*, 30(5), 577–592. <https://doi.org/10.1108/JOSM-05-2019-0131>
- Testbed for fair data economy – ihan.fi - Sitra*. (n.d.). Retrieved 29 November 2022, from <https://www.sitra.fi/en/projects/testbed-for-fair-data-economy-ihanfi/#latest>
- The Digital Services Act package | Shaping Europe's digital future*. (n.d.). Retrieved 26 November 2022, from <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- Thoring, K., & Müller, R. M. (2011). Understanding the creative mechanisms of design thinking. *Proceedings of the Second Conference on Creativity and Innovation in Design - DESIRE '11*, 137. <https://doi.org/10.1145/2079216.2079236>
- Turrecha, L. (n.d.). *Defining Privacy Tech. An attempt to avoid talking past each... | by lourdes.turrecha | Privacy & Technology | Medium*. Retrieved 19 October 2022, from <https://medium.com/privacy-technology/defining-privacy-tech-ae7b022888ec>
- vom Brocke, J., Hevner, A., & Maedche, A. (2020). *Introduction to Design Science Research* (pp. 1–13). [https://doi.org/10.1007/978-3-030-46781-4\\_1](https://doi.org/10.1007/978-3-030-46781-4_1)

- What are Privacy Centers and Should You Have One? - Privacy Policies.* (2022, July 1).  
<https://www.privacypolicies.com/blog/privacy-centers/>
- What is a Preference Center & Why Is It Important? - Securiti.* (n.d.). Retrieved 26 November 2022, from <https://securiti.ai/what-is-preference-center/>
- What is a Privacy Center & Why Does It Matter? - Securiti.* (n.d.). Retrieved 26 November 2022, from <https://securiti.ai/what-is-privacy-center/>
- What is GDPR, the EU's new data protection law? - GDPR.eu.* (n.d.). Retrieved 23 October 2022, from <https://gdpr.eu/what-is-gdpr/>
- What is ISO 27701? How is it different from ISO 27001? - Polymer.* (2021, July 5).  
<https://www.polymerhq.io/blog/iso-27001/iso27701vviso27001/>
- Why It's So Hard for Users to Control Their Data.* (n.d.). Retrieved 20 October 2022, from <https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data>

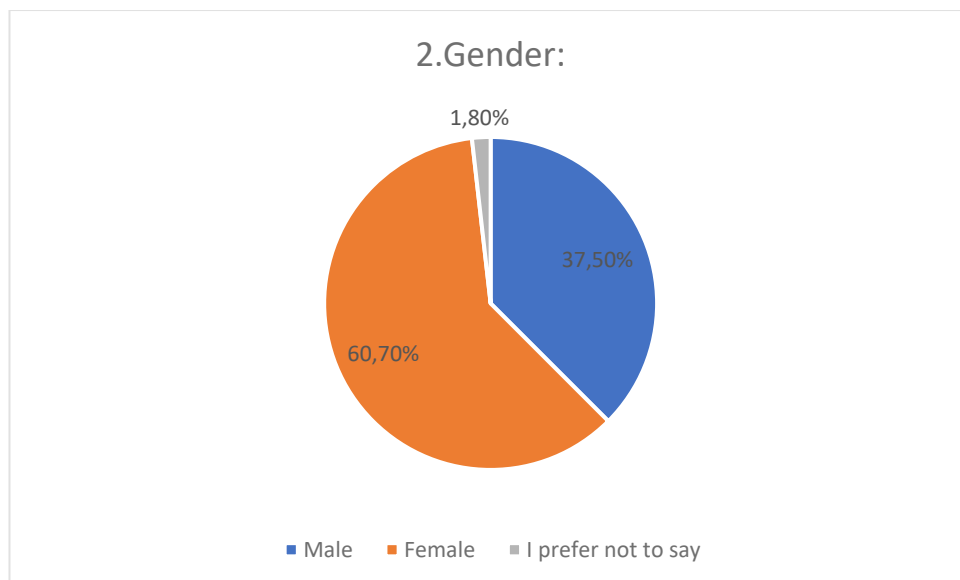
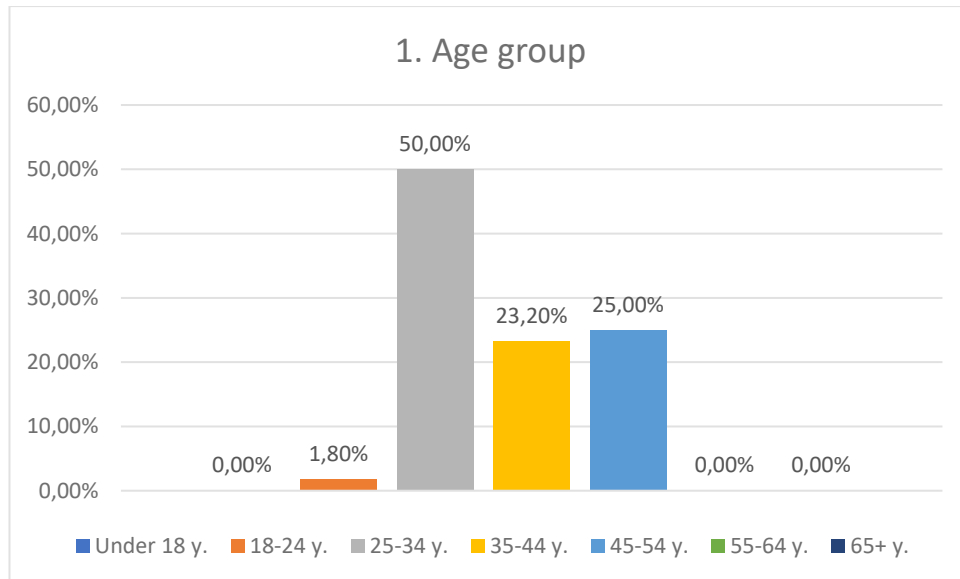
## Appendices

### Appendix 1: Questionnaire

## Questionnaire:

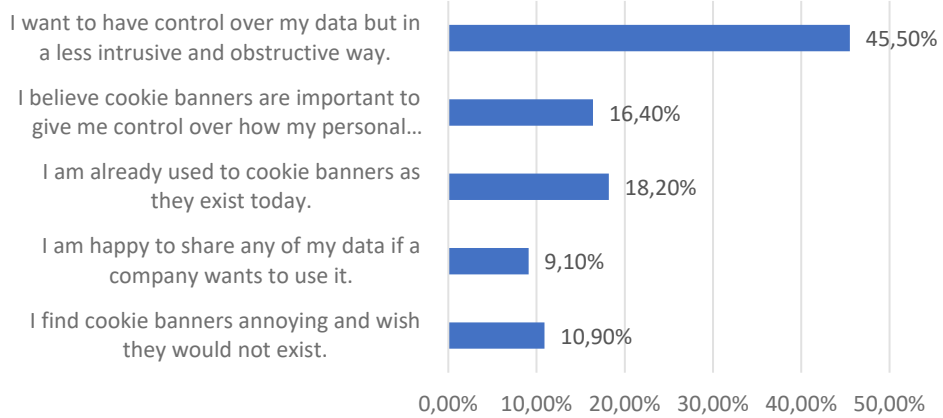
Out of 255 who received the questionnaire 56 answered which gives a response rate of 22% out of the total amount.

Background and demographics:

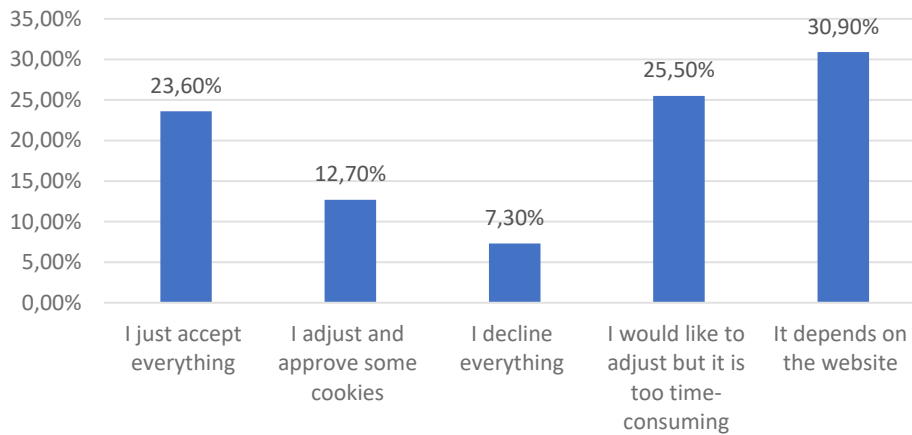


The age groups from 18-54 were presented with the majority in the age group of 25-34.

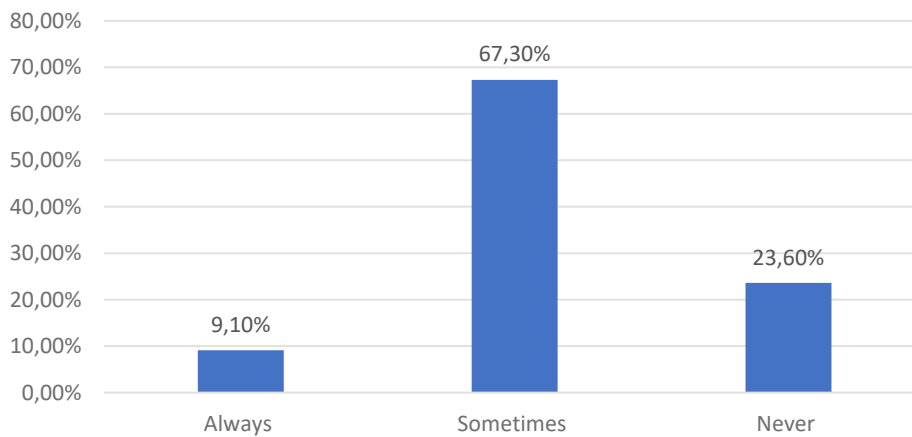
#### 4. Which of the following statements fits you the best?



#### 5. How do you usually select what cookies to choose?



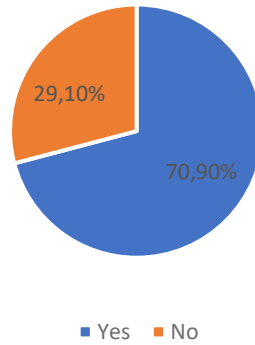
#### 6. How often do you select what cookies you give consent to?



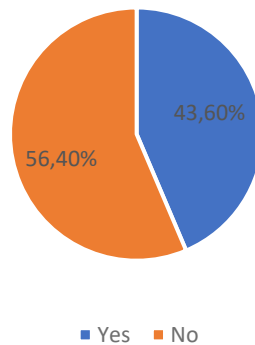
45,5% say that they want to have more control over their data but not with cookie banners as they are displayed today. About 10% always adjust or declines cookie settings. Up to 67,3% adjust

cookies sometimes and 23,6% never adjust anything but gives consent to all cookies. 25,5% would like to but find it too time consuming.

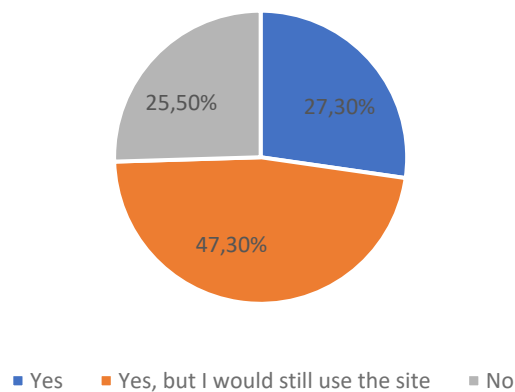
7. Have you ever stopped visiting a website because of a poorly designed cookie banner where making consent choices was difficult?



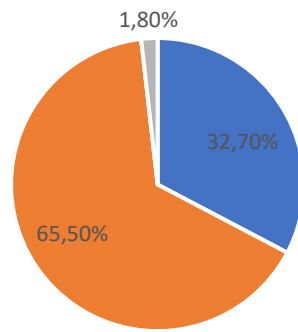
8. Have you ever stopped visiting a website because of a misleading or untrustworthy cookie banner?



9. Would you consider a website unsafe and suspicious if it does not have a cookie banner?



### 10. Would you use a website without a cookie banner?



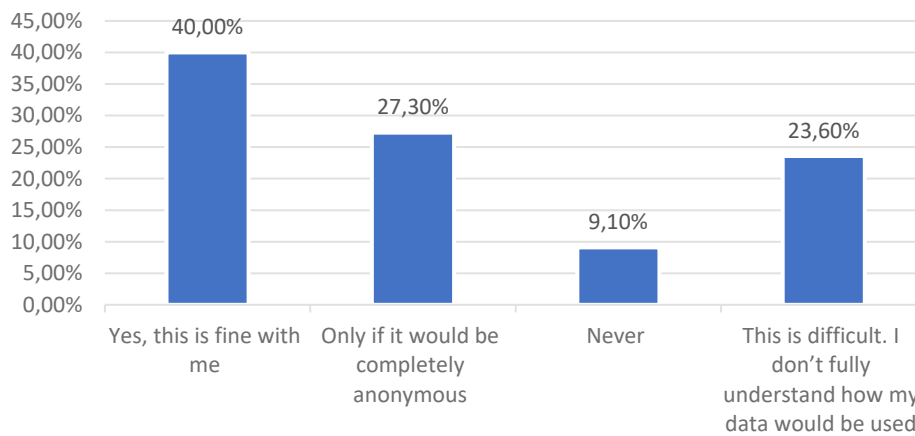
■ Yes ■ Yes, if it is a brand I trust ■ No

71% of users have stopped from using a website because of a poorly designed cookie banner but 56% have entered a website despite of a misleading or untrustworthy cookie banner.

If a website doesn't have a cookie banner 73% would consider it suspicious and 47% would still continue using the website.

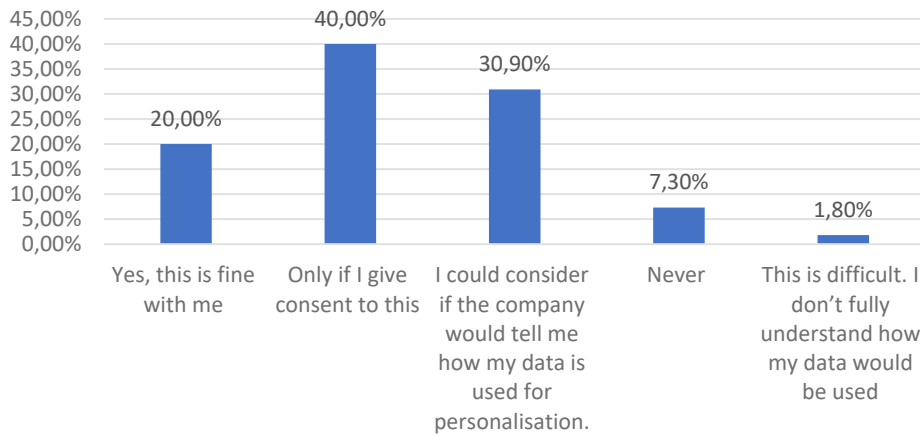
98% would use a website without a cookie banner if it is a brand they trust.

### 11. Would you give consent to analytics cookies to track your behaviour on a website?





### 12. Would you give consent to personalisation cookies to serve you targeted content and offers?

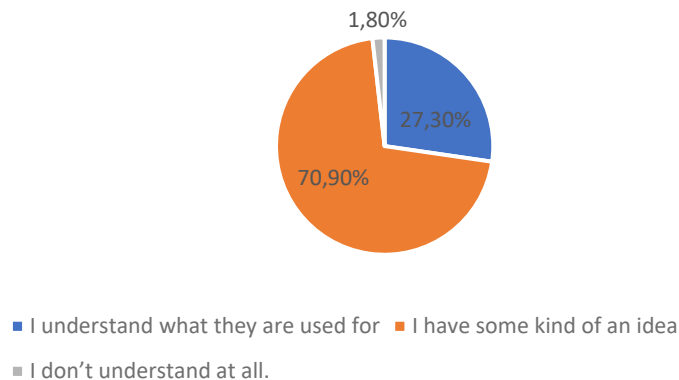


40% would approve to be tracked on a website with analytics cookies and 27% if it would be completely anonymous. 24% states that they don't fully understand how their data would be used.

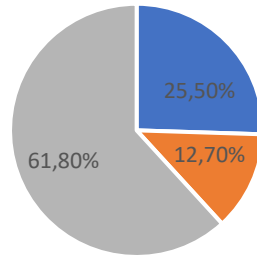
People tend to be stricter when it comes to personalisation because only 20% would not mind but 40% would be ok only if they have given explicit consent to be targeted. 31% would like to know how from the company how their data would be used for personalisation.

Only around 8% would never give consent to analytics or personalisation cookies.

### 13. How do you estimate your knowledge about different types of cookies and how they are used?



14. Would you give consent to cookies if you are not entirely sure about how your data would be used?

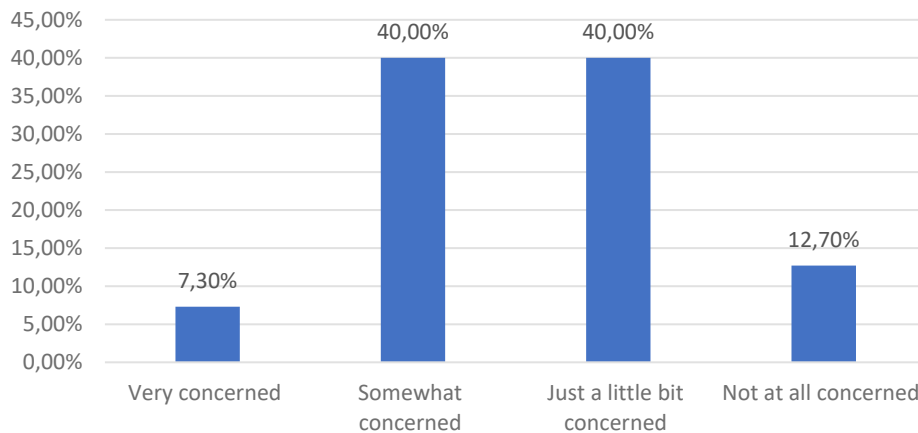


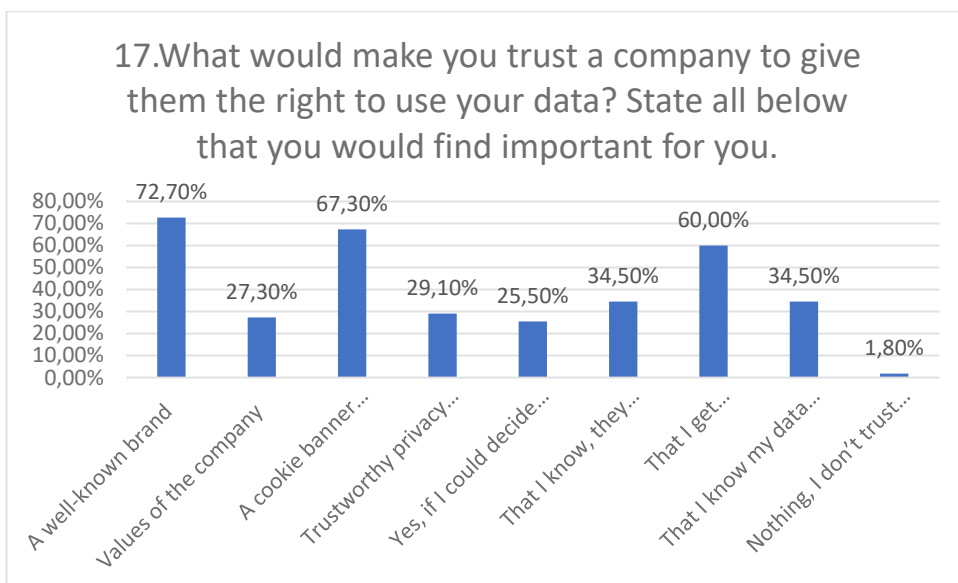
■ Yes ■ No ■ I might if I trust the company/ brand

71% of respondents have some kind of an idea what cookies are used for and 27% understands more in detail what cookies are used for. In total 98% of the respondents had some kind of an idea what the cookies are used for.

Only 13% would never give consent if they would not know how their data would be used. 25% would always give consent. 62% could consider giving consent if they would trust the company or the brand.

15. Are you concerned about how companies are using your personal data?



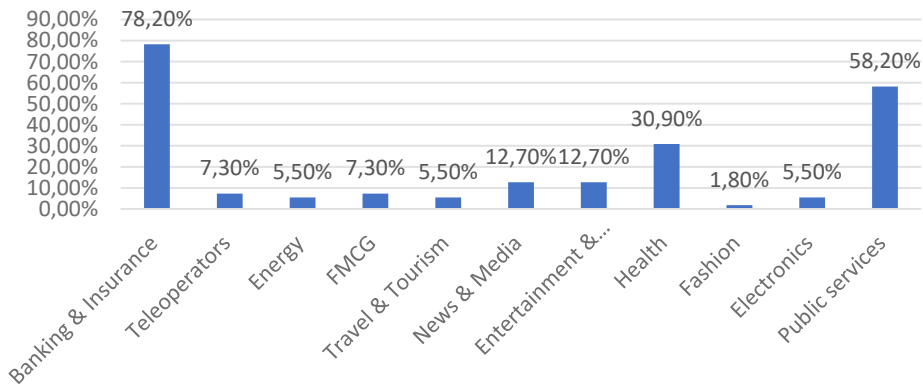


40% are moderately concerned how companies are using their personal data. 40% are a little bit concerned and 13% are not concerned at all. Only 7% are very concerned.

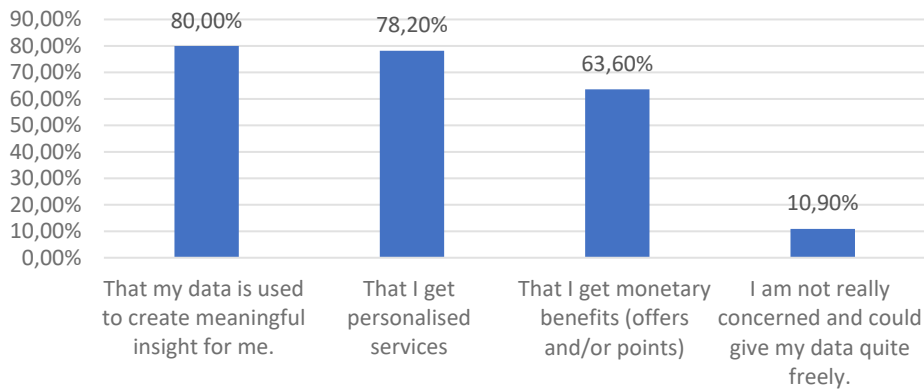
84% of the respondents only trust that some companies are using their data responsibly. 9% trusts that their data is always safe and 7% never trust that their data is safe.

A well-known brand would be the largest driver for users to trust companies, 73% would give consent. 67% would trust a company if it would be as easy to decline consent as it is easy to give consent. Transparency in informing about how the data is used was also highly rated up to 60%.

18. What type of business/ industry would you trust more than others to give consent to use your data?

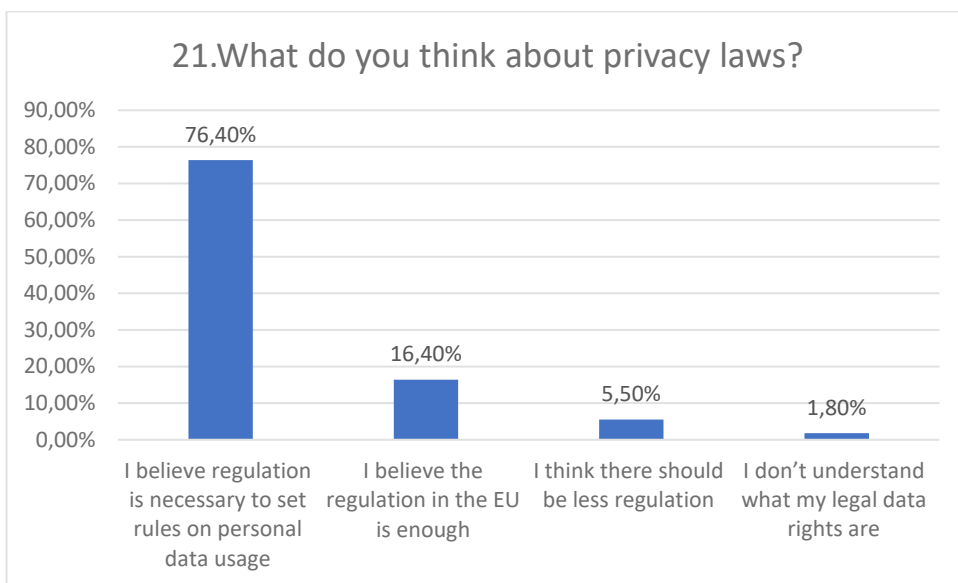
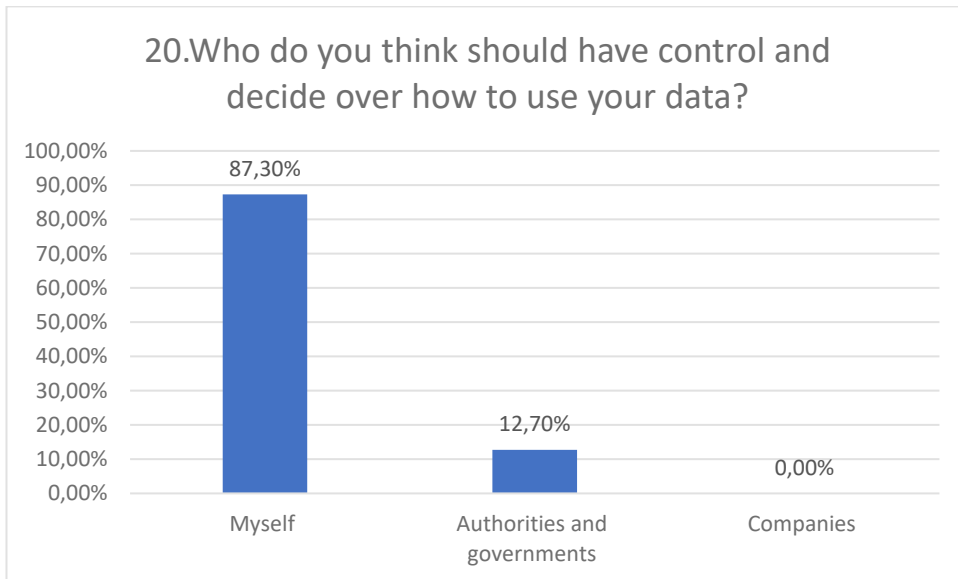


19. Which of the following would make you more willing to share your data with a company? Choose all statements that fit to you.



The type of industry plays a significant role where users would trust to give their consent. Banking & insurance was trusted up to 77%, public services up to 58% and health up to 29%. Travel and tourism and fashion had the lowest trust rates with 4% and 2%.

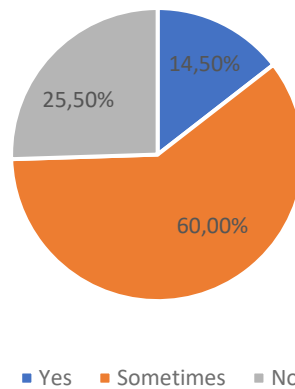
80% of users would give consent if the data would be used to create meaningful insight and 78% would give consent to get personalised services. Monetary benefits weren't that important but still valued up to 64%. 11% would not be concerned and would share the data freely.



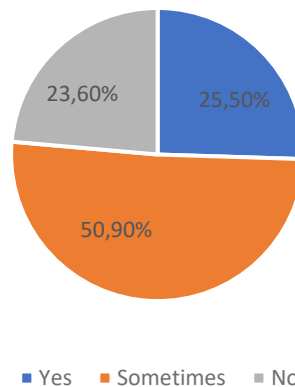
It was quite clear that user wants to have control over their data themselves with 87% of the respondents. 13% would trust authorities and governments. 0% would trust companies to control their data if possible.

76% of the respondents believe is necessary to set boundaries how personal data can be used. 16% believe that the current regulation in the EU is enough. 6% think there should be less regulation on personal data . 2% do not understand what their data right are.

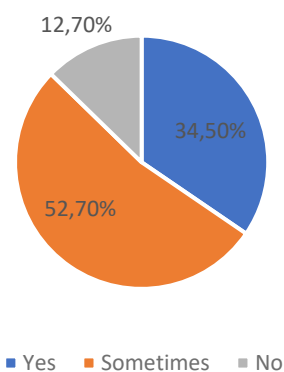
22. In your opinion, is it usually easy to continue to the site without giving consent to all cookies?



23. What is your perception? Can you usually use a website even without selecting cookies?



24. Do you usually continue to a website if it does not have an easily accessible button to decline non-necessary cookies?

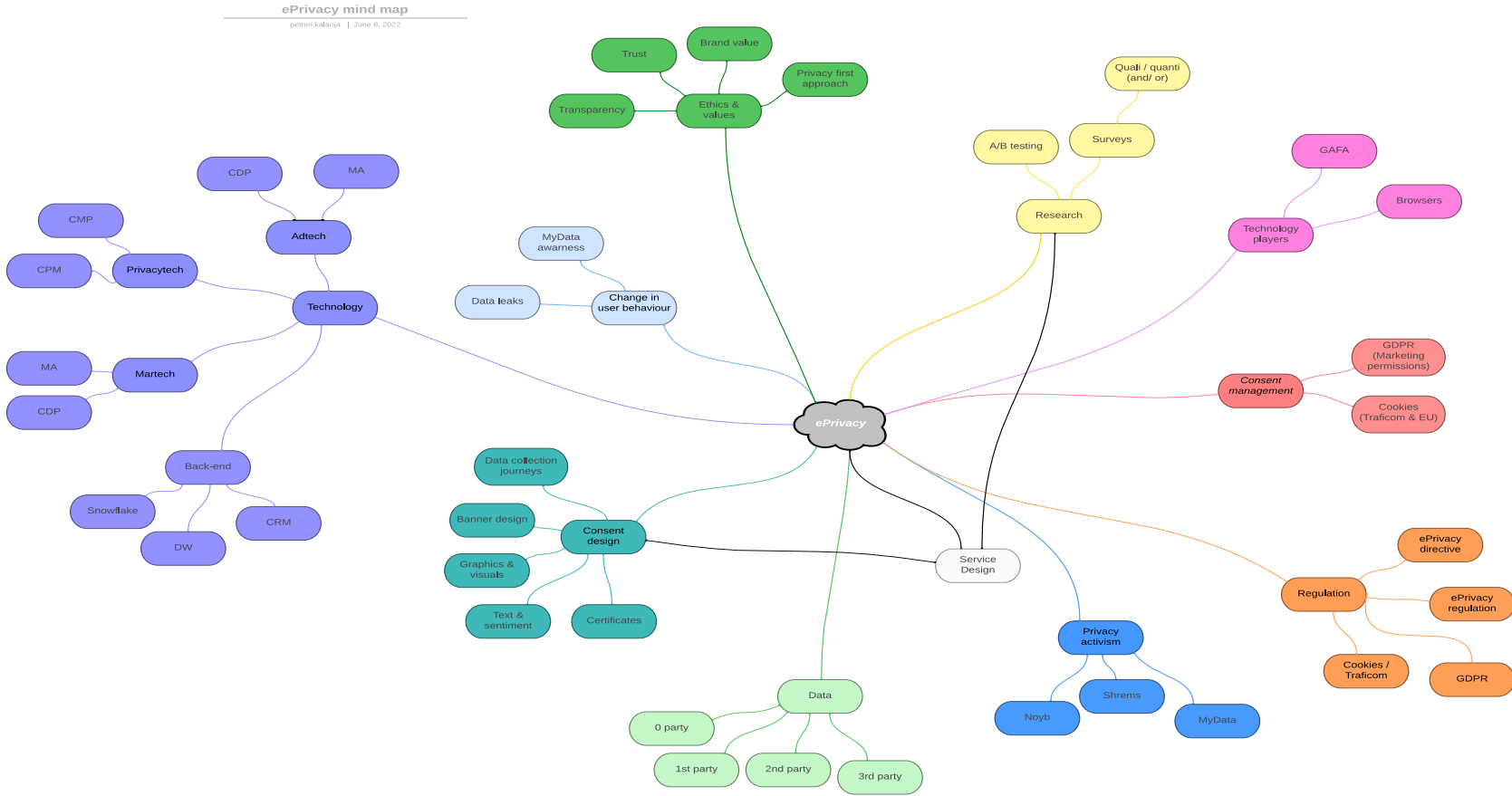


26% of the respondents think that is not easy to continue to a website without giving consent to all cookies. 60% say that it is sometimes difficult and 14% thinks it is always easy.

51% of users believe they can sometimes use a website without giving consent to cookies, 25% say that they can use a website without making any cookie selections. 24% say that they cannot use a website without making choices.

34% of users continue to a website even though they could not decline non-necessary cookies, 13% would never use a website where they could not decline cookies and 53% would use such a website sometimes.

Appendix 2: Mindmap





## Appendix 3: Consent and privacy toolkit

Topic	Legal & Regulation	Trends & insight	Tech & Data	Design, UI & UX	Ethics & Values	Business, Processes & Strategy
Why is this important	It is important to understand what new privacy laws and regulations obligates companies to do. The consequences can be substantial fines or reputational damage and consumer mistrust.	This is a very complex environment that is evolving very fast and there are many different factors to take into consideration. Changes can mean very time consuming, expensive and complicated processes to implement. The sooner you know, the better you can plan and be reactive.	Without technology consent and privacy cannot be handled.	Design plays an important part in how consent has to be acquired by law but also how design can be implemented in a way of creating trust and optimising a positive consent rate.	Consumers are demanding for more privacy, transparency and control over their own data. Regulators all over the world are setting stricter laws to meet these demands that are based and values such as trust and transparency.	All of these changes are changing fast in a very complex environment. It brings new rules and new ways of executing business cases that used to work before but will impact heavily many traditional business cases.
Context (examples)	<ul style="list-style-type: none"> <li>Regulation = what has to be executed and has to be in place (eg. GDPR, cookie compliance)</li> <li>The most important drivers. (Sanctions, reputation damage)</li> </ul>	<ul style="list-style-type: none"> <li>Change in consumer behaviour</li> <li>Technology landscape changes (Cookie depreciation)</li> <li>Privacy First approach</li> <li>Insight -&gt; actions</li> </ul>	<ul style="list-style-type: none"> <li>Tech needed to handle all of this (CMP, preference centers, CDP, server side)</li> <li>Support in selection of tech Tech implementation</li> <li>Audits</li> <li>Threat assessments</li> </ul>	<ul style="list-style-type: none"> <li>Fair design principles</li> <li>Tone of voice in communication</li> <li>A/B-testing</li> </ul>	<ul style="list-style-type: none"> <li>A sustainable approach to using data transparently</li> <li>Fair design principles</li> <li>Tone of voice in communication</li> <li>Utilisation of brand values</li> </ul>	<ul style="list-style-type: none"> <li>Iterative privacy processes (for different units)</li> <li>Skills (in-house / external)</li> <li>New business opportunities (e.g. preference center tools as personalisation enablers -&gt; better personalisation -&gt; Less op-outs)</li> <li>Automation</li> <li>Risk mitigation</li> <li>Customer journey planning for data collection</li> <li>Audit</li> </ul>
Elements	<ul style="list-style-type: none"> <li>Privacy regulation &amp; law <ul style="list-style-type: none"> <li>World</li> <li>EU</li> <li>Local/ country</li> </ul> </li> <li>Threat modelling</li> <li>Schrems II</li> </ul>	<ul style="list-style-type: none"> <li>Consumer behaviour</li> <li>Privacy regulation &amp; law</li> <li>Technology</li> <li>Unexpected change drivers</li> <li>EU initiatives <ul style="list-style-type: none"> <li>Data spaces etc</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Privacy technology <ul style="list-style-type: none"> <li>CMP, Privacy &amp; preference centers</li> <li>RegTech</li> </ul> </li> <li>Other relevant technology <ul style="list-style-type: none"> <li>CDP</li> <li>ID solutions</li> </ul> </li> <li>Threat modelling</li> </ul>	<ul style="list-style-type: none"> <li>Customer experience</li> <li>Privacy First approach</li> <li>Trusted design</li> <li>Privacy Communication strategy</li> <li>Trusted design</li> <li>Privacy-by-design</li> </ul>	<ul style="list-style-type: none"> <li>Values: transparency &amp; trust</li> <li>Brand values</li> <li>Customer experience</li> <li>Privacy frameworks</li> <li>Privacy First approach</li> </ul>	<ul style="list-style-type: none"> <li>Certificates <ul style="list-style-type: none"> <li>ISO standards</li> <li>CIPP-certificates</li> </ul> </li> <li>Business case strategy / evaluation</li> <li>Privacy frameworks</li> <li>Privacy strategy</li> <li>Data strategy</li> <li>Threat modelling</li> <li>Privacy audit</li> <li>Privacy-by-design</li> <li>A/B testing &amp; optimising</li> <li>Follow-ups with key stakeholders</li> </ul>

# Interview Questions and consent banner examples

Service Design

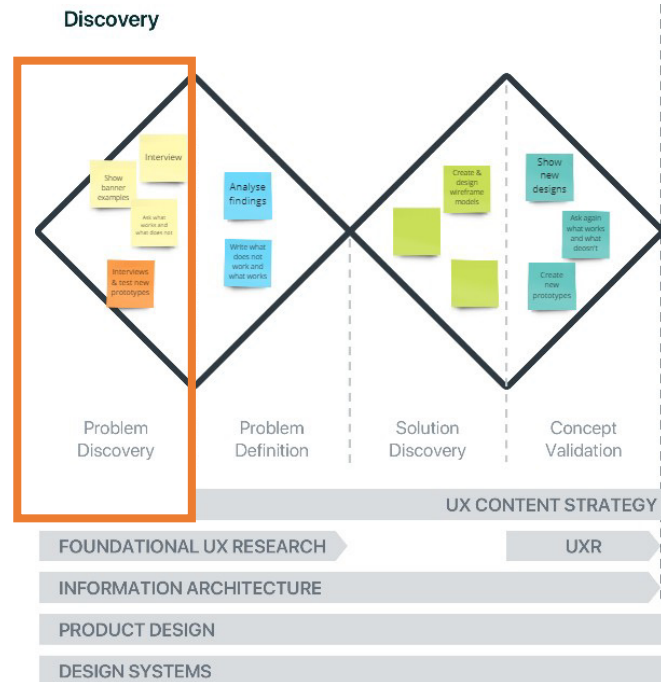
Double diamond discovery phase

# Interviewee background

- Gender
- Age group ■ Under 18 y. ■ 18-24 y. ■ 25-34 y. ■ 35-44 y. ■ 45-54 y. ■ 55-64 y. ■ 65+ y.
- Familiarity with the topic, scale 1-5, (1 bad – 5 best)

# Service Design

## Double Diamond



# Interview

We are trying to find out what kind of cookie banner designs are:

- Easy to understand
- Easy to find the necessary elements
- That is functional
- Quick to use
- Creates trust

I am going to show you various cookie consent banners. Tell me in your own words what you think about them, what is good, what is bad. Any ideas and thoughts are welcomed, no matter how silly or trivial you might think they are. There aren't any wrong or right answers. The point is to find all kind of views that will help us to design and create one or a few different consent banners that will display trust but also convert in the best possible way.

## Questions for each consent banner:

- Spontaneous first impression
- Would you read the text?
- What would you do here to get to the website?
  - Would you continue to the site at all?
  - Would you feel secure after clicking OK/Yes?
- Would you click:
  - OK/ accept all cookies
  - Decline
  - Adjust/ customise

# Interview – possible help questions

- What do you think about colours in general?
  - On buttons?
- What about the position of the buttons?
  - Does it matter if they are horizontally or vertically aligned?
  - What about their order from left to right?
- What about the text?
- What do you think about the banners where you can make adjustments and selections in the banner without a need of going an extra step into settings?
- Would you give consent more likely if you would trust that it would be done correctly e.g. EU legislation would be followed and honoured.
- As a last question: what kind of an banner would you like to see?

**YOUR LOGO**

Powered by **Cookiebot**  
by Usercentrics

**Consent**

Details

Ad Settings

About

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Do not sell my personal information

OK



Powered by **Cookiebot**  
by Usercentrics

**Consent**

**Details**

**About**

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

**Deny**

**Customize >**

**Allow all**

**YOUR LOGO** Powered by **Cookiebot**  
by Usercentrics

[Consent](#)      [Details](#)      [About](#)

---

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary <input type="checkbox"/>	Preferences <input checked="" type="checkbox"/>	Statistics <input checked="" type="checkbox"/>	Marketing <input checked="" type="checkbox"/>
---------------------------------------	--	---	--

**This website uses cookies**

We use cookies to personalise content and to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies by selection below.

Necessary      
 Preferences      
 Statistics      
 Marketing      
 [Show details >](#)

Allow all cookies

Allow selection

Use necessary cookies only

## Manage Cookies

We use cookies to provide and secure our websites, as well as to analyze the usage of our websites, in order to offer you a great user experience. To learn more about our use of cookies see our [Privacy Policy](#).

- Necessary
- Marketing
- Performance

Accept

All

Necessary



We use cookies on this site to enhance your user experience.  
For a complete overview of all cookies used, please see your [personal settings](#).

Accept all

Decline All

Customize

Advertising

Analytics

Customer Interaction

Essential

## This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Deny

Allow all

[Show details](#)

Necessary (6)

[Show details](#)

Preferences (2)

[Show details](#)

Statistics (5)

[Show details](#)

Marketing (42)

[Show details](#)

## This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Allow all

Deny

[Show details](#)

Necessary (1)

[Show details](#)

Preferences (0)

[Show details](#)

Statistics (3)

[Show details](#)

Marketing (1)

[Show details](#)

Allow selection

Cookie declaration last updated on 7/14/21 by [Cookiebot](#)

## Cookie Settings ✕

When you visit any of our websites, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and manage your preferences. Please note, blocking some types of cookies may impact your experience of the site and the services we are able to offer.

**Strictly Necessary** ?

**Performance Cookies** ?

**Functional Cookies** ?

**Targeting Cookies** ?

[Confirm my choices](#) [Accept all cookies](#) [Cancel](#)

## Manage Cookie Consent

We use cookies to optimize our website and our service.  
[Cookie Policy](#) - [Impressum](#)

Functional

Statistics

Marketing

[Accept all](#)

[Dismiss](#) [Save preferences](#)

## Cookies improve user experience

When you click 'Accept all' cookies, Aarhus University can give you the best user experience. Cookies store information about how a user interacts with a website. All your data is anonymised and cannot be used to identify you. You can always change your consent again under 'Cookies' in the website footer.

The university uses its own cookies and cookies set by our partners for the following purposes:

- STRICTLY NECESSARY**  
These cookies make it possible to use basic website functionality, e.g. navigation etc. The website does not work without these cookies.
- STATISTIC**  
These cookies provide the university with anonymised data on how the user interacts with the website. For example, information about how often the user visits the website, and which pages the user visits.
- TARGETING**  
These cookies make it possible for the university to target advertising on our websites and social media, so you will see the content that is most relevant for you.
- FUNCTIONALITY**  
These cookies store information about the user's choices on the website such as language or login.

Accept selected

Accept all

# Your Choices Regarding Cookies on this Site

Please choose whether this site may use Functional and/or Advertising cookies, as described below:



**REQUIRED COOKIES**  
These cookies are required to enable core site functionality.

**FUNCTIONAL COOKIES**  
These cookies allow us to analyze site usage so we can measure and improve performance.

**ADVERTISING COOKIES**  
These cookies are used by advertising companies to serve ads that are relevant to your interests.

## Functionality Allowed

- Provide secure log-in
- Remember how far you are through an order
- Remember your log-in details
- Remember what is in your shopping cart
- Make sure the website looks consistent

## Functionality NOT Allowed

- Allow you to share pages with social networks
- Allow you to post comments
- Serve ads relevant to your interests

CANCEL

SUBMIT PREFERENCES



## We use cookies

We use cookies and other tracking technologies to improve your browsing experience on our website, to show you personalized content and targeted ads, to analyze our website traffic, and to understand where our visitors are coming from.

**I agree**

**I decline**

Change my preferences



## We use cookies

We use cookies and other tracking technologies to improve your browsing experience on our website, to show you personalized content and targeted ads, to analyze our website traffic, and to understand where our visitors are coming from.

**I agree**

**I decline**

Change my preferences





## Manage Cookie Consent



To provide the best experiences, we use technologies like cookies to store and/or access device information. Consenting to these technologies will allow us to process data such as browsing behavior or unique IDs on this site. Not consenting or withdrawing consent, may adversely affect certain features and functions.

[Manage third parties](#)

Accept

Deny

View preferences

[Cookie Policy](#)

We use cookies to optimize our website and our service.

[Cookie Policy](#)

Accept all

Dismiss

Preferences

## Manage Cookie Consent

We use cookies to optimize our website and our service.

[Cookie Policy](#) - [Impressum](#)

- Functional
- Statistics
- Marketing

Accept all

Dismiss

Save preferences

## Manage Cookie Consent

We use cookies to optimize our website and our service.

[Cookie Policy](#) - [Impressum](#)

- Functional
- Statistics
- Marketing

Accept all

Dismiss

Save preferences

## Manage Cookie Consent

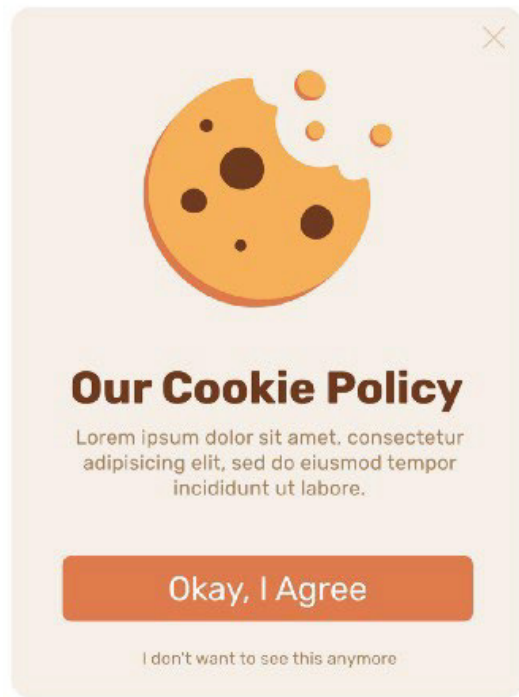
We use cookies to optimize our website and our services. For our policies, please visit our [Cookie Policy](#) - [Impressum](#)

- Functional Cookies
- Marketing Cookies

ACCEPT ALL COOKIES

FUNCTIONAL

SAVE PREFERENCES

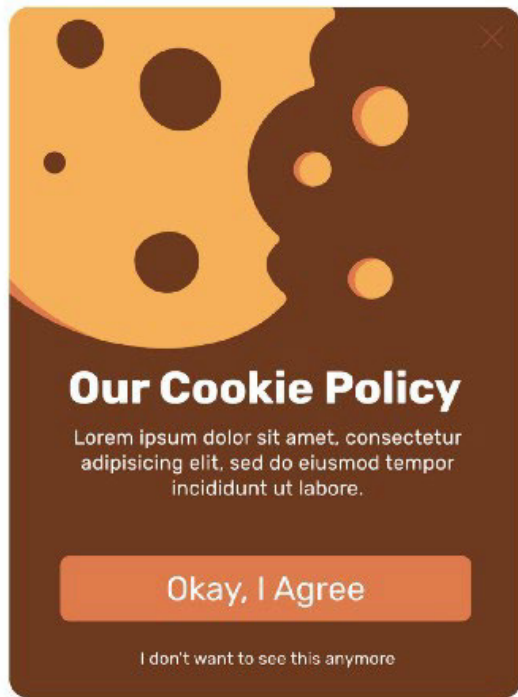


Our Cookie Policy

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore.

Okay, I Agree

I don't want to see this anymore

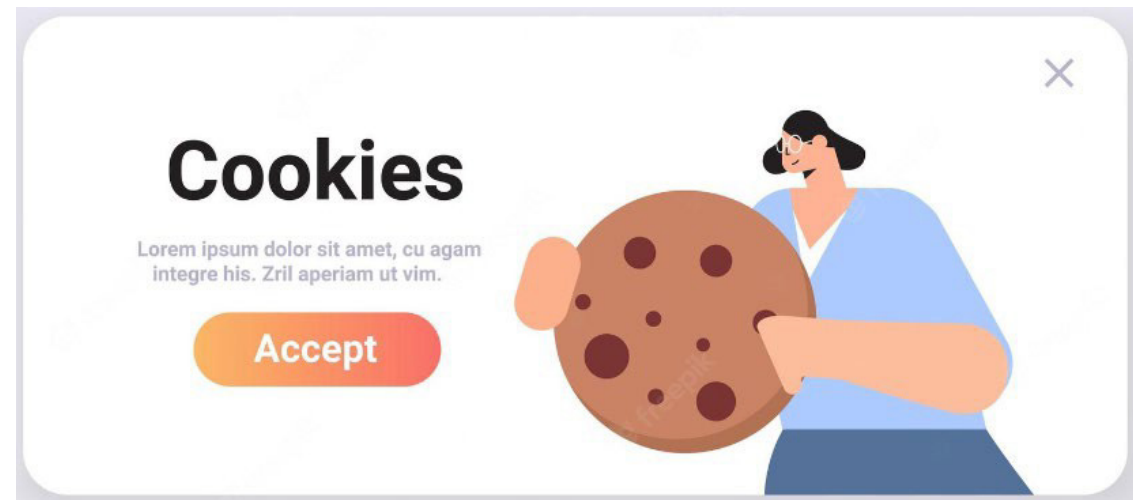


Our Cookie Policy

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore.

Okay, I Agree

I don't want to see this anymore



# Cookies

Lorem ipsum dolor sit amet, cu agam integre his. Zril aperiam ut vim.

Accept



# cookie?

We use cookies to make your experience on this website better.

Yes please!

No... I'm full



## Cookies

We baked some cookies that you have to accept, if you want to enjoy this website. It simply doesn't work without. In order to gather information and make improvements, we should use some third-party cookies too. Can we?

MANAGE COOKIES

ACCEPT



SHOP



# Use of cookies:

Cookies are small data files that are sent from a website's server to your web browser, from where they are stored on your device.



All cookies



Only essential cookies



No cookies :(



Essential cookies are used only to transmit the data online and are strictly necessary to make a website operational.

It's me !  
The spy pharaoh...



I waited to be sure that the content of this site interests you before disturbing you, but I would love to accompany you on your visit !  
Is it OK for you ?

We respect your privacy, here's how.

Consents certified by  axeptio

No, thanks

I want to choose

OK!



YOU ONLY HAVE TO DO THIS ONCE

## SO LET'S GET THIS OVER WITH

We use cookies to make Lunchbox's website the best in the food tech game. To learn more about our cookies, check out our Privacy Policy.

ACCEPT COOKIES

DECLINE COOKIES

CLICKING OUT OF THE WILL AUTOMATICALLY ACCEPT COOKIES

## Before you continue to YouTube

We use [cookies](#) and data to

- Deliver and maintain Google services
- Track outages and protect against spam, fraud and abuse
- Measure audience engagement and site statistics to understand how our services are used and enhance the quality of those services

If you choose to 'Accept all', we will also use cookies and data to

- Develop and improve new services
- Deliver and measure the effectiveness of ads
- Show personalised content, depending on your settings
- Show personalised ads, depending on your settings

If you choose to 'Reject all', we will not use cookies for these additional purposes.

Non-personalised content and ads are influenced by things like the content that you're currently viewing and your location (ad serving is based on general location). Personalised content and ads can also include things like video recommendations, a customised YouTube homepage and tailored ads based on past activity, like the videos that you watch and the things that you search for on YouTube. We also use cookies and data to tailor the experience to be age-appropriate, if relevant.

Select 'More options' to see additional information, including details about managing your privacy settings. You can also visit [g.co/privacytools](https://g.co/privacytools) at any time.

MORE OPTIONS

REJECT ALL

ACCEPT ALL



## Do you agree to let us use cookies?

We and [our partners](#) use cookies and trackers to

- Provide live support and access to our **help center**
- Generate **insights to improve the interface** and functionalities
- Help you navigate in the console and to **display important information** such as updates
- Measure **marketing campaign effectiveness** and **offer updates** about our products
- Manage **authentication** and monitor technical errors in our product

Some cookies are needed for technical purposes, they are therefore exempted from consent. Others, non-mandatory, may be used for personalized ads and content, ad and content measurement, audience insights and product development, precise geolocation data, and identification through device scanning, store and/or access information on a device. To learn more, visit our [privacy center](#).

Configure

I disagree

I agree



Hi! Just wanted to let you know that we use cookies on our site. These cookies enhance your experience, improve the quality of our site, and help us show you things that are more likely to be relevant to you. We also allow third parties (including our advertising partners) to place cookies on our websites. By clicking "Accept", you're agreeing to the placement and use of cookies as described in our [Cookie Policy](#). That is all. Thanks for reading!

I Accept

## We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.

Customize

Reject All

Accept All

## Your Privacy Rights



The Spruce and [our third-party partners](#) use cookies and process personal data like unique identifiers based on your consent to store and/or access information on a device, display personalized ads and for content measurement, audience insight, and product development. To change or withdraw your consent choices for TheSpruce.com, including your right to object where legitimate interest is used, click below. At any time, you can update your settings through the "EU Privacy" link at the bottom of any page. These choices will be signaled globally to our partners and will not affect browsing data.

### We and our partners process data to:

Actively scan device characteristics for identification. Use precise geolocation data. Store and/or access information on a device. Select personalised content. Create a personalised content profile. Measure ad performance. Select basic ads. Create a personalised ads profile. Select personalised ads. Apply market research to generate audience insights. Measure content performance. Develop and improve products.

[List of Partners \(vendors\)](#)

I ACCEPT

SHOW PURPOSES

## The choice is yours

We use cookies to give you the best possible experience when using our website. By clicking 'Accept All' we can bring you relevant advertising and personalised content – and generally give you a much more enhanced visit. If you'd rather take the time to set which cookies we can use, click 'Manage Settings'. Your choices can always be changed at a later date [here](#).

Manage Settings

Accept All

# Consent Banner Prototypes



## IT'S YOUR PRIVACY RIGHTS.

### What cookies may we use?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit

#### Necessary



#### Functional



#### Statistics



#### Marketing



Accept selected

Accept all

Adjust settings

## IT'S YOUR PRIVACY RIGHTS.

### What cookies may we use?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

#### Necessary



#### Functional



#### Statistics



#### Marketing



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Accept selected

Accept all

Adjust settings

## IT'S YOUR PRIVACY RIGHTS

### What cookies may we use?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit



Necessary



Functional



Statistics



Marketing



Adjust settings

Accept all

Accept selected

## IT'S YOUR PRIVACY RIGHTS

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit



### What cookies may we use?

Necessary



Functional



Statistics



Marketing



Accept selected

Accept all

Adjust settings

## IT'S YOUR PRIVACY RIGHTS

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit



### What cookies may we use?

Necessary



Functional



Statistics



Marketing



Accept selected

Accept all

Adjust settings

## IT'S YOUR PRIVACY RIGHTS

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem



### What cookies may we use?

Necessary



Functional



Statistics



Marketing



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Accept selected

Accept all

Adjust settings

## IT'S YOUR PRIVACY RIGHTS.

### What cookies may we use?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit

**Necessary**  Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

**Functional**  Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

**Statistics**  Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

**Marketing**  Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

Accept selected

Accept all

Adjust settings

## IT'S YOUR PRIVACY RIGHTS.

### What cookies may we use?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit

**Necessary**  
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

**Functional**  
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

**Statistics**  
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

**Marketing**  
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

Accept selected

Accept all

Adjust settings

## IT'S YOUR PRIVACY RIGHTS.

### What cookies may we use?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit



#### Necessary

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,



#### Functional

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,



#### Statistics

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,



#### Marketing

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

Accept selected

Accept all

Adjust settings

## IT'S YOUR PRIVACY RIGHTS

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet

### What cookies may we use?



#### Necessary

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,



#### Functional

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,



#### Statistics

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,



#### Marketing

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet,

Accept selected

Accept all

Adjust settings

# COOKIES

IT'S YOUR PRIVACY RIGHTS.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem

Necessary



Functional



Statistics



Marketing



Accept selected

Accept all

Adjust settings

# CONSENT

IT'S YOUR PRIVACY RIGHTS.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem

Necessary



Functional



Statistics



Marketing



Accept selected

Accept all

Adjust settings

# **Second iteration prototypes**

## IT'S YOUR PRIVACY RIGHTS.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit

### What cookies may we use?

---

Necessary



Functional



Statistics



Marketing



Accept selected

Accept all

[Read more about cookies](#)





## IT'S YOUR PRIVACY RIGHTS.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit

### What cookies may we use?

---

Necessary



Functional



Statistics



Marketing



Accept selected

Accept all

[Read more about cookies](#)

## IT'S YOUR PRIVACY RIGHTS.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit Lorem ipsum dolor sit amet, consectetur

### What cookies may we use?

---

#### Necessary



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

#### Functional



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

#### Statistics



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

#### Marketing



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Accept selected

Accept all

[Read more about cookies](#)

## IT'S YOUR PRIVACY RIGHTS.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Lorem ipsum dolor sit amet, consectetur adipiscing elit Lorem ipsum dolor sit amet, consectetur



### What cookies may we use?

#### Necessary



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna

#### Functional



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna

#### Statistics



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna

#### Marketing



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna

Accept selected

Accept all

Adjust settings