

Designing for Privacy

Design Patterns for Making Online Products GDPR Compliant

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieurin

im Rahmen des Studiums

Media and Human-Centered Computing

eingereicht von

Nataliia Avdosieva, MSc

Matrikelnummer 01528722

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Peter Purgathofer

Wien, 1. März 2019

Nataliia Avdosieva

Peter Purgathofer

Designing for Privacy

Design Patterns for Making Online Products GDPR Compliant

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieurin

in

Media and Human-Centered Computing

by

Nataliia Avdosieva, MSc

Registration Number 01528722

to the Faculty of Informatics

at the TU Wien

Advisor: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Peter Purgathofer

Vienna, 1st March, 2019

Nataliia Avdosieva

Peter Purgathofer

Erklärung zur Verfassung der Arbeit

Nataliia Avdosieva, MSc
1030 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 1. März 2019

Nataliia Avdosieva

Acknowledgements

At this point, I would like to thank everyone who contributed to this thesis. First of all, I would like to thank my advisor, Peter Purgathofer for guiding and supporting me over this process, for his inspiring ideas and always helpful and wise advice.

Besides my advisor, I would like to thank all professors involved in my study, for the many interesting courses during the Master's degree program, which enhanced my knowledge and helped me to acquire useful experience for my current profession.

I would also like to thank privacy and design experts and all people involved in my research for their insightful comments and input into the creation of the design patterns, and their valuable evaluation.

Last but not least, I would like to thank my family and my friends for their support, and constant encouragement I have gotten over the years.

Kurzfassung

Die Datenschutz-Grundverordnung (DSGVO), die am 25. Mai 2018 in Kraft getreten ist, setzt einen neuen Standard für die Verarbeitung, Speicherung und den Schutz der personenbezogenen Daten und der Privatsphäre von EU-Bürgern. Das Gesetz schreibt vor, dass Unternehmen, die eine Webpräsenz haben, Maßnahmen ergreifen, um sicherzustellen bzw. Kundendaten auf faire Weise verarbeiten, dass sie den Kunden deutlich erklären, wie lange ihre personenbezogenen Daten verwendet und gespeichert werden, und eine gültige Zustimmung ihrer Kunden dazu erhalten. Um die DSGVO-Konformität zu erreichen, müssen Unternehmen die Strategien für den Umgang mit personenbezogenen Daten von Kunden und die Gestaltung des Datenschutzes der Benutzer überdenken. Obwohl die DSGVO theoretisch einfach sein kann, ist sie immer noch schwer in die Praxis umzusetzen. In dieser Diplomarbeit stellen wir die Hilfe vor, mit der Designer oder Designerinnen durch DSGVO-konforme und datenschutzfreundliche Online-Systeme geleitet werden. Zunächst untersuchen wir bestehende Ansätze zum Erreichen der DSGVO-Konformität. Als weiteren Schritt führten wir den Workshop mit fünf Experten und Expertinnen für Datenschutz und Design durch. Die Ergebnisse des Workshops trugen dazu bei, die Aspekte zu definieren, die beim Erstellen von Design Patterns hervorgehoben werden sollten. Der erste Prototyp des Kartendecks „Designing for Privacy“ wurde von Datenschutzexperten und Datenschutzexpertinnen bewertet. Nach den Änderungsvorschlägen der Experten wurden die Design Patterns visualisiert und von vier Designern und Designerinnen evaluiert. Um zu definieren, ob entworfene Patterns auch für die Endbenutzer und Endbenutzerinnen verständlich sind, haben wir mit drei Teilnehmern und Teilnehmerinnen eine qualitative informelle Bewertung des datenschutzfreundlichen Webprototyps durchgeführt. Das positive Feedback der Experten und Expertinnen, der Endbenutzer und Endbenutzerinnen zeigt die Zweckmäßigkeit und Wirksamkeit des in dieser Diplomarbeit vorgeschlagenen Konzepts.

Abstract

Having come into force on May 25, 2018, the General Data Protection Regulation (GDPR) sets a new standard for processing, storing and protecting the personal data and privacy of EU citizens. The law requires businesses that operate online take actions to ensure that they process customer data in a fair way, that they clearly explain to customers how long their personal data will be used and stored, and that they receive valid consent from their customers to do so. As follows, in order to achieve GDPR compliance, companies need to rethink strategies for dealing with customer personal data and designing user privacy. While simple in theory, the GDPR turns out to be quite difficult to interpret and understand. In this thesis, we present the aid to guide designers through the process of creating GDPR compliant and privacy-friendly online systems. We began by examining existing approaches to achieving GDPR compliance. As the further step, we conducted the workshop with five privacy and design experts. The results of the workshop helped to define the set of aspects that should be highlighted while creating design patterns. The first paper prototype of the card deck ‘Designing for Privacy’ was evaluated by privacy experts. After having made changes according to the experts’ feedback, the design patterns were visualized and evaluated by four designers. To define if designed patterns are also understandable for the end users, we conducted a qualitative informal evaluation of the privacy-friendly web prototype with three participants. Received positive feedback from the experts and end users demonstrate expediency and effectiveness of the concept suggested in this thesis.

Contents

Kurzfassung	ix
Abstract	xi
Contents	xiii
1 Introduction	1
2 Existing Approaches to Make an Online Product GDPR Compliant	3
3 Workshop	7
3.1 Understanding the GDPR	7
3.2 Workshop Preparation	20
3.3 Conducting a Workshop	21
3.4 Analysis of Findings	21
4 Prototype of the Card Deck	35
4.1 Creativity Card Deck & Design Patterns	35
4.2 Analysis of Existing Card Decks	37
4.3 Ideation Process	41
4.4 Paper Prototype	43
4.5 Prototype Evaluation	45
5 Visual Design	49
5.1 Setting the Stage	49
5.2 Asset Library	50
5.3 Design of Cards	52
5.4 Design of Introduction Sheet & Case	55
6 Evaluation	59
6.1 Design Evaluation	59
6.2 Evaluation of the GDPR Compliant Web Prototype	62
6.3 Final Improvements	69
	xiii

7 Conclusion	71
7.1 Discussion	71
7.2 Summary	73
7.3 Limitations and Future Work	74
List of Figures	75
List of Tables	79
Appendix	81
Bibliography	121

Introduction

The EU General Data Protection Regulation (GDPR) [1], introduced on May 25, 2018, presented a lot of challenges for businesses that function online. The GDPR was designed to address the process of collecting and processing user data [2] [3], and to give the control over their privacy on the web back to the individuals [4]. It states that all organizations that collect, use or store customer data have to *”take appropriate measures to provide any information [...] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language [...]”* [1].

While simple in theory, practically, however, it is a little more complicated than that. Businesses need to adjust their existing privacy policy and the way it is presented online [3]. The GDPR requires companies to have a comprehensive understanding of all the data they collect and use, whether it is personal data or not [4]. This brings new challenges for the user experience (UX) and user interface (UI) designers, who have to rethink about the design of online systems.

The complexity of the privacy law raises the issue of understanding how to design an online product that is compliant to the GDPR [5]. What changes should be done in order to process to the data subject in a concise, transparent, intelligible and easily accessible form? What is clear and plain language for a user, and in which way the user interface should be changed to correspond privacy regulation? The aim of this work is to provide UX/UI designers with support and help in answering these questions, as well as in gaining a deep understanding of how to design for user’s privacy.

In order to identify a set of useful design patterns for making online products GDPR compliant, the next methodological approach was applied. At the beginning of the research, key issues of the GDPR and suitable articles from the experts in the privacy field were reviewed and investigated. In the further step, the workshop with privacy and UX/UI experts was conducted. Having based on the workshop’s findings, a prototype of design patterns was created and then followed by expert evaluation. After that,

the visual prototype of a privacy-friendly website was developed and tested with end users. Finally, visualized design patterns were improved according to the expert and user recommendations.

The rest of this work is structured as follows: Chapter 2 examines existing approaches to make an online product GDPR compliant. In Chapter 3 we describe a methodology of the research including a workshop with experts and analysis of findings. Chapter 4 represents the concept of the card deck ‘Designing for Privacy’, the prototype of the design patterns and its evaluation by privacy experts. Following Chapter 5 illustrates how the design patterns were visualized. In Chapter 6, we evaluate visualized cards by UX/UI designers and created GDPR compliant web prototype with end users. Finally, we draw a conclusion, define limitations of the project and discuss future work in Chapter 7.

Existing Approaches to Make an Online Product GDPR Compliant

Before a new EU Data Regulation Law (GDPR) was introduced on May 25, 2018, a lot of discussions about its completeness and challenges that it brings to the web have already been started. Those companies that do not comply will face penalties of up to 4% of their annual global turnover or €20 million, whichever is greater. Companies that attempt to hide the cyber-attack from customers could also face penalties [6]. Referring to a recent survey conducted by data management provider Solix [7], 22% of organizations do not realize they must comply with the GDPR if they hold EU and UK citizens' data, even if they are based outside of the EU and UK. Additionally, a government survey [8] has found that many companies are unprepared to comply with the GDPR, or completely unaware how its rules will affect them: *“Only one in four businesses in the construction sector are aware of GDPR, and awareness in manufacturing is also low. The finance and insurance sectors are said to have the highest awareness of the legislation.”* Based on this survey data, it is clear that the majority of organizations are not prepared to meet GDPR requirements. Such a statement raises the issue of the necessity to introduce alternative approaches that will help organizations with achieving GDPR compliance.

Several works have compiled different sets of patterns to address privacy issues from various angles. In one of the works about privacy transparency [9], the author created two privacy transparency patterns to help users with understanding how and what data are used by the system. In another research [10], the authors provided software engineers with the means to facilitate user privacy decisions in a manner consistent with the GDPR. By contrast, it has been addressed in [11], that so far, privacy is simply not a primary consideration for engineers when designing systems, but it should be embedded in system development life cycle from the beginning. There are also more concrete recommendations and explanations of how GDPR should be respected by UX/UI design [3] [12]. Their

focus is, however, primarily on user consent and user rights to manage or delete their data.

In turn, IT companies have already begun to develop and sell users new tools that can make their web services GDPR compliant. For example, Evidon's Trackermap [13] offers its customers an audit of all of the third party vendors on the site; the Contract Shop [14] sells for \$255 a template "GDPR Compliant Terms & Conditions + Privacy Policy for Your Website". The developers of the content management systems, from the other side, are also working on providing their users with GDPR compliant templates and plugins. One of the examples is an integrated into WordPress GDPR enhancement tool [15], that includes Comments Consent, Data Export and Erase Feature, Privacy Policy Generator, Contact Forms and other related to data privacy features. Because of the dynamic nature of websites, however, no single platform, plugin or solution can offer 100% GDPR compliance. Furthermore, suggested plugins work with concrete content management systems and cannot be applied to every website.

Another option to ensure that a website is GDPR compliant is to hire a GDPR consultant. Being very effective from the one side, this approach can be very expensive for the small businesses.

To sum up, there are several approaches to how to make an online product GDPR compliant:

1. Study the GDPR law
2. Follow experts' recommendations and best practices
3. Use already developed GDPR compliant templates and plugins for content management systems
4. Hire a GDPR consultant

Found advantages and disadvantages of existing approaches are represented in Table 2.1.

Overall, the problem of existing approaches is that they focus on a concrete issue (consent, cookies, privacy policy template) rather than on the whole process. Furthermore, the majority of suggested solutions have a lack of clear explanation or visual examples that can help UX/UI designers with making their concept design GDPR compliant. Thus, suggested in this work approach to create visual design patterns, represents a modern, promising and perspective solution to help UX/UI designers in the stage of creating a usable and user-friendly online product that complies with GDPR requirements.

Table 2.1: Analysis of existing approaches to make an online product GDPR compliant

Approach	Advantages	Disadvantages
Study the GDPR law	Learning from the legal source without interpretations from third parties.	Can cause difficulties in understanding and interpretation of legal language. Has a lack of clear explanation of how it should be applied.
Follow experts' recommendations and best practices	Provides readers with clear explanations of the law and the best practices examples that can help to understand the law better.	Offers rather separate solutions to the problem. Usually does not describe how to design a GDPR compliant online system.
Use existing compliant templates and plugins	Easy to use, automated and reliable solution.	Can be applied only to concrete content management systems.
Hire a GDPR consultant	Effective and reliable solution.	Can be very expensive especially for small businesses.

Workshop

This chapter will focus on the understanding of the core element of this thesis – General Data Protection Regulation. In Section 3.1 the main principles and aspects of the law will be discussed before the preparation for the workshop in Section 3.2, and conducting the workshop with privacy and UX/UI experts in Section 3.3. Findings of the workshop will be analyzed in Section 3.4.

3.1 Understanding the GDPR

Having introduced new regulation strengthens for data protection, the GDPR claims new and expanded privacy rights for over 500 million individuals in the EU [16]. The core idea of the GDPR is to reformat the way in which businesses collect, process and store user data. The businesses that operate online, must be sure that they have sealed consent management processes [2], that their data are processed in a fair and transparent way. The regulation represents an essential step to strengthen the rights of individuals on the web and to provide business with explicatory rules on how to achieve this [17].

This regulation establishes rules relating to the protection of individuals with regard to the processing of personal data, and rules concerning the free movement of personal data (Article 1(1)). By ‘personal data’ is meant “*any information relating to an identified or identifiable natural person (‘data subject’); [...] a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*” (Article 4(1)).

3.1.1 GDPR Principles

Regarding Article 5 of the GDPR, there are six principles that emphasize the GDPR aim to drive compliance:

1. Lawfulness, fairness, and transparency
2. Purpose limitations
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

The controller (a service/organization/the natural or legal person/public authority that processes personal data) shall be responsible for these principles, and be able to demonstrate compliance with them (Article 5(2)).

Lawfulness, fairness, and transparency

“*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*” (Article 5(1a)). This means that organizations need to make sure their data collection process does not violate the law and that they are not hiding anything from their users [18]. The personal data must be used in a fair way: the organizations should be clear and open with their customers; they should declare everything that they do with personal data of customers [19]. The description of how the data were processed must match how it was done [16].

Purpose limitations

Personal data can only be obtained for “*specified, explicit and legitimate purposes*” (Article 5(1b)). This means that data can only be used for a specific processing purpose [16]. Organizations must clearly specify each purpose of the data collection as well as keep collected data only for as long as it is required to complete that purpose. Explicit consent from the individuals must be obtained and recorded for each of the purposes. Organizations can use personal data for a new purpose if either this is matching the original purpose, they gain consent to, or they have a clear basis in law to do so [20].

Data minimization

Data collected on a subject should be “*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*” (Article 5(1c)). Organizations must ensure that the personal data they are processing match the stated purpose and that they do not keep more data than they need for that purpose [21]. In other words, no more than the minimum amount of data should be held for specific processing [16].

Accuracy

Personal data shall be “*accurate and, where necessary, kept up to date*” (Article 5(1d)). This principle requires good data protection [16]. If an organization discovers that personal data is incorrect or misleading, reasonable measures should be taken to correct

or remove it as soon as possible [22]. Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days [18].

Storage limitation

Personal data must be kept “*for no longer than is necessary for the purposes for which the personal data are processed*” (Article 5(1e)). Organizations must periodically review the data they store and remove or anonymize it when they no longer need it [16] [23].

Integrity and confidentiality

This is the principle that deals with data security. The GDPR states that personal data must be “*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures*” (Article 5(1f)). Organizations must take all necessary measures to fulfill this principle. The personal data must be protected in an appropriate (for example, by encryption). Encryption of data helps it to remain confidential and secure even in case if it falls into the wrong hands. It also reduces the breach impact for both organizations and individuals whose data it is [24].

Overall, these principles set a foundation about data protection by design and by default. When developing, designing, selecting and using applications, services and products that are either based on the processing of personal data or process personal data to fulfill their task, data protection should be considered to make sure controllers are able to comply with their data protection obligations [25]. Thus, to demonstrate compliance, organizations should adopt internal privacy policies and implement measures, which meet discussed earlier principles of data protection by design and data protection by default.

From the other side, there is still a range of nuances of consent and other articles of GDPR, complexities and coordination activities associated with implementing a program to meet GDPR compliance [16]. Such topics include privacy policy, cookies, consent, user rights and will be discussed in the following subsections.

3.1.2 Privacy Policy

A privacy policy is a document that declares the ways how organizations collect, use, store, releases and manage customer personal data. It corresponds to a legal requirement to protect user privacy. In other words, the privacy policy supplies users with information about what data is collected, and whether it is kept confidential, shared with partners or sold to other companies [26]. In order to comply with the principle of fair and transparent processing of GDPR, organizations should disclose to their users the information stated in the GDPR [27].

According to Articles 13-14 of the GDPR and basing on the research [28], when the personal data of data subject are collected, all of the following information should be provided:

- What data are collected? (What is the type of data you store about me? What content do these data have, where did they come from, what are they processed for, to whom were they transmitted or are they still being transmitted?)
- What is the purpose of the data collection?
- Where are the data stored?
- How long are they kept? (How long do you save my personal information? If no time is provided, what criteria have you set for the duration?)
- Who has access to the data? (To whom was or is this data transmitted?)
- What do the data look like? (Which nature of data is processed? What are the contents of this data?)
- How to access the data?
- How to erase the data? (When will the final deletion of the data occur?)
- How frequently are the data sent?
- Which communications are protected?
- What paths do the data follow?
- What information does the device receive from other sources?

Organizations will need to supply their customers with more comprehensive information in their privacy notices relating to how they process personal data. All processing activities will need to be transparent [27].

The objective of this thesis, however, is not to discuss each information point that should be stated in the privacy policy, but to understand how such volume of information can be presented to the user “*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*” (Article 12(1)). As one of the good examples to tell users about their privacy issues is Google Privacy & Terms (see Figure 3.1): supported by illustrations and explanation videos, Google’s Privacy Policy tries to convey to the user in a simple way how do they collect and process user personal data.

By contrast, H&M provides its customers with a long privacy notice text (see Figure 3.2), that would be barely read by them.

Overall, the privacy policy is a complex issue that introduces a range of challenges to the designers: how to deal with the huge value of unstructured content in the privacy policy? We do not want to overload the visual design or include too many steps to the user journey, but at the same time, still need to communicate complex ideas. This challenge will be discussed with experts during the workshop.

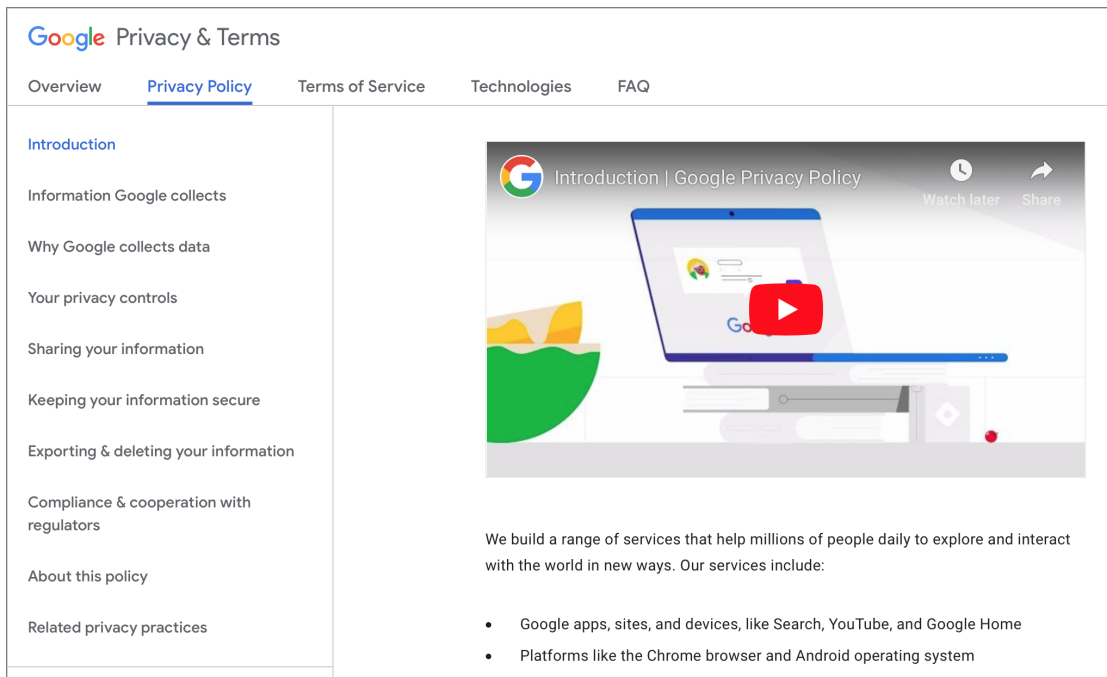


Figure 3.1: Google Privacy & Terms

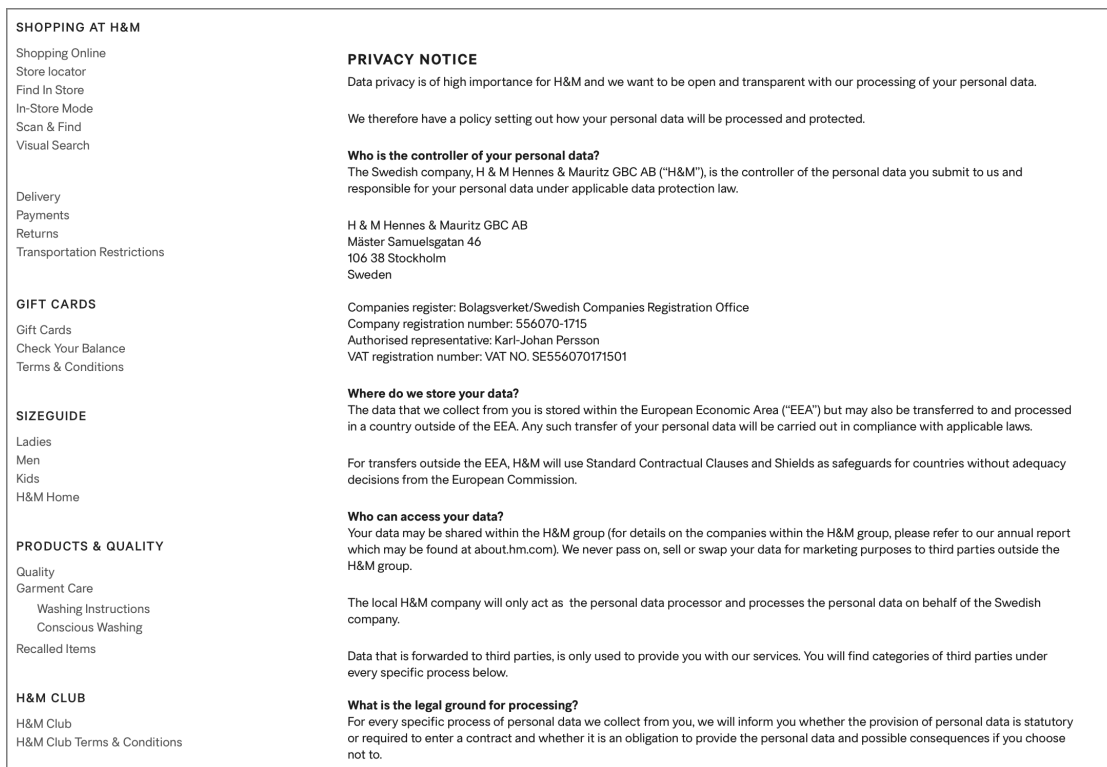


Figure 3.2: H&M Privacy Notice

3.1.3 Data Subject's Consent

Processing personal data is generally prohibited unless it is expressly allowed by law, or the data subject has consented to the processing. The GDPR defines 'consent' as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*" (Article 4(11)). The element 'free' means that the consent is invalid if there is any element of pressure that can influence the data subject's decision.

Under specific and informed consent means that the data subject should be provided with all the necessary information about the controller's identity, the type of data that will be processed, what is the purpose of the processing and how it will be used [29].

Consent must be unambiguous, it cannot be implied and must always be given through an opt-in. The recitals of the regulation highlight that such action should include "*ticking a box when visiting an internet website, or choosing technical settings for information society services*" (Recital 32). One of the examples of an opt-in is shown in Figure 3.3: by selecting 'Accept' or 'Decline' button, the data subject can consent or deny the use of cookies on the website. Another example represents a form for subscribing to a newsletter (see Figure 3.4): the button 'Yes, sign me up' is inactive till the data subject gives his or her consent for their data to be stored and processed.

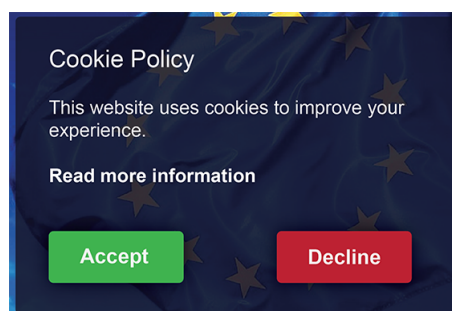
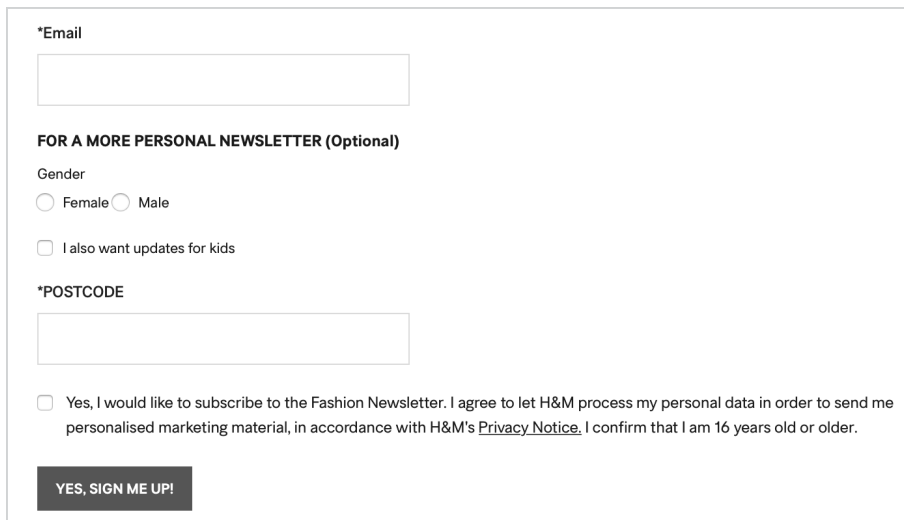


Figure 3.3: Opt-in cookies bar

It is also important to understand that consent should be distinguishable from other matters and, thus, never bundled with other terms and conditions: "*If consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters [...]*" (Article 7(2)). This means that consent request should be separated from general terms and conditions; one purpose – one consent [30]. For example, while sending a newsletter, each purpose should be clearly specified to the subscribers: if there is a subscription for both a company and its subsidiaries or partners, separate consent tick-boxes are needed (see Figure 3.5) [31].



***Email**

FOR A MORE PERSONAL NEWSLETTER (Optional)

Gender

Female Male

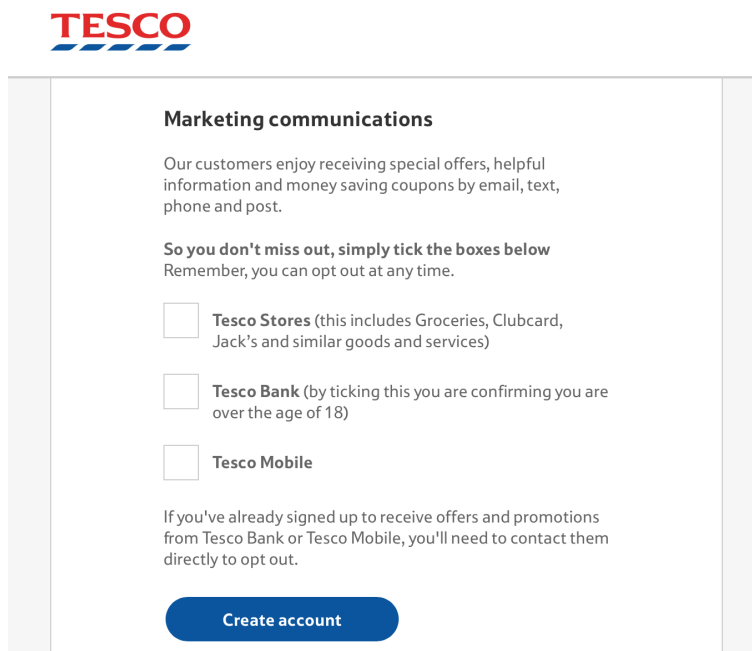
I also want updates for kids

***POSTCODE**

Yes, I would like to subscribe to the Fashion Newsletter. I agree to let H&M process my personal data in order to send me personalised marketing material, in accordance with H&M's [Privacy Notice](#). I confirm that I am 16 years old or older.

YES, SIGN ME UP!

Figure 3.4: Newsletter form of H&M with an agreement consent



TESCO

Marketing communications

Our customers enjoy receiving special offers, helpful information and money saving coupons by email, text, phone and post.

So you don't miss out, simply tick the boxes below
Remember, you can opt out at any time.

Tesco Stores (this includes Groceries, Clubcard, Jack's and similar goods and services)

Tesco Bank (by ticking this you are confirming you are over the age of 18)

Tesco Mobile

If you've already signed up to receive offers and promotions from Tesco Bank or Tesco Mobile, you'll need to contact them directly to opt out.

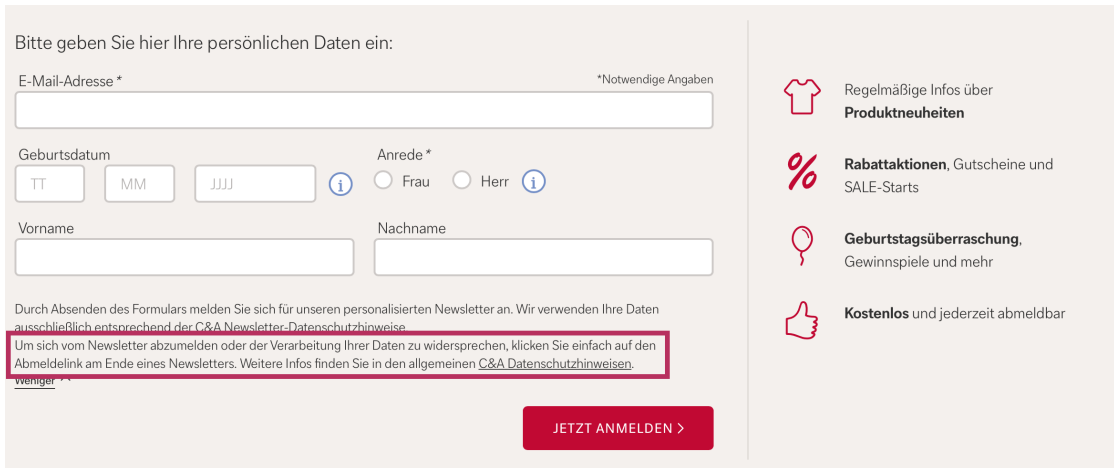
Create account

Figure 3.5: Separate consent for three different email lists

At any time, the data subject must have the right to withdraw consent. Organizations must respond and act upon the request in a reasonable timeframe [32]. The withdrawal must be as easy as giving consent [29]: “*The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness*

3. WORKSHOP

of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.” (Article 7(2)). This means that, firstly, before consent is given, the data subject should be informed about the possibility and the way he or she can withdraw it (see Figure 3.6).



Bitte geben Sie hier Ihre persönlichen Daten ein:

E-Mail-Adresse * *Notwendige Angaben

Geburtsdatum Anrede*

TT MM JJJJ i Frau Herr i

Vorname Nachname

Durch Absenden des Formulars melden Sie sich für unseren personalisierten Newsletter an. Wir verwenden Ihre Daten ausschließlich entsprechend der C&A Newsletter-Datenschutzhinweise.

Um sich vom Newsletter abzumelden oder der Verarbeitung Ihrer Daten zu widersprechen, klicken Sie einfach auf den Abmelde-link am Ende eines Newsletters. Weitere Infos finden Sie in den allgemeinen C&A Datenschutzhinweisen.

[weniger](#)

JETZT ANMELDEN >





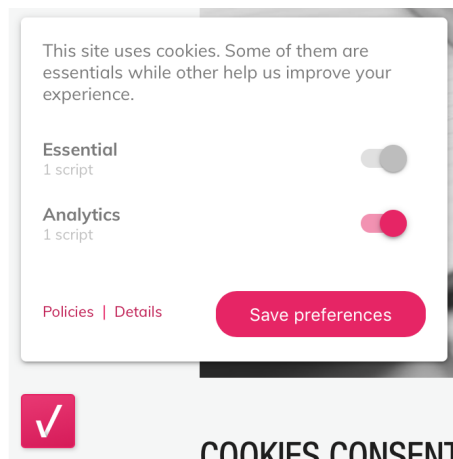
-  Regelmäßige Infos über **Produktneuheiten**
-  **Rabattaktionen**, Gutscheine und SALE-Starts
-  **Geburtsüberraschung**, Gewinnspiele und mehr
-  **Kostenlos** und jederzeit abmeldbar

Figure 3.6: Subscription form with the information how a newsletter consent can be revoked

Secondly, if the consent was given over the online form, a company should provide an online form for withdrawing consent as well. Figure 3.7 shows an example of how the data subject can withdraw cookie consent at any time, as easily as it was given.



This site uses cookies. Some of them are essentials while other help us improve your experience.

Essential
1 script

Analytics
1 script

[Policies](#) | [Details](#) **Save preferences**


 **COOKIES CONSENT**

Figure 3.7: Opt-out cookies bar with the possibility to withdraw cookies anytime

To revoke a subscription to a newsletter, the data subject can easily do it in the same form that he or she subscribed to it (see Figure 3.8).

The image shows two side-by-side screenshots of a website's email subscription and unsubscribe forms. The left form is for subscription, and the right form is for unsubscribing.

Subscription Form (Left):

- Text: "Abonnieren Sie unseren Newsletter, um alle Neuigkeiten, Trends, Angebote und Aktionen für Ihr Zuhause zu erhalten."
- Input field: "E-Mail *"
- Checkbox: "Ich willige ein, kundenspezifische Werbemittelungen von ZARA HOME per E-Mail und anderweitig zu erhalten"
- Button: "ABONNIEREN"
- Link: "Nein danke. Ich möchte mich abmelden >"

Unsubscribe Form (Right):

- Text: "Geben Sie Ihre E-Mail-Adresse ein, wenn Sie keine Neuheiten und Angebote mehr erhalten möchten. Sie können sich jederzeit wieder anmelden. Wir werden Sie vermissen!"
- Input field: "E-Mail *"
- Button: "ABBESTELLEN"
- Text: "< Ich habe es mir anders überlegt. Ich möchte mich anmelden."

Figure 3.8: Subscription and unsubscribe forms can be found in the same place on a web page

To sum up, consent is one of the vital elements of the GDPR, that should not be left without attention. It requires a lot of clear explanation about what happens to the personal data, and gives users a free right to agree or disagree with his or her data to be processed.

3.1.4 Cookies

A cookie is a small chunk of data generated by a Web server to store information about a user on the user's hard disk. The stored in cookie information might be, for example, the information about the purchases a user made in the past. Later, when the user returns to the website, the website's software can retrieve the cookie-based data and use the data to create a custom page that contains products similar to those the user has purchased in the past [33].

Websites use cookies to [34]:

- Monitor user's path through a website to keep track of the pages the user viewed or the items he or she purchased
- Gather information that allows a Web server to present ad banners targeted to products the user previously purchased at that website
- Collect personal information the user submits to a web page, and retain it for the next time the user visits the website
- Verify that the user has logged in to a site using a valid user ID and password, if necessary

As an example, in a cookies policy of Amazon states "*We use cookies to recognize your browser or device, learn more about your interests, and provide you with essential features*

and services and for additional purposes [...] to provide you with product recommendations, display personalized content, recognize you as a Prime member, enable you to use 1-Click purchasing, and provide other customized features and services.” Thus, by ordering some products on Amazon, users will receive a list of products recommended for them basing on their previous purchasing (see Figure 3.9).



Figure 3.9: Amazon’s recommendations based on cookies

As we see, cookies can be used to uniquely identify a person, therefore they should be treated as personal data. That means that, first of all, users must be given a choice [35]. The fact that they use a website does not mean that they agree to all cookies. The type of phrase such as “By using this website, you accept cookies” (see Figure 3.10) widely used at the moment is not informative enough and it does not give users a choice (see Figure 3.11). Users should not be forced to accept cookies in exchange for information.

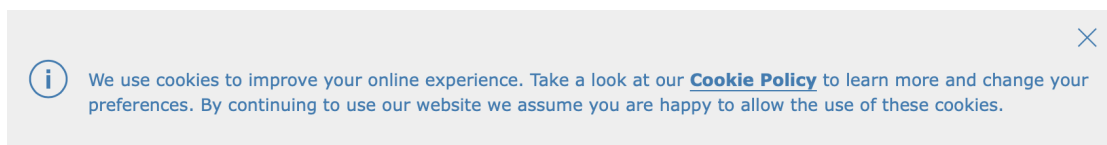


Figure 3.10: Classic cookie hint bar without the possibility to decline to store cookies

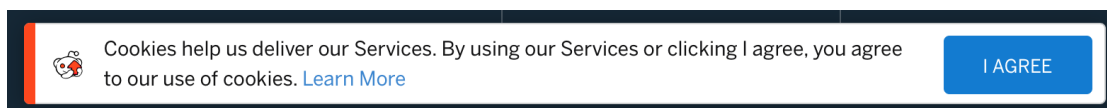


Figure 3.11: Classic cookie hint bar without positive opt-in

Secondly, like all other consent under the GDPR, consenting to cookies needs to be a clear affirmative action. An example is clicking through an opt-in box or choosing settings from the menu (see Figure 3.12).

A good example would be to present users with the option to select the level of consent they want to give (see Figure 3.13). The website should not have pre-ticked boxes on the cookie consent form.

Finally, according to the GDPR, users should be able to withdraw consent as easily as they gave it (opt-out). For cookie agreement, this means that users should be able to

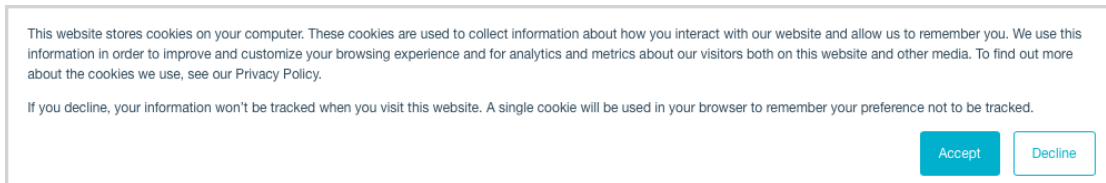


Figure 3.12: Cookie bar with opt-in box to decline the use of cookies

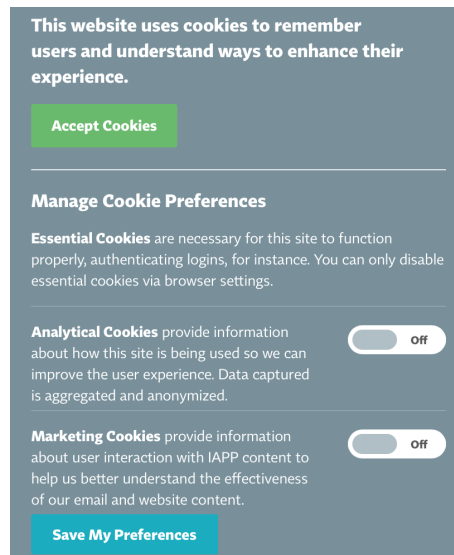


Figure 3.13: A cookie bar with the option to choose the level of consent

revoke consent through the same action as when they gave consent. For example, if they consented by clicking through the settings, they have to be able to find the same settings form to revoke consent (see Figure 3.14).

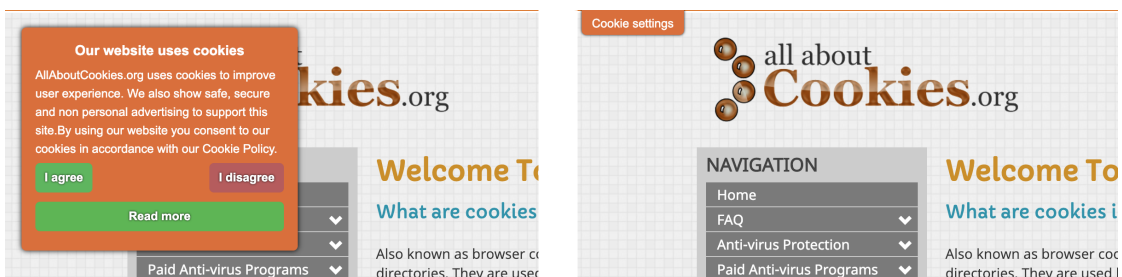


Figure 3.14: Withdrawal of the consent from the same settings window where the consent was given

As it was already mentioned earlier, web cookies can be divided into different categories [36] [37]. Some cookies are strictly necessary for the normal functioning of the

website. These cookies cannot be disabled because the website will no longer work properly [35]. However, these cookies do not store any personal data of users.

Cookies used for analytics are not required for the operation of the website, they are used to track user's performance. As follows, they cannot be imposed on users: users should be able to disable them at any time [35].

Most of the functional cookies are provided by third parties, they are optional and can be disabled by users. For example, if Vimeo or Youtube are used to show videos on the web page, the switching off their cookies will mean that the videos may not work [35].

Advertising or marketing cookies are optional. They are usually used by the advertising partners to define a profile of users in order to supply them with personalized ads on other websites [37].

Designers need to proactively highlight the information about used cookies in a clear way. The data subject should understand that some cookies cannot be switched off while others are optional. Third party cookies need the most attention: the data subject should be aware of each third party and its purpose to store and process the personal data. Figure 3.15 shows Cookie Policy of designmodo.com, where the organization explains which third party cookies are collected and why.

Overall, when cookies can identify an individual via their device, it is considered personal data. Thus, to collect, store and process these data, organizations have to get consent from the data subjects by offering them clear choices around cookies. The data subjects should be provided in a clear and transparent way with all necessary information about cookies the website uses; they should be given the possibility to withdraw their consent as easy as it was given.

3.1.5 Right to Be Forgotten

The GDPR gives data subjects more control by enabling them to object to processing which is based on the legitimate interests of the controller or a third party (including profiling based on that ground) [27]. The data subject shall have “*the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay*” where special grounds applied (Article 17(1)). Thus, data subjects have the right to erasure, also known as ‘the right to be forgotten’ (Article 17). The scenarios under which users can request their data erase are mentioned in Article 17(1).

For the privacy by design, the ‘right to be forgotten’ means that users should be provided with transparent information about their rights together with an option to submit a quick and simple request to change or remove their data. One of the good examples of such option is already applied in iCloud (see Figure 3.16). The service provides its users with a range of functions for managing their personal data: get a copy of the data, correct the data, deactivate or delete an account. A user can get an overview of all personal data stored on iCloud, as well as make a request about his or her data to be erased. After the

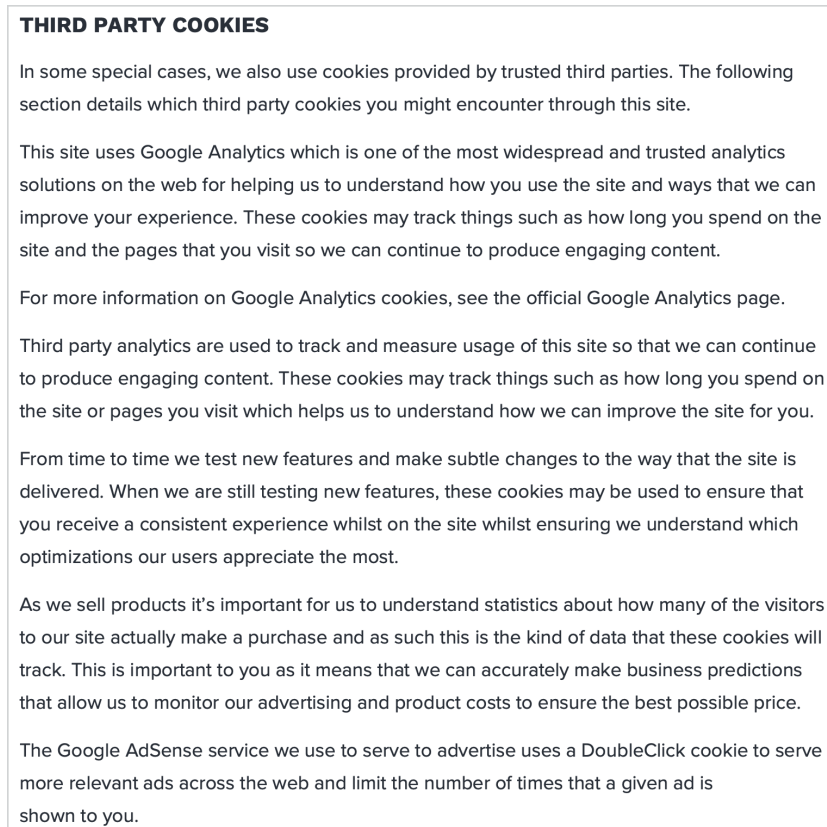


Figure 3.15: Information of third party cookies used at designmodo.com

user makes a request about deleting his or her account, he or she will get information about the process and notification once the account is deleted.

Overall, ‘right to be forgotten’ provides the data subjects with the possibility to have their data deleted with no grounds for retaining it.

3.1.6 Data Breaches

According to Article 34 GDPR, “*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*”. That means that if a data breach or hack to personal data occurs, organizations have to provide their customers with information that their data has been compromised. Organizations are required to notify the appropriate national bodies as soon as possible in order to ensure their users can take appropriate measures to prevent their data from being abused [38]: “*In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority [...]*” (Article 34).

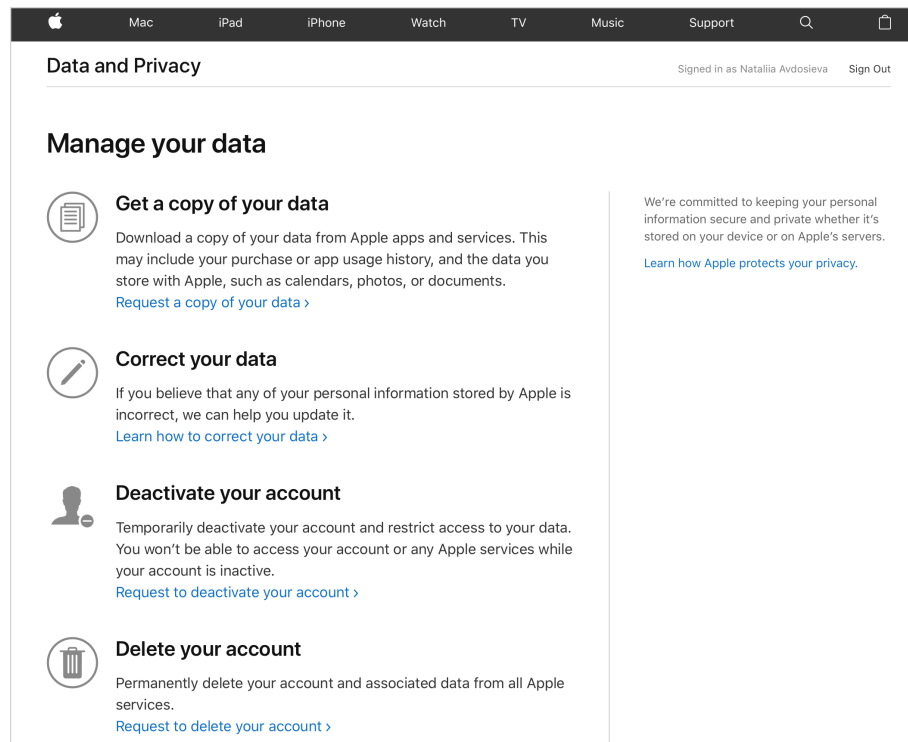


Figure 3.16: Managing personal data at iCloud

To sum up, the written above section demonstrates the complexity of the GDPR and highlights critical moments and challenges on the way of making an online product GDPR compliant. Knowledge and experience obtained by a deep literature review will further be investigated and discussed during the workshop with experts in privacy, user experience and design fields.

3.2 Workshop Preparation

To gather valuable information and asquire a deep understanding of GDPR compliance, a workshop as a method was chosen. The reason to conduct a workshop was that it could provide a way to find the real answers, discover new ideas and introduce new concepts, spurring participants with different experience to investigate it together in a short amount of time. Rather than just a simple set of interviews with questions and answers, an informal workshop is a good deal of discussion in addition to participation.

The preparation to the workshop started with defining main use cases to be discussed with experts. Basing on the deep literature review, a workshop guideline with 11 use cases was made (see Appendix A). Grouped in five categories such as Transparency, Privacy Policy, Cookies, Forms & Consent, Manage Personal Data, each use case represents a

real scenario of users' activity on the website and is supported by bad and good visual examples.

A plan of the workshop is to review and discuss prepared in advance bad and good use cases; to suggest and analyze possible solutions and improvements of reviewed cases; to try to define a set of practical tips, patterns that can help to design GDPR compliant online systems. A format of the workshop is informal. Since it is expected that participants know each other, it would be easy to conduct the workshop as a friendly meeting, but take into account that everyone will get some personal attention and the chance to be heard.

3.3 Conducting a Workshop

The workshop was conducted with five participants – colleagues from the consulting company “Usecon”. Two of the participants were privacy experts, two – user experience experts and one – UX/UI designer. The workshop was provided with the following materials: examples of designs, a dashboard for ideas, stickers, markers, a laptop, and a projector. The duration of the workshop was about two hours.

At the beginning of the workshop, all of the participants were informed about the format, goal, agenda, and rules of the workshop. During the workshop, the participants had the possibility to tell and discuss their own ideas, as well as draw their solutions on the dashboard. After the discussion of concrete use cases, the participants were given a chance to describe their feelings and thoughts about the idea to have an aid that can help them in designing GDPR compliant websites.

All comments, ideas and recommendations made by the participants were recorded and noted. There was an equal part of the involvement of each participant in the conversation and heated discussion. It is also worth to mention that in most cases participants were complementing each other with one main idea rather than arguing about controversial issues. The workshop ended with recapping what has been done, what has been achieved and a definition of next steps and tasks. All gathered findings in form of ideas, solutions and recommendations were then documented for the further analysis.

3.4 Analysis of Findings

All findings of the workshop discussions are grouped into five main topics: transparency, privacy policy, cookies, consent, manage personal data. Together with the last part of the workshop ‘Feeling and Thoughts’, findings will be represented in the following subsections.

3.4.1 Transparency

While during the literature review it was found that introduction pop-up (see Figure 3.17) with a short message “We care about your privacy” is a great idea because “*it immediately*

3. WORKSHOP

gets the user's attention and notifies them about privacy policy updates in a friendly manner" [12], participants criticized this move. First of all, a pop-up window that greets the visitors at the beginning can be really annoying. If we think about a user who visits a hundred websites per day, and each of these websites greets this user with a pop-up, we can imagine how sick and tired the user will be already after third such a pop-up. Secondly, users are not paying attention to pop-up windows anymore: "users prefer to quickly close it and continue browsing web page rather than read some text in this intro message." Especially when users see a huge volume of continues text, the probability that it will ever be read is really small.

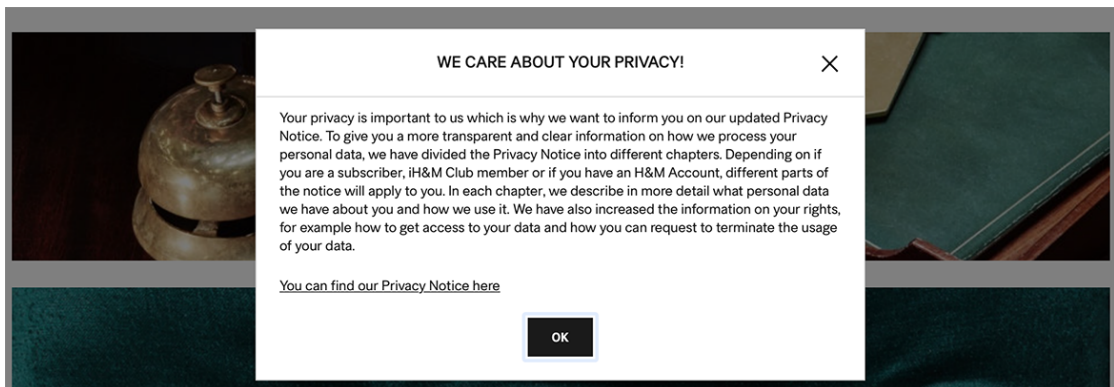


Figure 3.17: Introduction pop-up with a short message about the privacy policy of H&M

As possible improvement, one of the privacy experts mentioned the necessity to interact with the users and convince them to visit your website later by: "informing users in a few words what data you are recording from them, what benefits they will get after allowing you to record their data, what do they lose when they disagree; think about wording and representation of information: use pictures, bullets, short message." (see Figure 3.18).

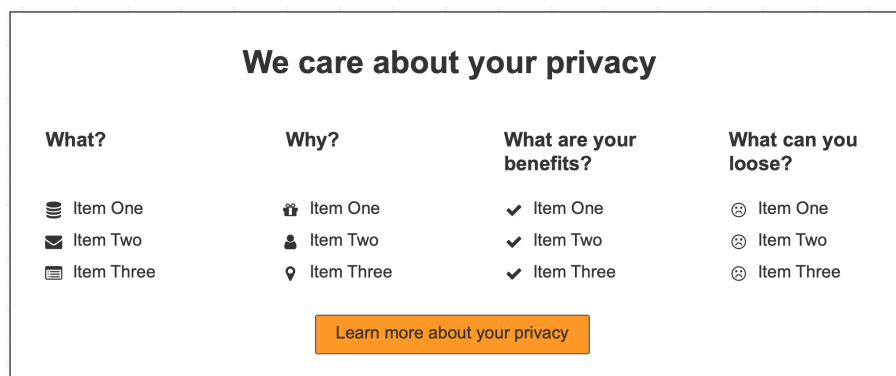


Figure 3.18: Solution to introduction message

3.4.2 Privacy Policy

The issue about a privacy policy got the most attention from all participants. They mentioned that the placement of the link to the privacy policy should be consistent at all websites, so users can easily find it no matter on which web site they are now. Basing on user experience, the most expected place for the privacy policy link is in the footer. In addition, the participants agreed that it can be great and transparent move to give users the overview of privacy issues (see Figure 3.19), however, only when it has a positive character.

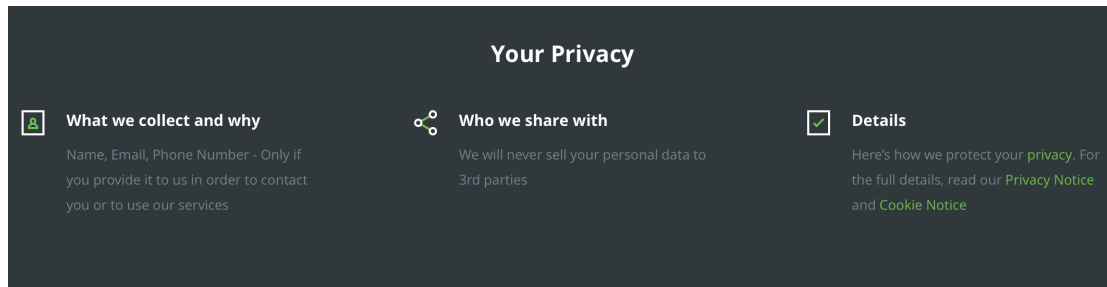


Figure 3.19: Short overview of user privacy, located in the footer of the web page

The experts also found it as a bad practice to use another resource (website) with a privacy policy: *“do not bring a user to another website with the privacy policy, since it can cause misunderstanding and feeling that something is wrong.”*

A considerable discussion was triggered by a problem of how to motivate people to care about their privacy issues more: *“Users stopped paying attention to what they agree. Nobody reads the privacy policy before clicking ‘I accept’”* – stated a privacy expert – *“similar to cigarettes package with the warning ‘smoking is killing’, people attend not to pay attention to such messages anymore. There should be a trigger that will motivate people to think about their privacy, what data they share and why.”* Experts, however, could not formulate what exactly should be done to increase users motivation.

Speaking about long privacy policy texts, participants cited that one of the main problems of this is that they are written by a lawyer for a lawyer. This decreases the probability that users will read and understand the language. *“By writing these texts, we should think about User Centred Design and people who will actually read them instead of trying to write something in ‘legal’ language.”* – stated an experience expert. As a worthy example, participants highlighted Google Privacy Policy (See Figure 3.20): *“the policy is well-structured, each privacy issue of Google is written in the user-to-user language and, in addition, it is provided with short videos as explanations.”*

Since a privacy policy tends to change and updates with time, users should be always informed about the history of changes (see Figure 3.21).

During the discussion, a UX/UI designer suggested an alternative to the written privacy policy: *“It would be nice if a website can have some Chabot: a user can ask a question about*

3. WORKSHOP

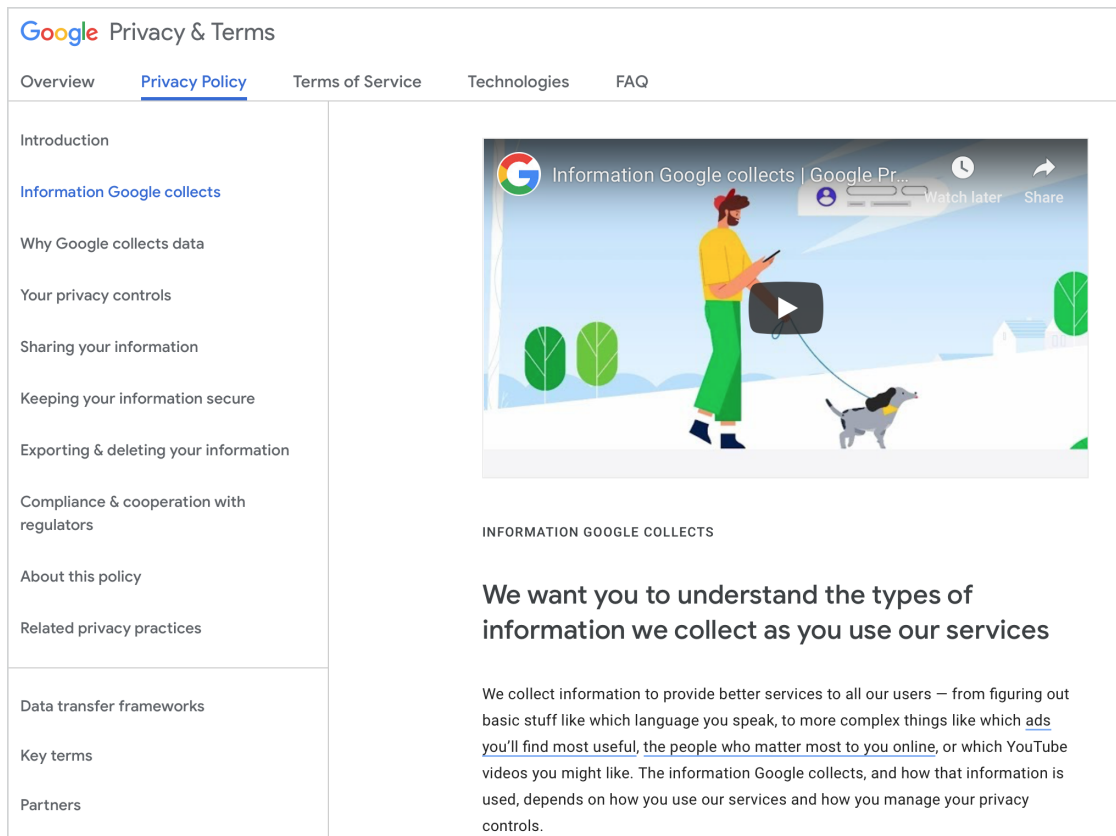


Figure 3.20: Representation of Privacy & Terms by Google

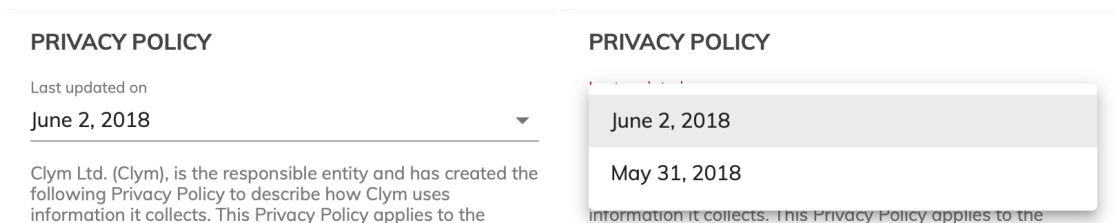


Figure 3.21: Privacy policy history

its privacy and receive a fast and concrete answer from the Chabot.” The implementation of such a Chabot would be, however, complicated and time consuming. Another idea was to have a web browser extension (similar to the Ad Blocker), where “*users can set up their own privacy policy once for all websites and then get a message if it is followed or not. For example, green sign – if everything is okay; yellow – when the privacy is partly followed with information what is not; red – when there is a serious violation of user rights.*” This solution, however, does not change the fact that each website will still have to provide its users with the detailed privacy policy. From the other side, in addition to

the clear privacy policy, organizations can provide their customers with the possibility to contact service about their privacy concerns: customers may use a contact form to send their concerns regarding privacy-related issue (see Figure 3.22).

The screenshot shows a web form titled "Privacy concerns" on the GitHub website. On the left is a navigation menu with links: "Contact GitHub", "Get help with GitHub", "Report abuse", "Report content", "Copyright claims (DMCA)", "Privacy concerns" (highlighted), "Premium Support Portal", and "Business Support Portal". Below the menu is a note: "Reporting a security vulnerability? Please review our [Responsible Disclosure Policy](#)." The main form area has the heading "Privacy concerns" and a sub-heading "Contacting GitHub about privacy concerns". Below this is a paragraph of text: "Please read GitHub's [Privacy Statement](#). It contains a lot of information about how we collect, use, and share the information we have, and how our users can access and delete their data. Our Privacy Statement may answer your questions." The form contains several input fields: "Name" with a placeholder "Your name", "Email" with a placeholder "Your email address", and "Subject" with a placeholder "Privacy concerns". Below these is a large text area for "How can we help?" with a placeholder "Please be sure to include your country of residence." At the bottom right of the form is a green button labeled "Send request".

Figure 3.22: Privacy concerns

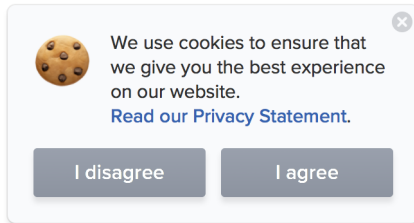
3.4.3 Cookies

The findings of this section include a lot of violation and misunderstanding issues referring to the cookie bar, cookie policy, and information about third parties. When in the GDPR it states that the processing of user data requires a freely given consent, most of the websites continue ignoring this rule. One of the bad examples is a cookies bar with a message 'Pay or Okay (see Figure 3.23). According to this cookies bar, a company handles cookies without users consent and, furthermore, tries to charge users with a fee for not doing so.

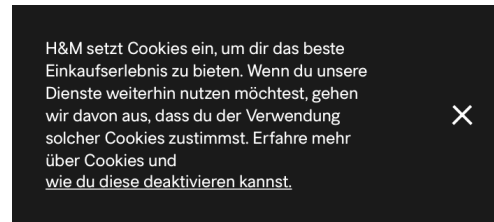
The screenshot shows a dark grey cookie bar with white text. The text reads: "Ich stimme der Verwendung von Cookies zu. Sie können unsere Website auch werbefrei*, also ohne die Verwendung von Werbe-Cookies nutzen." Below this is a smaller line: "*ausgenommen Native Advertising (Advertorials) und Pre-Rolls". At the bottom right are two buttons: a red button labeled "PAY" and a green button labeled "OKAY", with the word "oder" between them. At the bottom left, it says "Weitere Informationen finden Sie in unserer [Datenschutzrichtlinie](#)."

Figure 3.23: Non-compliant cookies bar that forces users to share their data if they do not want to pay for the browsing a website

Another less harmless, but still confusing cookies bars are shown in Figure 3.24. Both examples raised next questions among the participants: “*what in fact happens when a user just closes cookies window? Will the personal data be still collected or not? Does the website collect users data if they do not interact with cookies bar at all?*” Furthermore, it is not clear how users can withdraw their cookies consent after they close the cookies bar.



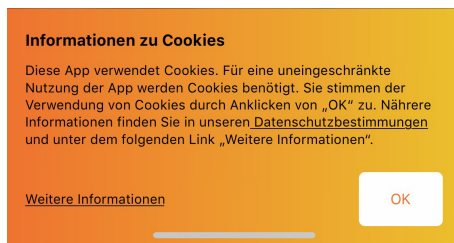
(a) Cookie bar with the possibility to disagree all cookies



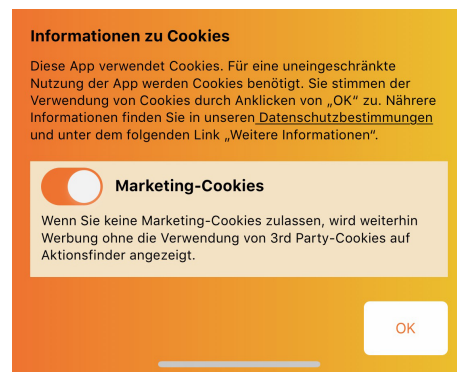
(b) Cookie bar with a link to information how to turn cookies off in the browser

Figure 3.24: Cookie bars

One more non-compliant example can be seen in Figure 3.25: the possibility to configure cookies is bundled in ‘Additional Information’ window (Figure 3.25b). Furthermore, all cookies are active by default.



(a) Classic cookie bar with a link to more information



(b) Cookie information window with configuration function

Figure 3.25: Cookie bar with a hidden configuration function

To avoid such confusing cookies bars, participants suggested providing users with a clear short message about their privacy and the possibility to configure the cookies (see Figure 3.26). If users do not do anything or select close the pop-up, it is clear, that their rights are not violated.

After users set up their choice, there should be the possibility to change it (withdraw the consent) as easy as it was made. One of the worthy examples for opt-in is represented as a sticky button (see Figure 3.27): users can select a sticky button and change their cookies settings any time.

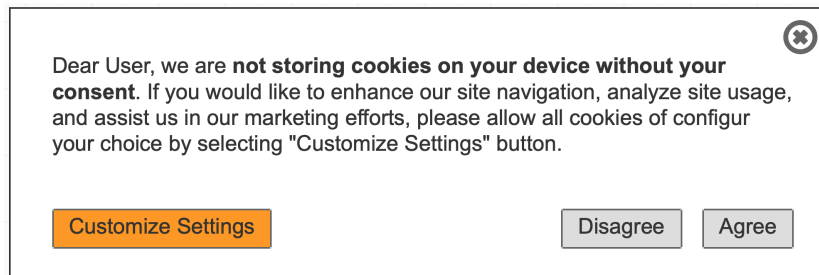


Figure 3.26: Solution to the compliant cookie bar



Figure 3.27: A sticky button with an option to change cookies preferences any time

The arrangement of cookies into intelligible categories: functional, analytics, performance, marketing, etc. was marked by experts as a good practice. The grouping cookies into categories and explaining the purpose of each of them can be an easy and transparent way to get users consent. Cookie categories that do not handle personal data may be pre-checked (necessary for the website to function properly), whereas those that do, must be actively opted into by the user to be compliant (see Figure 3.28).

Some participants, though, mentioned that if every website will provide the same functionality, it can be annoying for users to set up cookies at any website they visit. One of the participants mentioned: *“I would prefer to set up my choice for cookies once for all websites I visit and never again. I would like to have an app similar to the ad blocker, where I can save my preferences once and say ‘do not share my data with any web pages’, and the possibility to create some list with trusted websites, which I will allow to use my data (for example, my camera or microphone, etc.)”* Thus, the idea of doing it once in browser does not sound wrong. However, users still should be informed that even without setting up their cookies in the browser or by using some browser extension, their personal data are not processed.

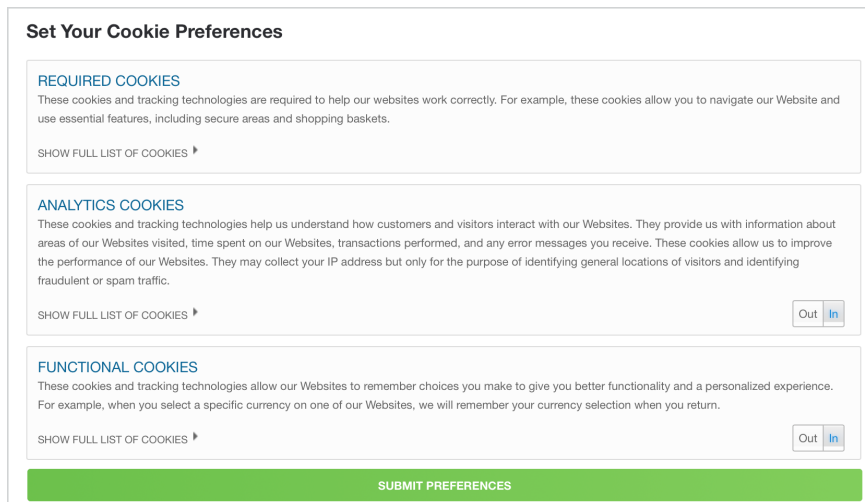


Figure 3.28: Cookies configuration window with the cookie arrangement

When the case about cookies configuration was under discussions, another challenge was recognized. Some of the websites share users data with third parties as well. Furthermore, the number of these parties can be extremely large. The GDPR requires transparent representation of all third party cookies. Even though some companies provide users with this information, the representation of third parties details does not respect GDPR law. In Figure 3.29 it can be seen that in order to read detailed information about each company a website shares data with, a user has to open every company block separately. Such an approach originally intended that people will not read the information about third parties.

Company	Domain
+ AOL Advertising	advertising.com
+ AdStir	ad-stir.com, syn...
+ AppNexus Inc.	ib.adnxs.com
+ Facebook Inc.	connect.facebo...
+ Google Inc.	doubleclick.net,... Show All
+ IPONWEB GmbH	bidswitch.net
+ Improve Digital International BV	ad.360yield.com

Figure 3.29: Information about each third party is represented as an expandable box

In another example (see Figure 3.30), a website uses pre-selected checkboxes for each partner of the company by default. In order to configure the cookies, a user has to manually unselect every checkbox. This approach is an example of outrage.

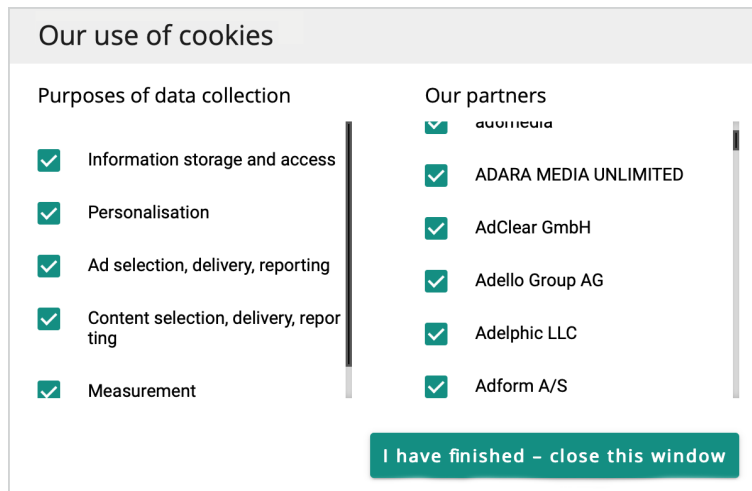


Figure 3.30: Usage of pre-selected checkboxes for each third party and purpose

In the end, the participants mentioned that it was difficult to define the best way to show all third parties and their information, however, the overall picture of all parties should be clear for a user at first sight: *“Are there 3 or 500 of them? What are the primary purposes and types of the data they process and store?”* Otherwise, users preferred to have an option to select/unselect the groups of third parties in a simple way. The possible solution to the cookie declaration is shown in Figure 3.31.

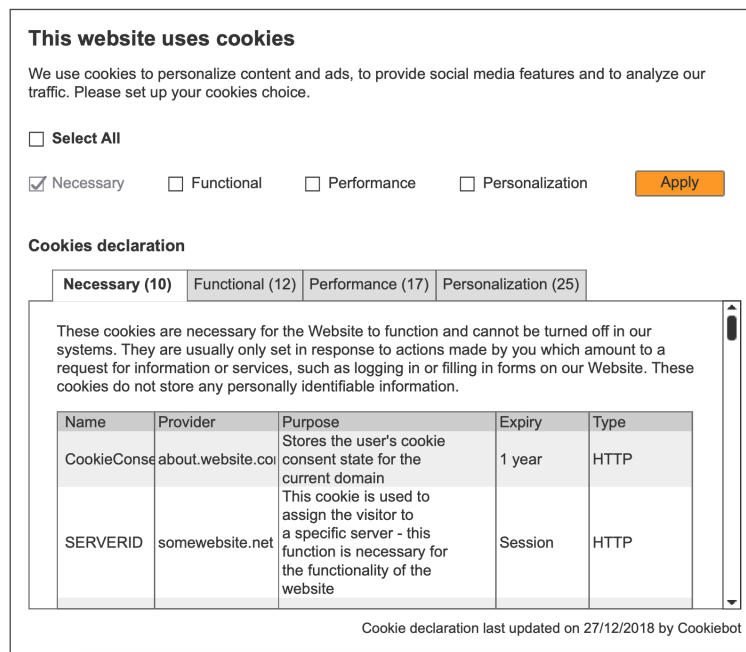


Figure 3.31: Solution to third party cookies declaration

3.4.4 Consent

During the discussion about a newsletter and other types of subscription, experts stated that two-steps subscription with ‘email field’ and button ‘OK’ (see Figure 3.32) can be confusing: “*Users do not expect that they will go to another page after they select OK button. This raises an issue about their privacy and misunderstanding in what will happen to their data next.*”

(a) Step 1: Enter an email

(b) Step 2: Fill the subscription form

Figure 3.32: Two-step subscription to a newsletter

While speaking about the consent, the participants were trying to define the most effective way to explain users what they give their consent for: “*From the one side, it is good to have a full information about the consent, without extra link, since the probability that a user will go to this link is really small. From the other side, short texts can look incomplete (see Figure 3.33) while long texts can look unfriendly.*” As a solution to this issue, the participants offered to provide users with a link to the full information about the consent and make the button ‘Send’ available only after a user at least opened this link.

Figure 3.33: Consent agreement with a link to full information

For a newsletter subscription, the participants agreed that it is a good idea to give users the possibility to set up what they want to receive (see Figure 3.34), otherwise after information overload they will probably just unsubscribe the whole newsletter. Furthermore, if it is expected that a company sends newsletters every day, users should be given the possibility to configure this option as well: “*Periodicity of a newsletter is also a good way to make emailing less annoying for users.*”

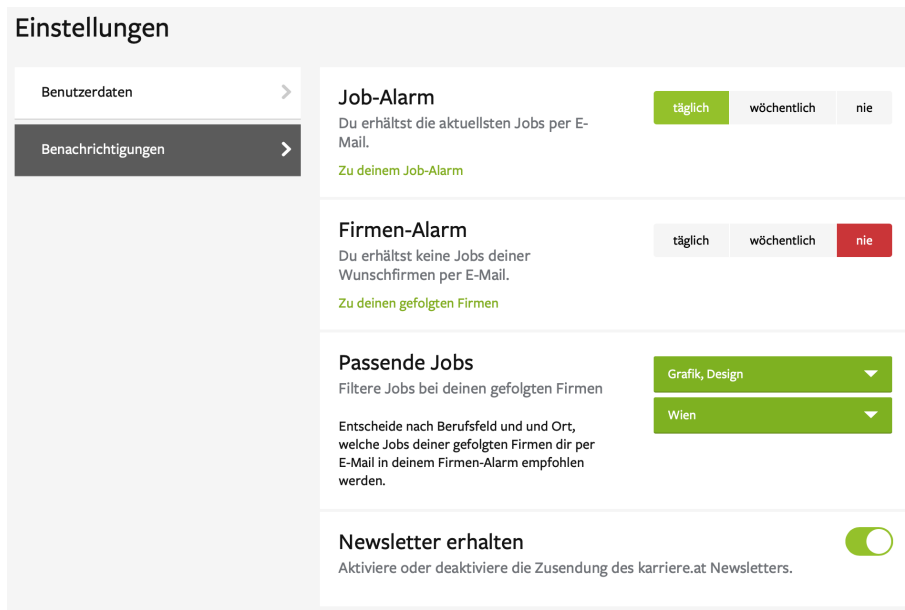


Figure 3.34: Configuration of newsletter topics

According to the GDPR, users should be able to withdraw consent as ease as they have given it. In comparison to the cookie consent, a newsletter consent can be withdrawn in a few ways: in profile settings (see Figure 3.35), on the web page (see Figure 3.36) or directly from the email (see Figure 3.37). The participants mentioned that “*Users should be informed how can they withdraw the consent. They should not be forced to participate in a survey or charged a fee before they are able to say ‘Unsubscribe’. Furthermore, users do not have to specify a reason for their withdrawal if they do not want to.*”

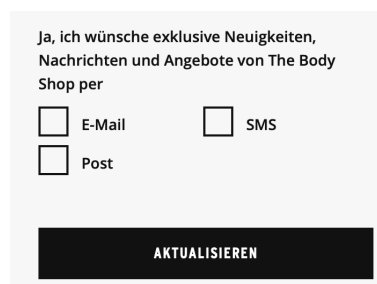


Figure 3.35: Unsubscribing from a newsletter in Profile Settings

It was also suggested that “*if a newsletter has different category settings, give users the possibility to unsubscribe from some of them in convenient way, but do not force them to unselect all categories one by one*” (see Figure 3.38). It is also important, to inform users what happens after they unsubscribe from a newsletter: does it mean that their data/account will be also deleted?

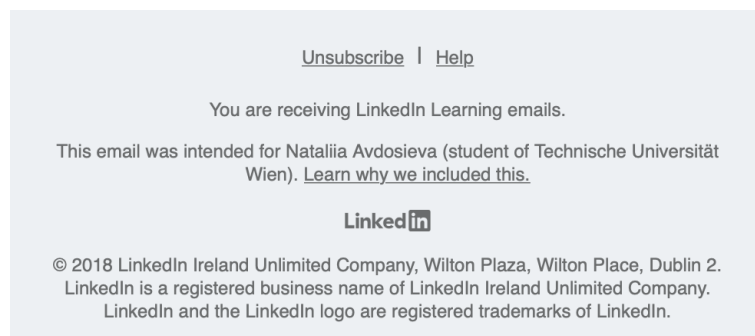


Figure 3.36: Unsubscribing from a newsletter directly from email

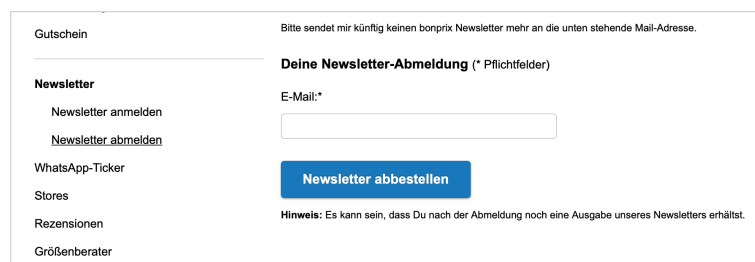


Figure 3.37: Unsubscribing from a newsletter on the web page

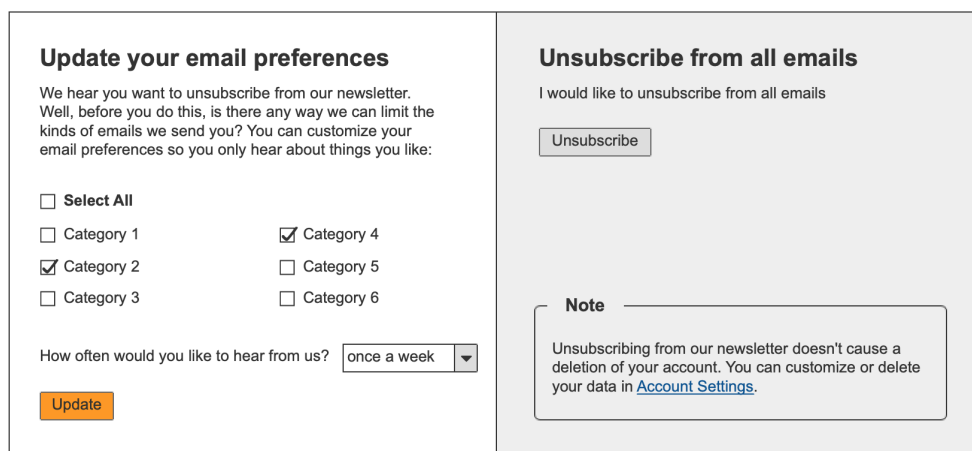


Figure 3.38: Solution to unsubscribing form

3.4.5 Manage Personal Data

Regarding to the data transparency, participants agreed that having the possibility to get a copy of all data that the online service stores about users, is a positive example of the company's transparency: "A user can look at what data about him or her they store and decide if he or she wants to change or erase something."

One of the participants also mentioned that users should be aware what data they have right to erase and exactly happens when their accounts are deleted in order to avoid future surprises (for example, an erase of a credit history leads to deleting both bad and good credit history). As a friendly and modern way to request data changes or data erase, the participants selected an online form with a simple way of user identification. As it can be seen in Figure 3.39, in case of a request to access, change or erase user's data, a user has to fill his or her data, enter identification data (email and phone number), write a request and submit it in electronic form. The user is also provided with explicit information about the further procedure and how this request will be processed.

3.4.6 Feelings and Thoughts

At the end of the workshop, the participants spoke about an idea to have an aid that can help them in designing GDPR compliant websites. Most of the participants liked the idea to have a set of cards with design patterns that can help them to make a GDPR compliant product. They also highlighted the necessity to include both good and bad examples in the patterns since it can be extremely helpful in understanding what should and what should not be done. Furthermore, it would be useful to have a reference to the real GDPR article where designers can find more information about GDPR rules if they need to.

A few other ideas that came from participants were about having an online GDPR Compliant Generator: *“A service can generate a web page basing on the functions users set up”* or *“A user has a Use Case he or she is looking for answers for. He or she types the issue and receives a set of advice on how to solve this case.”* These ideas, however, focus on implementing a template rather than on providing an understanding of how it should be done right.

Another issue mentioned in this discussion was that the aid should represent interaction flow instead of giving separate solutions. While supporting designers in making compliant online products, it needs to be based on the whole process instead of solutions for each concrete problem.

To sum up, the findings from the workshop demonstrated a broad overview to the understanding of the research topic. Thus, the issues mentioned by the participants will find their application in the following chapter of this work.

Personal Data Access, Rectification and Erasure Request Form

Please fill out this form if you are a resident of the European Union and wish to exercise your right to access, rectify, delete or object to further processing of the Personal Data we may have about you.

If you do not wish to complete this form, you may also submit a written request to info@website.com

First Name*

Last Name*

Email*

Phone Number*

Request Type*

Please describe your request*

About your Personal Information

The information you provide here will be processed solely for the purpose of verifying your identity, identifying the information you're requesting and answering your request. Your personal information will be accessed by our designated staff only.

How we will process your request

We will answer your request, or request additional information from you **within 30 days**. We may extend this process for up to two months, in which case we will notify you of the extension within a month.

The processing of this request is free of charge, but we reserve the right, as allowed under GDPR Article 12 (5), to charge an administrative fee under certain circumstances.

Please note that we may refuse to act, as allowed under GDPR Article 12 (2) and 12 (5), on requests that are insufficiently substantiated, unfounded or excessive.

Figure 3.39: Online form to access/change/erase user data

Prototype of the Card Deck

This chapter will focus on creating a paper prototype of the card deck ‘Designing for Privacy’. Firstly, the terms creativity card deck and design pattern will be discussed in Section 4.1, followed by a review of existing creativity card decks in Section 4.2. Then, basing on the formulated in Section 4.3 idea and concept of design patterns, a paper prototype will be created in Section 4.4. Section 4.5 represents a process of prototype evaluation and analysis of findings.

4.1 Creativity Card Deck & Design Patterns

Having been seen in the past as a play, today card decks (see Figure 4.1) are applied as creative toolkits for clarifying thoughts and develop ideas, for inspiration, problem definition and problem-solving. They give an overview of the key aspects of processes, guide players to be creative at the various stages of any process or situation where new ideas are searched.

In turn, a term ‘design pattern’ represents “*A repeatable solution to a commonly occurring problem in design. A design pattern is not a finished design that can be transformed directly into code. It is a description or template for how to solve a problem that can be used in many different situations*” [39]. One of the good examples of design patterns is ‘UI Pattern card deck’ (see Figure 4.2). The UI Pattern card deck is a printed card deck presented in a manner easily referenced and used as a brainstorming tool. Each card describes one design pattern and suggests ways to apply it to the design of online products [40].

In the study [41], based on 81 reviewed creativity card decks, the author defined 8 types of card decks: the classics, framework cards, index cards, libraries cards (index + framework hybrid), strategy cards, grid cards, visual inspiration cards, empty cards. Below, types of card decks that are the most related to current work will be discussed.

4. PROTOTYPE OF THE CARD DECK



Figure 4.1: ‘Superpowers Card Deck’



Figure 4.2: Examples of cards from ‘UI Pattern card deck’

Framework Cards present the DNA of a field with each perspective or thing as a card. The cards are often open for discussion; they represent what needs to be done. Framework cards are good for aligning groups around a project or defining in which order things should be done, how important each part is or if something was forgotten [41].

Index Cards contain a lot of information on them, e.g. a description of a creative method or exercise. They are more like books without binding. Index Cards support their readers with all necessary knowledge about numerous concepts or aspects. Compared to framework cards, index cards are hard to use in workshops as participants can get overloaded with information [41].

Libraries cards describe parts of the process, they represent a combination of framework and index cards. Combining the parts in different ways could trigger new ideas or add

alternative dimensions to already existing concepts. This type of cards is most suited for idea generation [41].

Strategy cards are used to help with tips and strategies on how to think. Strategic cards summarize a field from a more strategic point of view than checklist cards [41].

Grid cards can be used for designing grids and scales. They can help with sorting ideas according to different values [41].

Basing on the purpose of this work to create a helpful tool for UX/UI designers, it can be noticed that ‘libraries cards’ type will be the most suitable for suggested design patterns. From the one side, by introducing each step of ‘Designing for Privacy’ cards users will not be overloaded with information; from the other side, users will have the possibility to have an overview of the whole process.

4.2 Analysis of Existing Card Decks

In order to define a set of characteristics that makes card deck a creative, useful and helpful toolkit, 40 different card decks were reviewed and analyzed. It was found that most of the card decks are informative, visual, interactive, grouped and structured. In addition, they may contain good and (or) bad examples (patterns), have a manual how to use them, and include links to related patterns. More details of the found characteristics will be given below.

Cards are informative: they include all necessary information to make each point of the process clear to its players. For example, in ‘IDEO Method Cards’ [42] is explained how and why each method should be applied (see Figure 4.3).



Figure 4.3: IDEO Method Cards

4. PROTOTYPE OF THE CARD DECK

Cards are visual: each of the cards is accompanied by a visual example (iconic illustration, photo, design pattern etc.) that helps to explain the card's content. For example, 'Silk Method Deck' [43] uses photos as a visual tool to illustrate methods and principles represented in the cards (see Figure 4.4). As another example, each card of 'Roadblocks to innovation lpk' [44] has a useful and simple icon to outline a key topic of the deck (see Figure 4.5).



(a) Front side with illustration

(b) Back side with content

Figure 4.4: Visualization of 'Silk Method Deck' card



Figure 4.5: Iconic visualization of 'Roadblocks to innovation card deck'

Cards are interactive: they focus on the interaction between cards and players. Thus, 'MethodKit' [45] offers its players a bunch of interaction methods such as mapping (see Figure 4.6), sorting, clustering, aligning, prioritizing and more.



Figure 4.6: Workshop using the MethodKit cards as headlines for sorting thoughts and ideas

Cards contain good and (or) bad examples (patterns): in order to support their players with better understanding what is a good pattern and what is not, card decks can contain useful design patterns or bad examples to the concrete situations. Such an approach is applied in ‘Design with Intent’ card deck [46]: the author uses real examples to explain principles represented in each card (see Figure 4.7).



Figure 4.7: Card with a visual example from ‘Design with Intent’ card deck

Cards are grouped and structured: all cards are grouped by categories (by a topic, by a method, by activity it represents, etc.). As an example, ‘Zig Zag creativity card deck’ [47] consists of 48 cards, which are grouped to follow Sawyer’s 8-step ideation process: ask,

4. PROTOTYPE OF THE CARD DECK

learn, look, play, think, fuse, choose, make (see Figure 4.8). In addition, each card of the deck has its unique number so a player can easily remember it and find it.



Figure 4.8: Grouped cards of ‘Zig Zag creativity card deck’

Cards have a manual how to use them: each card deck is provided with introduction information about the cards and how to use them (see Figure 4.9). In addition, they may include an overview of all cards (table of content) that are included in the card deck [48].



Figure 4.9: Manual how to use ‘Strategy Card Deck’

Cards have related patterns (connections): in case different cards of the deck are related by some topic or similarity, they have a connection mark on them. For example, cards of the ‘Group Works Card Deck’ [49] have related patterns: up to seven other patterns that

are most closely related to or most useful to consult when considering how to enact this pattern (see Figure 4.10).



Figure 4.10: Card of ‘Group Works Card Deck’ with a list of related patterns

Among other parameters of card decks, it was found that they have a rectangular shape with rounded corners; they are colorful; the size of cards varies from about A8 to A6 format; the number of cards in one set is usually about 40-60 cards.

Overall, the review of existing card decks has shown a widespread use of cards in creative design thinking processes, highlighting their interesting approaches and expediency. The analysis of existing approaches to creativity card decks has become an essential element in the process of understanding how to create an effective and helpful toolkit.

4.3 Ideation Process

The idea of the design patterns ‘Designing for Privacy’ is to support UX/UI designers with visual examples and explanations in the process of creating a user-friendly online product that complies with GDPR requirements. Findings from the workshop (see Section 3.4) and analysis of existing card decks (see Section 4.2) helped to define the main characteristics of the structure, content, and design of the patterns.

‘Designing for Privacy’ card deck consists of two sets of cards: ‘set of principles’ and ‘set of recommendations’. While the purpose of ‘set of principles’ cards is to introduce the core principles of GDPR, ‘set of recommendations’ is like a step-by-step instruction that guides designers in their practical choices by giving them standard reference points. Visual design patterns focus on presenting to users bad and good practices but they do

not state that a suggested solution is the only one that is correct. The goal is to set designers on the right path, rather than tell them what they must do.

Different categories of cards highlight various aspects of the GDPR. For example, all issues related to privacy are grouped in the category ‘Privacy Policy’; issues about cookies – in the category ‘Cookies’, etc. Cards of each category represent so-called workflows, that means the order in which cards are used is important. For example, a designer should not apply card ‘Withdrawable cookies (opt-out)’ before ‘Compliant cookies bar (opt-in)’ since the implementation of withdrawing the consent cannot be done before implementation of cookie bar and cookies configuration.

Another important issue is that some cards can be connected to each other as they represent a part of an aspect. For example, ‘Withdrawable Consent’ aspect is represented in 4 cards: allow users to withdraw the consent, notify how to do this, give them the choice what to withdraw, inform users about consequences. As it can be seen, all these cards are connected by one topic, and they cannot be merged into one card because of their complexity in actions.

Last but not least, some cards of the deck can be skipped. For example, if an online service does not provide a ‘sending a newsletter’ function, obviously, it does not need to be implemented.

Therefore, a card deck ‘Designing for Privacy’ should include the following:

- A folded instruction sheet with an introduction, manual how to use it and a table of content, so designers can clearly understand and navigate through the cards
- ‘GDPR Principles’ – set of 6 cards with fundamental GDPR principles
- ‘GDPR Aspects’ – set of 32 cards with advice to how to create a GDPR compliant online product. All cards are grouped by 4 topics: privacy policy, cookies, forms & consent, manage personal data
- A case for cards

Considering the content of the cards, each card from the card deck should contain the following:

- Number: to allow easy navigation through the set
- Category: to clarify and get direct access to the concept
- Name of the pattern (recommendation) or principle
- Short description: to highlight the key aspect of the card
- Explanation: to describe an issue in more details

- Related GDPR Article(s): to present the possibility for users to find more information related to the current design pattern
- Mark that this is a UX advice
- Dark or (and) light patterns: bad and good visual examples to illustrate the aspect

Suggested concept design of cards from principles and aspects sets are represented in Figure 4.11 and Figure 4.12 respectively.

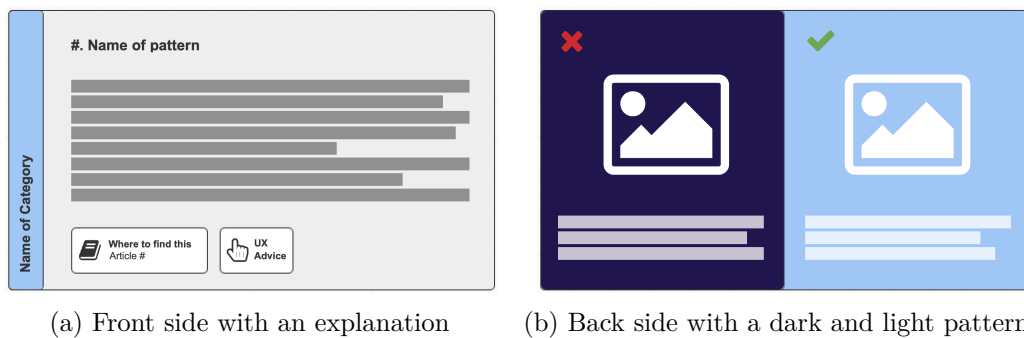


Figure 4.11: Concept design of a card with a privacy recommendation

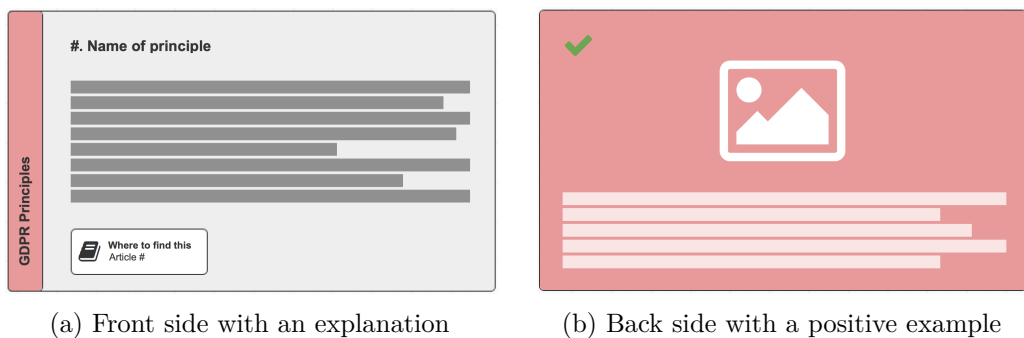


Figure 4.12: Concept design of a card with a privacy principle

4.4 Paper Prototype

Paper prototyping represents the fast and easy way to design and refine user interfaces [50] or, in our case, design patterns. As a generative process, prototyping often leads to innovation and significant savings in time, effort and cost [51]. Thus, without much effort to details such as design, colors, alignment and graphics, paper prototyping is an effective tool to evaluate the concept of the project. The aim of the paper prototyping of design cards is to check if all aspects represented there are right and can be easily understood by designers; if bad and good examples, highlighted in the literature review and the

4. PROTOTYPE OF THE CARD DECK

workshop with experts, make sense and are logical; if any other important aspects were overlooked.

To simplify the process of prototyping, each card of the paper prototype contains a text explanation of dark and light patterns instead of a graphical representation of these patterns (see Figure 4.13). Elements such as ‘where to find it’, connections to other cards, were also skipped for the prototype. The categories of the cards are distinguishable by 4 randomly chosen colours.

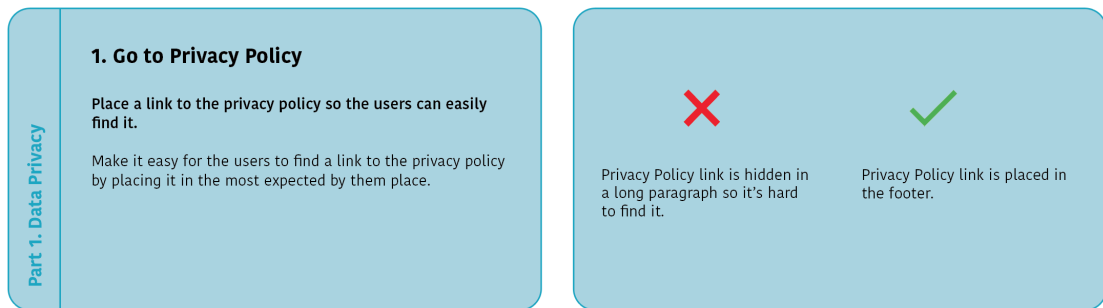


Figure 4.13: Prototype of a card (front and back)

Overall, the paper prototype of the toolkit ‘Designing for Privacy’ with 32 cards was created (see Figure 4.14). At the next step of this work, the printed prototype will be evaluated by privacy experts and end users.

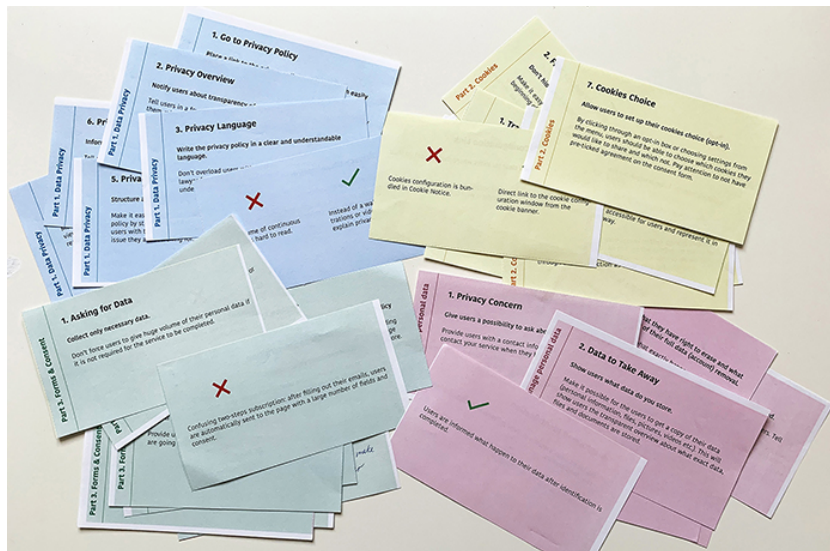


Figure 4.14: Paper prototype with 32 design cards

4.5 Prototype Evaluation

Prototype evaluation is a very important part of the design process. It simply confirms that the product will work as it is supposed to, or if it needs refinement. It helps identify potential faults, which in turn allows the designer to make improvements. Identifying potential problems at the early stage allows to reduce the time and cut the costs necessary for the design and implementation phase.

In the following sections, the evaluation of the paper prototype and analysis of findings received during the evaluation will be reviewed.

4.5.1 Evaluation of the Prototype by Privacy Experts

The goal of the prototype evaluation is to verify the correctness of the created cards before the time consuming design process begins. The focus is particularly on issues related to the content of the cards including the discussion of negative and positive examples. In this stage, it is critical to understand if all the necessary aspects of GDPR are reflected in the cards; if they have a logical sequence and structure; if they are formally accurate. The scope of this evaluation plan is to ensure the functionality and usability of the cards from a privacy perspective.

An expert interview was chosen for the evaluation of the prototype since at this stage no one but a privacy expert could approve the content of the cards. Overall, two expert interviews were conducted. During the interview, experts were told about the project, its goals, and objectives of the interview. Then, step by step, each card of the set was introduced and discussed. Feedback to each card was documented on the cards during the interview. When all cards were presented and validated, experts were asked to provide overall feedback about the card deck and to define if there are still some open GDPR aspects that were not highlighted in cards.

Expert interviews were conducted one after each other. Before the second evaluation, the prototype was improved basing on the previously given expert feedback. Analysis of findings and review of expert feedbacks will be represented in the following section.

4.5.2 Analysis of Findings

In the interview with the privacy expert A it was suggested to make the following changes:

1. Add a card about data breaches: *“It would be necessary to provide designers with a design pattern how to communicate data breach. For example, a pattern with an email that contains a message that user’s data was compromised and a link to the ‘password reset’ function.”*
2. Add a card about privacy concern: *“Users have to be provided with the possibility to contact service if they have some questions about their privacy.”*

3. Add a card about simple identification: “*Make it easy for users to prove their identity during the data access/erase request.*”
4. Add a card about informed identification: “*Inform users what will happen to each data they provide during their identification. For example, if the photo they upload will be stored or deleted, or how long this information will be kept?*” As a solution to this issue, one of the experts suggested to create a data protection icon and locate it to each field of the form. A user can get quick privacy information about concrete data he or she provides to the service (see Figure 4.15).
5. Explain more carefully about ‘right to be forgotten’: “*Users should be aware of what their data can be erased from the system and if they have the right to do this.*”

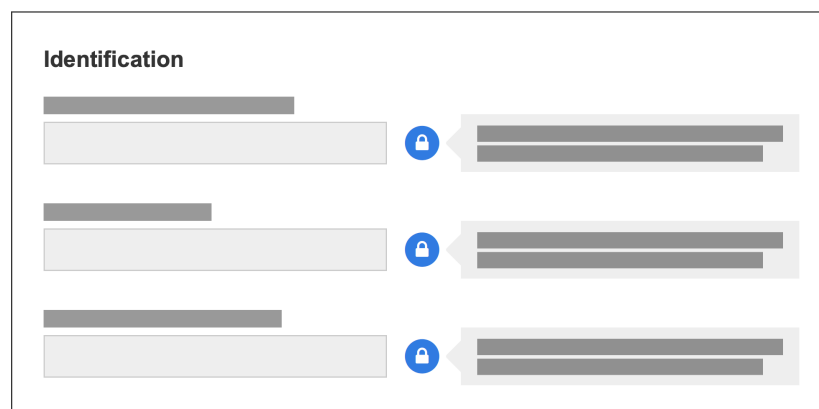


Figure 4.15: Solution to the card with informed identification

Among other recommendations, the expert A proposed to group cards by six main principles of GDPR. This idea, however, was rejected due to the fact that in this case cards would not represent a logical flow required for the design process. Another suggestion was to replace a reference to the Article of GDPR by a QR-code that leads to this Article online. Realization of such an approach would need to increase the size of the cards. Furthermore, since it cannot be guaranteed that a QR-code would be used by everyone, a written link to the Article would be still required.

After the card deck had been updated and new cards had been added to the set, the second interview with the privacy expert B took place. In his review, the expert B mentioned the following:

1. Misleading of cards where states that it is not legal to limit users in the functionality of the website till they give their consent: “*The limitation of the access to the web site is legal if the website possesses unique or paid content. It is also legal to ask a user to pay if he or she does not want to be tracked by the system.*” In such case, the expert highlighted that if the user is given an alternative in order not to be

tracked, this kind of behavior of the system is absolutely legal (see Figure 4.16). Being legal, however, does not always mean to be user-friendly. One of the Internet users stated [52]: "*Pay, or give up basic rights' is not exactly what the new GDPR meant by 'voluntary' consent. As it is 'Der Standard' that is acting that way is hurting me in particular.*" Thus, it was decided to remove this pattern from the card deck since it can be confusing or provoke more people to force their users to be tracked if they do not want to pay.

2. The content of 'Two-step subscription' card can also have a different meaning: "*Two-step subscription typically indicates that after subscribing to a newsletter a user has to confirm his or her email address. This helps to avoid the subscription of third parties instead of an owner of the email.*" The expert suggested including one more card that represents this aspect as well as rethinking about correct naming for the existing card.
3. Personal data breach notification form: "*European Data Protection Supervisor source provides a good example of notification form for a data breach. Link to this form can be also useful for designing this process.*"
4. Missing card about the accessibility for people with disabilities: "*Web services should pay attention to provide the information about user privacy, in a way people with disabilities can perceive and understand it as well.*" This point brings us to the question about Web Accessibility Initiative [53], a necessity in understanding and following of Web Content Accessibility Guidelines (WCAG) [54] in order to make web content more accessible to people with disabilities.

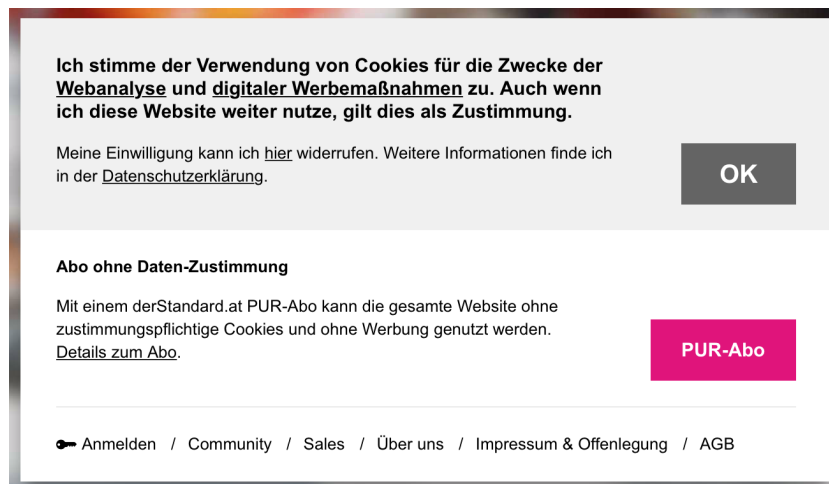


Figure 4.16: Legal content limitation: users are asked to pay a PUR-Abo if they do not want to be tracked

4. PROTOTYPE OF THE CARD DECK

Among other concerns from the provided feedback, the expert B pointed on the issue about data declaration: “*You should declare to users everything you do with their data.*” This issue will be presented and explained in the set of cards with GDPR principles.

Overall, both privacy experts mentioned the completeness and correctness of the evaluated cards. They suggested some minimal rearrangement of cards, content rephrasing and adding some extra cards that were missing. The experts emphasized the usefulness of the developing toolkit in total, and they believe that this tool will fulfill a significant role in understanding how to create a GDPR compliant online product.

Visual Design

This chapter will focus on the visual design of the card deck ‘Designing for Privacy’. The process starts in Section 5.1 with defining the layout, shape, and dimensions of the cards. Then, an asset library will be created in Section 5.2. Visual design of the card deck will be represented in Section 5.3, design of an introduction sheet and a case for cards in Section 5.4.

5.1 Setting the Stage

Layouts are like stages. The images, headlines, text, graphics, logos, patterns, and colors that fill layouts are like characters on a stage [55]. The design starts with defining the shape and dimensions of the stage.

The format size of the card deck (150x90 mm) was chosen basing on the maximum amount of the content that each card of the deck can contain. This choice of the card size is also reasonable since it is compact enough to be convenient to hold cards in hands, and from the other side – big enough to be readable.

For the back side of the card, a 2-column grid was applied (see Figure 5.1). Such a layout makes it easy to view and compare negative and positive design patterns at first sight. Left vertical space on the front side of a card is selected for the placement of a category title.

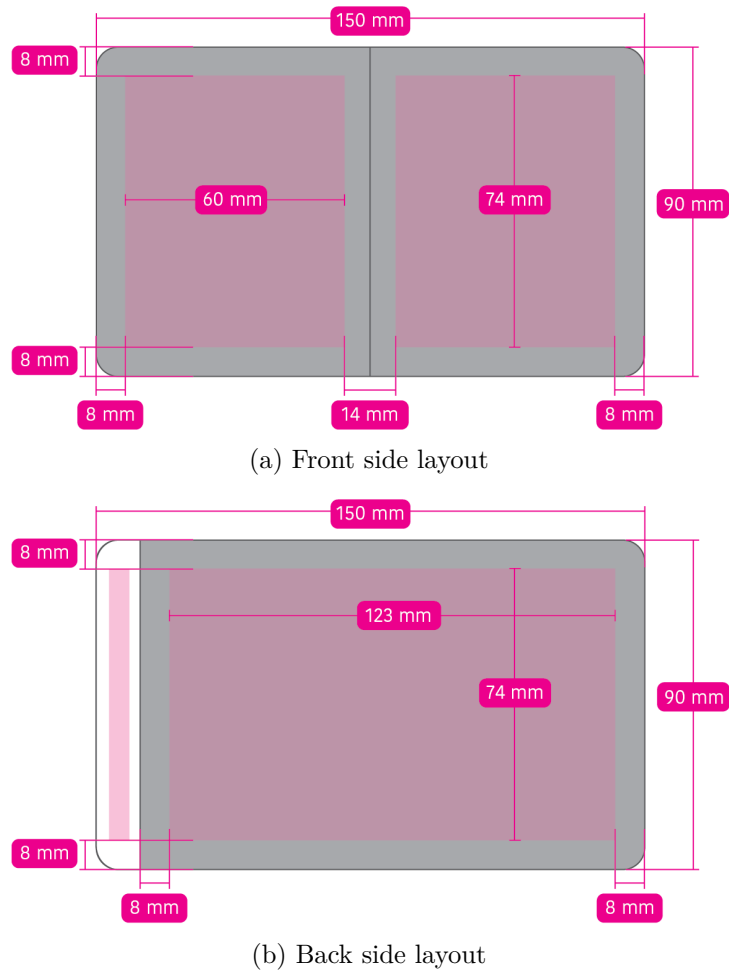


Figure 5.1: Layout and measurements of a card

5.2 Asset Library

An asset library is an organized collection of vectors, icons, images, color palettes, fonts, and other available design elements [56]. The purpose of the asset library is that stored in repository files can be easily accessed and reused by users [57]. To achieve the consistency in design of cards and considerably simplify the design process, the asset library for card deck ‘Designing for Privacy’ was created. The library includes the following:

- Elements of design such as color palette, fonts, icons
- Elements of the user interface

The color palette of six various combinations was chosen to represent six different categories of the card deck (see Figure 5.2). The font hierarchy refers to present the

content in a way that visually tells where to look, and in what sequence. The icons set was created basing on the principle of recognition.

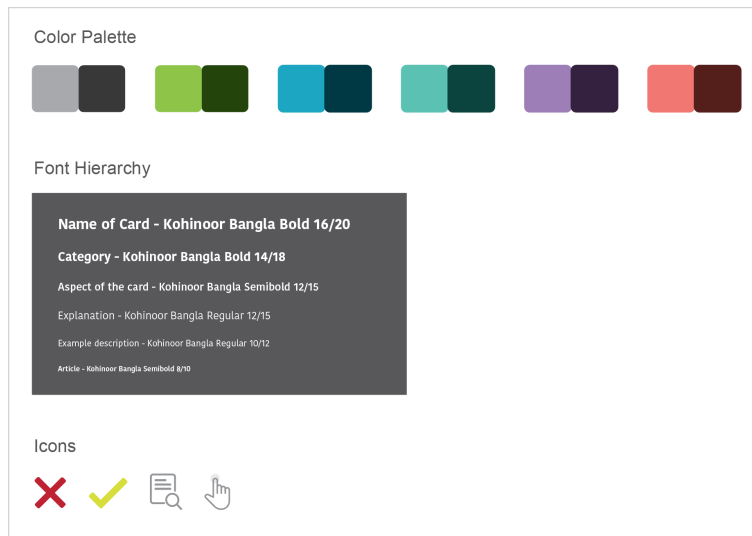


Figure 5.2: Asset library with the color palette, font hierarchy, and icons

Elements of the user interface are made as a symbolic representation of real web user interface (see Figure 5.3). The goal was to create design elements that are simple but at the same time easy to understand and recognize by users. Among these elements are a content block, video, input fields, buttons, images, lightbox, table, dropdown list, etc.

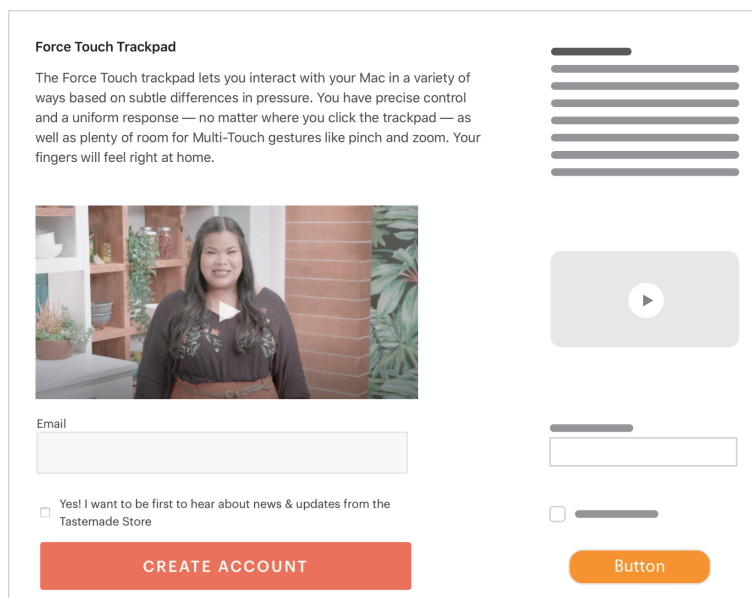


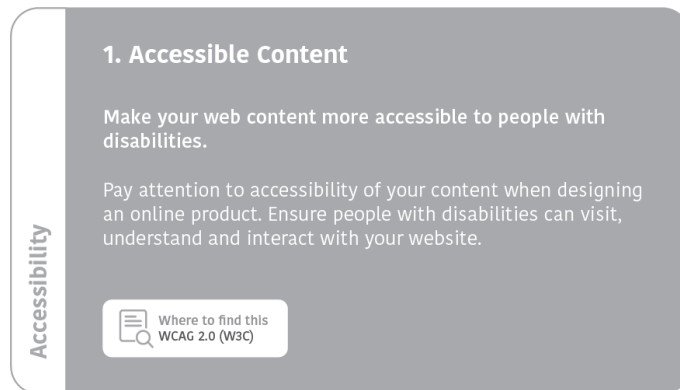
Figure 5.3: Transforming a real user interface into abstract one

Full asset library created for the card deck is represented in Appendix B.

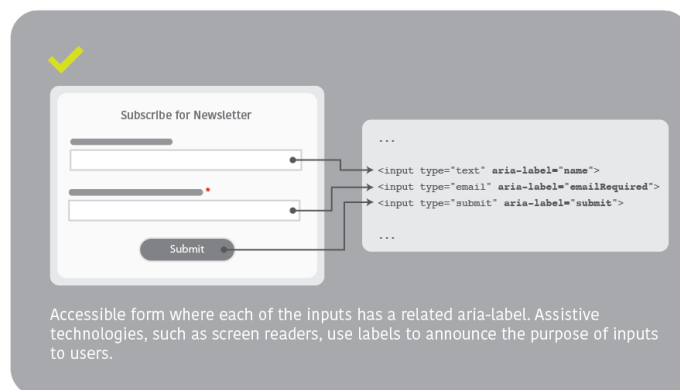
5.3 Design of Cards

After the concept has been generated (see Section 4.3), the layout has been defined (see Section 5.1) and the asset library has been created (see Section 5.2), three variants of cards were designed: a card with both dark and light patterns, a card that contains only light pattern, and a card that contains only dark pattern. Overall, as it was decided after the expert evaluation, the card deck 'Designing for Privacy' includes three sets of cards: Accessibility (1 card), GDPR Principles (6 cards), GDPR Aspects (35 cards). Depending on to which category a card belongs to, its color and labeling will be different.

The 'Accessibility' category contains only one card and is represented as an antecedent card to the all others (see Figure 5.4).



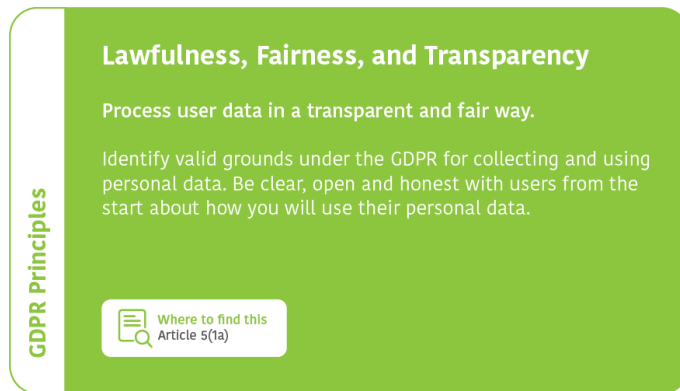
(a) Front side with an explanation



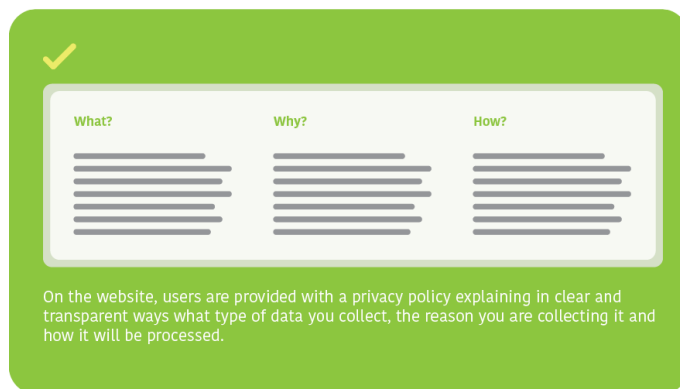
(b) Back side with a light pattern

Figure 5.4: Design of the card 'Accessibility'

All cards of the 'GDPR Principles' set are of the same color. Each card has the name of the principle, its description, and explanation on the front side. In addition, users are provided with an 'article block', where they can find GDPR Articles related to the cards (see Figure 5.5a). The back side of the card includes information and a visual example of what can be done to achieve this principle (see Figure 5.5b).



(a) Front side with a principle explanation

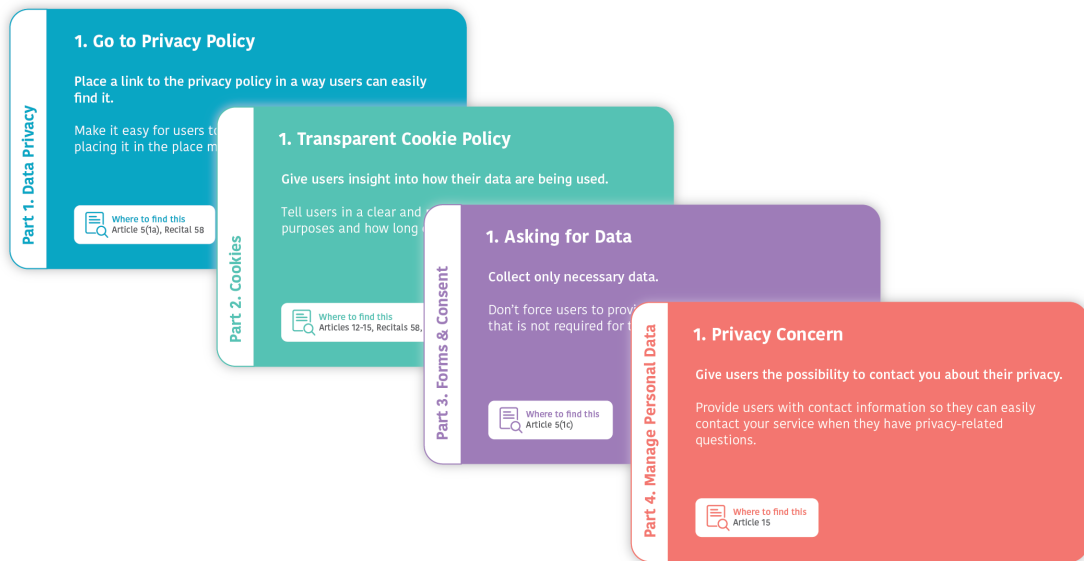


(b) Back side with a light pattern

Figure 5.5: Design of a card from the set 'GDPR Principles'

Cards of the 'GDPR Aspects' set are divided into four categories (see Section 4.3), each category has its own color for faster search and an easier distinction between them (see Figure 5.6). The front side (see Figure 5.6a) of each card includes a name of the category, a number of the card, a name of the aspect, its description, an 'article block' or/and 'UX advice' mark. Depending on the content, the back side of each card (see Figure 5.6b) can contain dark, light or both design patterns with visuals and text explanation.

Some of the patterns may contain the user flow to illustrate the interaction process. For example, the pattern that illustrates the interaction with a sticky 'cookie' button (see Figure 5.7).



(a) Front sides with explanations



(b) Back sides with design patterns

Figure 5.6: Variations of the cards from the set 'GDPR Aspects'

During the creation of the card deck, following design principles [58] [59] were taken into account:

- **Simplicity:** people tend to perceive complex images as the simplest as possible. Example: a simple visualization of design patterns.

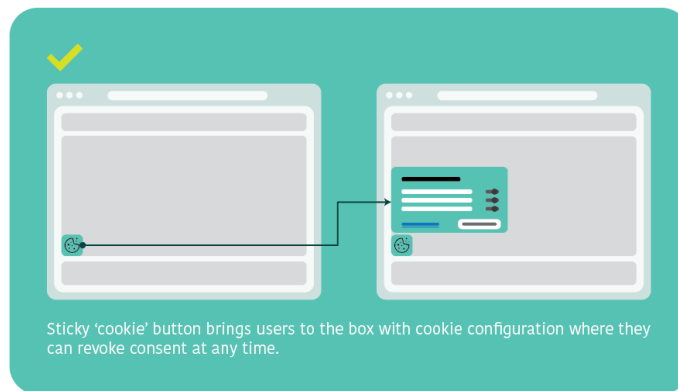


Figure 5.7: Light pattern with a user flow

- **Similarity:** objects that look similar at the shape, size or color are perceived as been grouped. Example: grouping of text lines.
- **Alignment:** vertical and horizontal alignment helps to achieve cohesive unity of the elements. Example: grid and layout.
- **Proximity:** elements placed closer together are perceived as being related to each other. Example: grouping of the content of dark and light patterns.
- **Repetition:** reusing of the same or similar elements throughout design. Repetition of certain design elements in design brings consistency and cohesiveness. Example: same elements such as title, a name of a card, article block, etc. are placed in the consistent parts of the cards.

5.4 Design of Introduction Sheet & Case

The purpose of the introduction sheet is to introduce the design patterns to the readers. It is an 8-page manual that contains the structure of the card deck, explanation how to use them and a table of content for the navigation through the cards. The introduction sheet will help UX/UI designer in understanding how the cards can be used for designing GDPR compliant online product. Design of the introduction sheet is represented in Figure 5.8.

In order to store the card deck, it was decided to design and build a cardboard box with a lid (see Figure 5.9).

In the following stage, the cards designed in this section will be evaluated by UX/UI designers.



Figure 5.8: Design of the Introduction Sheet



Figure 5.9: Design of the box

Evaluation

This chapter will focus on the evaluation of design patterns. The process starts in Section 6.1 with evaluation by UX/UI designers. Basing on the collected feedback, the cards will be improved and used for prototyping a GDPR compliant online product in Section 6.2. Finally, a prototype of the GDPR compliant online product will be tested with end users in Section 6.3.

6.1 Design Evaluation

The purpose of the design patterns evaluation is to define how easy it is for UX/UI designers to understand them. The results of the evaluation will be used to analyze and improve design patterns.

6.1.1 Methodology

To evaluate the design patterns suggested in the toolkit ‘Designing for Privacy’, four participants – two senior and two junior UX/UI designers, were chosen. Different level of experience of the participants will help to define if designers with less experience require more time to understand the design patterns. From the other side, senior designers can provide the most significant feedback to how the toolkit can be improved.

The applied methodology of design evaluation included the following:

1. Each participant received one part of the card deck to evaluate (Privacy, Cookies, Forms & Consent or Manage Personal Data).
2. Participants were asked to consistently scan and examine the content of the cards, and raise the questions if something was not clear (pattern or description, or both).

3. After the familiarization with the cards, each participant received 3 tasks – real use cases – to solve. The tasks (see Appendix C) contained use scenarios, examples of web pages or their elements that reflect aspects of the GDPR. They focused on how the aspects of the GDPR studied with the toolkit were understood and could be applied by the participants in the future.
4. During the task-solving process, the think-aloud strategy was applied. The participants were asked to say out loud what they are thinking about when solving problems.
5. Results of the evaluation, including open issues and comments obtained during the think-aloud session, were documented.
6. To obtain final feedback, at the end of the evaluation, each participant received a short questionnaire (see Appendix D) about the whole process of evaluation.
7. Collected during the evaluation data is then discussed and analyzed.

6.1.2 Analysis of Findings

All findings of the design patterns evaluation with four UX/UI designers are divided into three parts: findings from cards review (think-aloud), findings obtained during the task-solving process (observation) and analysis of the final feedback.

During the cards review, following issues about design patterns were raised by the evaluators:

- For the ‘Privacy Language’ cards, the experts mentioned that it is hard to understand this pattern since examples chosen for this card represent different situations: *“It would be nice to know which wording is good and which is bad for the same situation.”*
- It was not clear for the experts what is meant in the pattern ‘Redirected Privacy’: *“Firstly, you ask people not to redirect users to another website for the privacy policy, then, you ask them to include a link to go back to your website.”* It was recommended to rethink about the wordings for this card.
- The card ‘Double opt-in’ caused difficulty in its understanding: *“This card has too technical wording. Try to replace phrases such as ‘deployment list’ or ‘incentive emails’ in a simple way.”*
- ‘Simple Identification’ and ‘Informed Identification’ patterns were not clear for the experts: *“What kind of identification process is represented here? Make it clearer.”*
- The ‘Purpose limitation’ card appeared to be very similar to the previous card in this set: *“The explanation of this principle is way too similar to ‘Lawfulness, fairness, and transparency’. Designers can be confused with a difference between*

these two principles. The dark pattern for this principle is also not clear: why is it bad?"

- The experts mentioned that the ‘Storage limitation’ pattern is misleading: *“The pattern that is given for this principle is misleading. Some other better examples for this principle can be found.”*
- GDPR principles require negative examples as well: *“Showing only light patterns for some principles is not enough. For example, it is understandable what is a good example of data minimization, while it is not absolutely clear what should not be done.”*

All issues collected during the cards review will be taken into account for further cards improvements.

The task-solving part of the evaluation was successfully completed by all participants. However, since all participants already had experience in similar issues, it is difficult to say if the review of cards helped to solve evaluation tasks or the experience that each participant has.

The final feedback gathered from the participants includes discussion about navigation issue, visual language and suggested improvements.

Regarding the navigation issue, participants mentioned that cards are well grouped and completely fit each category: *“It is good that when I just need to design a compliant cookie banner, I quick look to the table of content, and I have a card (or cards) I need for this.”* The question about having references to the GDPR Articles was answered positively, however, three of four participants told that they would probably not need it.

Regarding the visual language of the cards, one participant suggested that in addition to color labeling some symbols can be used: *“Adding the icons to each category of the cards would make cards accessible for people with poor color vision.”* Besides, other participants considered the visual design of cards clear and consistent: *“Some patterns do not even need explanation text, you just have to look to the visual pattern and everything is clear.”*

Regarding improvements that can be made in the future, the participants suggested that *“It would be useful to have an online version of the cards, maybe with more detailed examples.”*

Altogether, the findings of design evaluation appeared to be well promising: from the one side, evaluation helped to validate the usefulness of the design patterns and understand how designers can apply cards knowledge to develop their online websites; from the other side, expert feedback has delivered a range of ideas of how created design patterns can be improved in the future.

6.2 Evaluation of the GDPR Compliant Web Prototype

The purpose of the evaluation of the GDPR compliant website is to define how easy and intuitive are implemented design patterns for end users. This stage of the study plays a significant role since the users are the data subjects for whom privacy-friendly online systems are designed. The results of the evaluation will be used to analyze how users understand and interact with the privacy-friendly online system.

6.2.1 Web Prototyping

Prototyping is an essential part of any digital design process. It helps to simulate designs, explore different user experiences, and test user journeys and user flows within the projects. The goal of the website prototyping described in this section is to conduct a qualitative usability testing with the end users. The task is to gather opinion from the users and to understand if the practical application of created design patterns is clear.

Before starting the prototype process, five use cases for usability testing were defined. Each use case represents a user flow (task) that has to be completed by the user during the evaluation process. The description of use cases and their user flows (main and alternative) are represented below.

Use case 1: Cookie Settings (See the flowchart in Figure 6.1)

You visit a website and you would like to receive a relevant advert on the website. To do so, the website needs to use Advertisement cookies. You need to find out how to allow the website to use Advertisement cookies.

Later, you decided that you would like to experience less targeted advertising. You need to find how to revoke your consent.

Use case 2: Cookie Purpose (See the flowchart in Figure 6.2)

You are curious what are the purposes of the cookies that the website uses. You need to find out what is the purpose of Advertisement cookie with the name ‘Google Analytics’.

Use Case 3: Privacy Concerns (See the flowchart in Figure 6.3)

You would like to contact the service about your privacy issues. You need to find out how to do this.

Use Case 4: Newsletter Subscription (See the flowchart in Figure 6.4)

You would like to subscribe to a company newsletter. Before you do so, you want to be sure that you can cancel your subscription any time. You have to find the information about how to unsubscribe from the newsletter before you sign up.

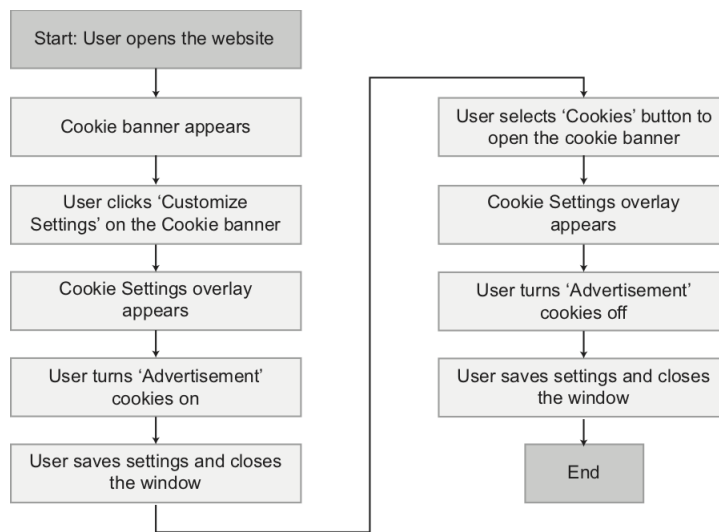


Figure 6.1: User flow of the 'Cookie Settings' case

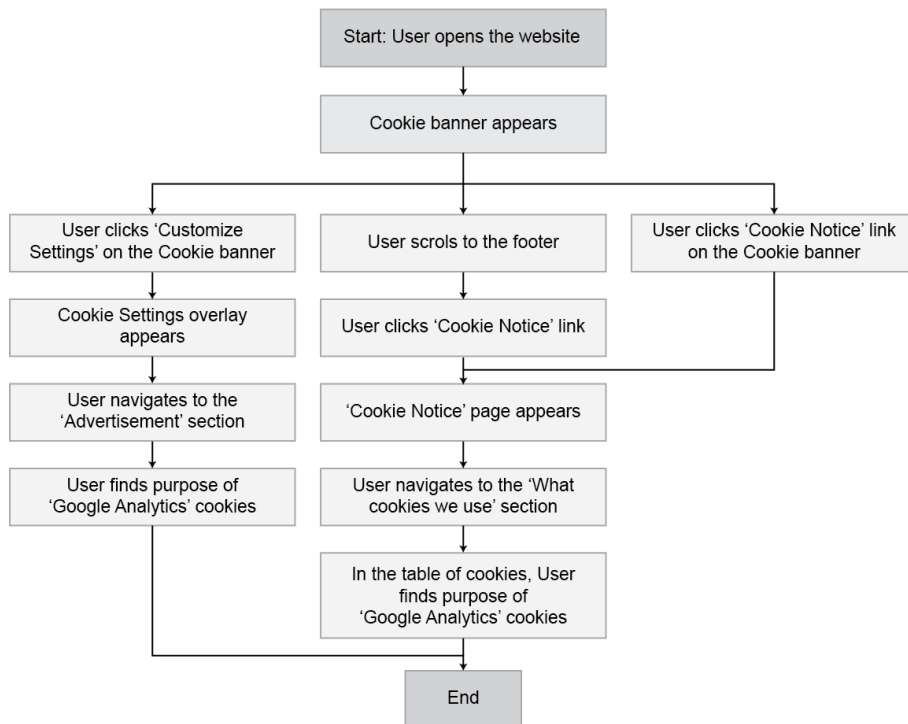


Figure 6.2: User flow of the 'Cookie Purpose' case with 3 different scenarios

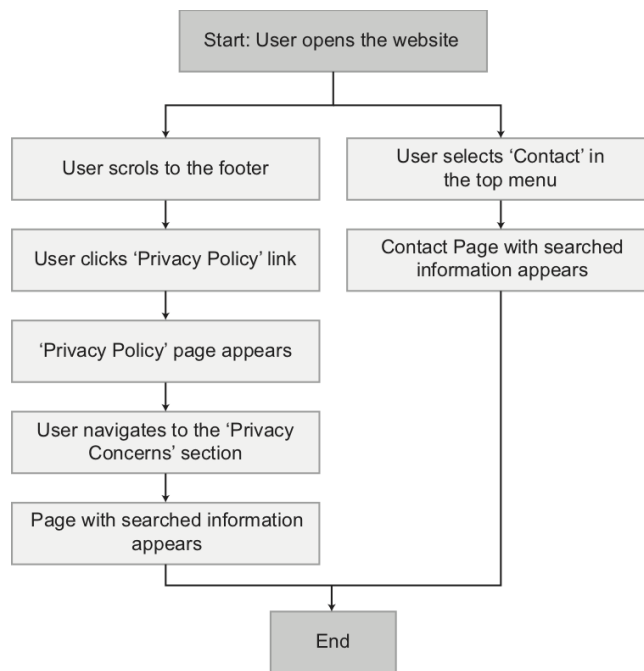


Figure 6.3: User flow of the 'Privacy Concerns' case with 2 different scenarios

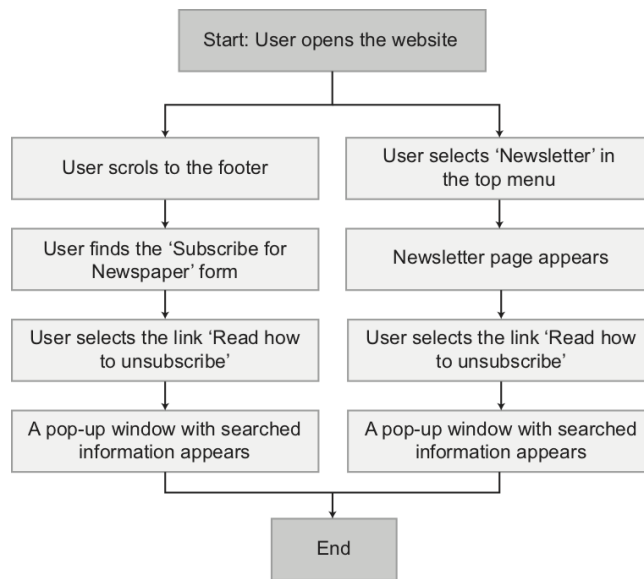


Figure 6.4: User flow of the 'Newsletter Subscription' case with 2 different scenarios

Use Case 5: Identification (See the flowchart in Figure 6.5)

You are on the page with a request to erase your data from the system. In this step, you are asked to verify your identification by uploading a copy of your passport. Find out how your passport copy will be processed and stored.

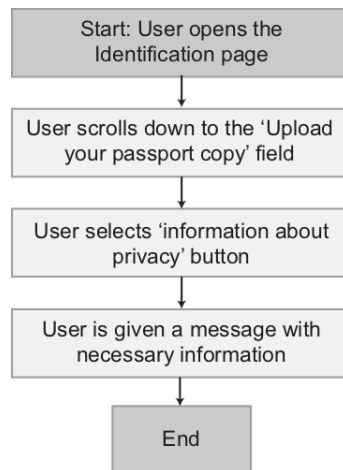


Figure 6.5: User flow of the 'Identification' case

After the use cases and user flows were defined, a visual prototype (see Figure 6.6) was created by the combination of tools such as Sketch, Invision, and Craft Plugin. While Sketch is used to create a skeleton and design of the prototype, Invision provides its users with the possibility to make interactive workflows for usability testing.

The complete wireframing for usability testing is represented in Appendix E. In the following chapter, the usability testing with end users will be conducted and analyzed.

6.2.2 Usability Testing

To evaluate the web prototype created in the previous section, three participants – end users – were chosen. The method of the evaluation can be described as informal qualitative usability testing (see Figure 6.7), with open questions interview (see Appendix F) and the think-aloud technique. Each participant received the online web prototype and five tasks to test it (see Subsection 6.2.1). During the assignment, the participants were asked to comment on their actions and explain why they are solving the task in that way. To get final feedback, at the end of the assessment, the participants were asked to share their thoughts and feelings about the privacy-friendly level of the website that they have evaluated.

For further analysis, the usability testing was documented by screen capturing and audio recording.

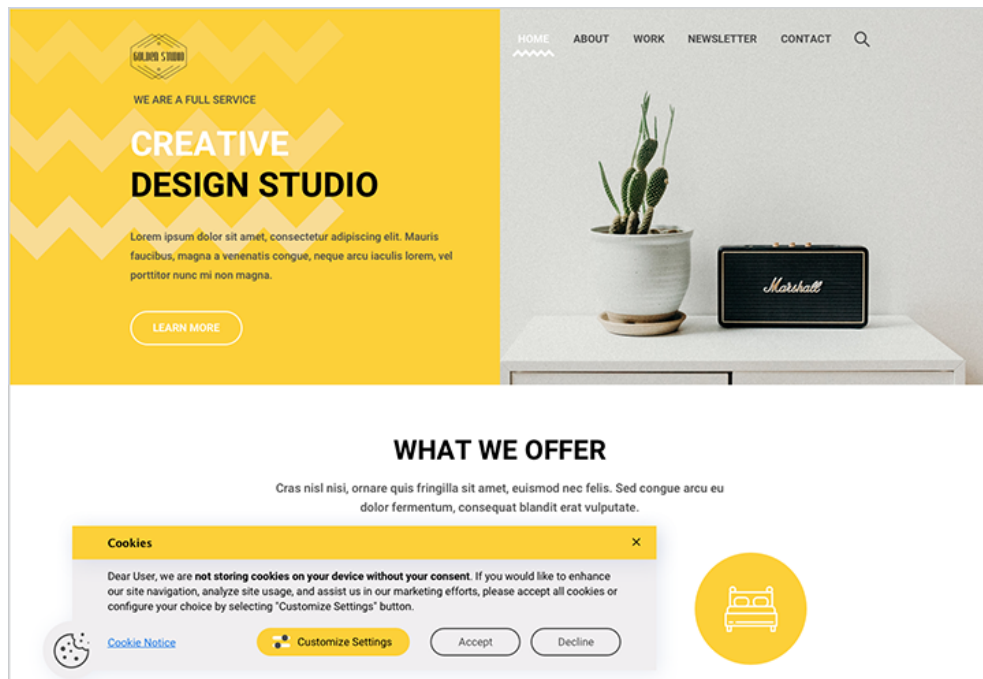


Figure 6.6: Visual prototype of GDPR compliant website

6.2.3 Analysis of Findings

Usability testing with end users presented interesting results. All participants completed given them tasks, however, they followed different scenarios to do it.

Regarding the task ‘Cookie Settings’, two participants were quick to find how to configure the cookie choice from the cookie banner, while third participant automatically closed this banner and was searching for the cookie notice link in the footer of the page. Interestingly, that after closing the cookie banner immediately, this participant was unable to find how to reopen it: *“I thought that this cookie button is an element of the design and did not realize that it has cookie settings function.”* Furthermore, to close the cookie banner, this user clicked ‘Accept’ button without paying attention to the other options: *“I got used to the banners where there is only button ‘OK’ or ‘Accept’. Because of this, I am not paying attention to other options, I just click the familiar button in order to close this pop-up as soon as possible.”* Such behavior shows that ‘careless’ users should be provided with even more noticeable messages and motivation to read them. Another participant mentioned that now knowing that this function to set up cookie choice exists, he will pay more attention to it and will try to customize his consent when it is necessary for him. All participants were confused about ‘Necessary cookie’ toggle button (see Figure 6.8): *“It is not clear what cookies are already on and why, for example, necessary cookie cannot be switched off. If they don’t collect my data, this information should be highlighted. I would also suggest not to do them with toggle button, since it is disabled anyway.”*

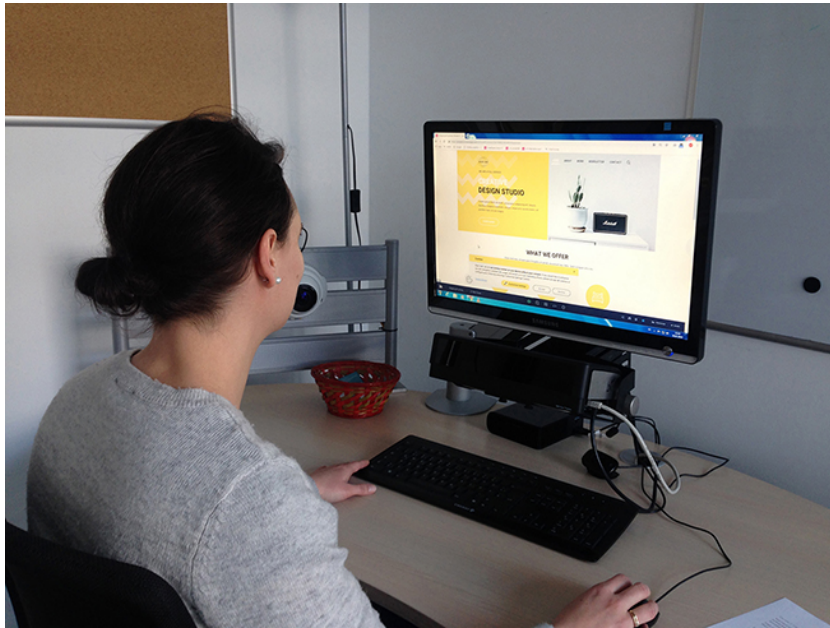


Figure 6.7: Usability testing process

During the ‘Cookie Purpose’ task, two participants were searching for the Cookie Notice page, while third one went to ‘Customize Settings’ window from the familiar sticky cookie button. For one user, however, it was unclear what the information near type of the cookie represents (see Figure 6.8): *“I did not understand that this was a purpose of cookies written there. To have some label or pointing on it would be nice.”*

To complete ‘Privacy Concern’ task, all of the participants selected menu item ‘Contact’ even though, contact form about privacy concern was also represented on the Privacy Policy page: *“Maybe I would go to the Privacy Concern page when I am already in the Privacy Policy. Otherwise, it is easy to find this function in the general contact information.”*

‘Newsletter Subscription’ task caused no difficulty in its solving. Participants, however, mentioned that they never pay attention to unsubscription function: *“It is pretty clear for me that I can unsubscribe from a newsletter directly from company’s emails.”*

During solving ‘Identification’ task, the participants did not understand ‘privacy’ icon with a lock (see Figure 6.9): *“I do not understand what this icon means. It felt for me more like I want to lock some data rather than get information about it. In my point of view, a recognizable ‘i’ or ‘?’ button would make more sense here.”* This feedback, however, is only partly true. The idea to introduce the privacy button is that this button would not be mixed with information message. Thus, for example, if a user needs to know what format of a document he or she can upload (PNG, JPG, etc.), info icon will provide them with this information. When a user needs to get information about privacy issues – privacy button is placed for this purpose.

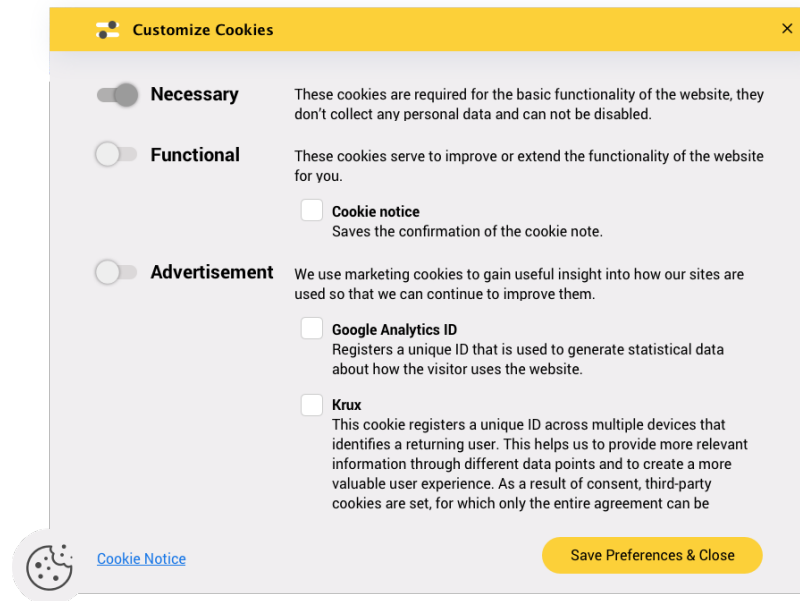


Figure 6.8: Customize Cookies window with disabled toggle button for Necessary cookies

Figure 6.9: Part of Identification form with the privacy button and information text

Findings from the interviews have shown that end users need to receive more attention to their privacy: *“I think that a privacy-friendly website should be a website that catch my attention to my privacy. For example, some banner with a button ‘Watch what will happen to your data’ or some introduction message where it states what happens to my data, etc.”* It means, that it is not enough to a GDPR compliant when users have no idea what are cookies and why do they need to turn them off or on. Users tend not to pay attention to their personal data, they avoid messages regarding their privacy and try to get rid of them as soon as possible. From the other side, one participant stated that after this usability testing, his level of awareness about privacy issues increased, that means that now he will pay more attention to what is going on with his data online.

Overall, the participants have provided positive feedback about the privacy-friendly prototype. They highlighted its transparency and easy-to-understand approach: *"I liked your prototype. It was easy to find information that I needed. No hidden texts or tricks, it is clear what the website collects and for which purpose. I like the idea of having the sticky button that is always available and some useful links where I can find more information about my privacy."*

6.3 Final Improvements

Basing on the feedback gathered from UX/UI designers and end users during the evaluation process, the following changes in design patterns were made:

1. To make cards more distinguishable and accessible for people with color blindness, icon labeling was added to each category of the cards (see Figure 6.10)
2. The content of the cards that were mentioned as being too technical or misleading was changed
3. Misleading and confusing design patterns were corrected regarding to the given by end users recommendations
4. New visual patterns for GDPR principles such as Purpose Limitation, Data Minimization, and Storage Limitation were created

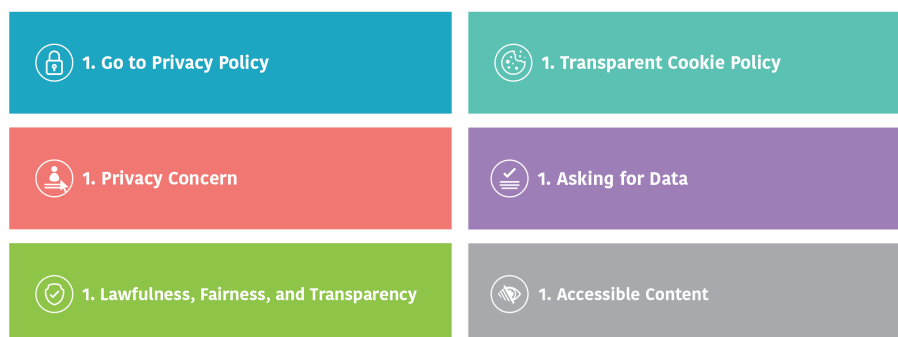


Figure 6.10: Icon labeling of the categories

To sum up, the improved card deck ‘Designing for Privacy’ represents clearer and visually more understandable concept of how to make an online product GDPR compliant. The final version of the card deck ‘Designing for Privacy’ is represented in Appendix G.

Conclusion

This chapter summarizes the results of the thesis and all the insights we gained during the design and evaluation process. We will start with the discussion of possible alternative solutions and critiques to our approach in Section 7.1. Then, we conclude our findings in Section 7.2. Finally, we define limitations and possible improvements for future work in Section 7.3.

7.1 Discussion

In this section we will discuss the experts' and users' feedbacks gathered during the workshop and design evaluation; we will review and reflect to the suggested alternative solutions.

Firstly, given that the focus of this thesis was on creating an aid for UX/UI designers there is a possibility that other effective approaches and techniques can be applied. As it was reviewed in Chapter 2 and pointed during the workshop with privacy and UX/UI experts, existing software solutions (templates, plugins) are developed to offer online businesses a variety of options to make their online products compliant. Some companies even offer a personal assistant that will guide organizations through the process of guarantying GDPR compliance. This approach, however, is quite expensive and does not pay off for small organizations. Furthermore, using similar templates for the privacy concerns, can intensify the problem of reducing the attention of users. In other words, by seeing the same pattern of a cookie banner on every visited website, the likelihood that users ignore information written there would be higher.

Secondly, one of the experts suggested the concept to have an online privacy generator to design a compliant online product. If a designer is interested in creating a cookie bar, he or she can set up their settings and the program will generate a compliant cookie bar. Without a doubt, this solution is more effective and less time consuming

than the use of design patterns. However, such an approach does not provide designers with understanding why it has to be done in that way. In addition, similar to the previous approach, suggested solution can make the web monotonous and privacy issues unremarkable.

Another discussion was focused on user's privacy and possible tools that can help users to protect their data. These include, for example, special applications that search and delete cookies on user's devices. Thus, users will not be tracked even if a website uses cookies without user's consent. Another example can be a software that checks if a visited website does not violate user's privacy. It could also provide users with the possibility to set up their privacy preferences once for all websites they visit. These listed examples, however, focus on how users can protect their personal data, and not on how to make the Internet in such a way that additional data protection is no longer required. Imagine that instead of trying to prevent and solve crimes, the police ask people to stay at home. It should not work in a way that only those users who have special software can be sure about their data safety. From the other side, the idea to have a function where users can set up a level of consent can be quite useful. For example, a user can specify that he or she does not want to share advertisement cookie with any of websites. This setting would reduce the amount of time a user would need to spend on setting up cookie choice at each website he or she visits.

Finally, the richest discussion of the research was related to the users' awareness. The findings from the workshop (see Section 3.4) and usability testing (see Subsections 6.1.2, 6.2.3) have shown that people do not pay attention to their privacy. Due to the ubiquitous technologies, they may not even be aware of privacy choices they make. They do not know and are not even interested in how their personal data are collected, stored and processed. People tend not to read a provided privacy policy; they agree with the use of their personal data for different purposes without recognizing potential risks related to information disclosure. This problem is well represented in the study [60]. The author underlines that since privacy harms may be invisible and not tangible, it is difficult for people to understand possible outcomes or risks of privacy decisions they make. The author suggests that "*[...] it is necessary to gain a better understanding of people's privacy decision-making process. This will enable the building of better privacy choice architectures, providing people with transparent, easy to understand privacy information compliant with legal requirements, such as the GDPR, that may improve people decisions and risk awareness.*" However, this situation does not question the need to create compatible online products, but it raises the necessity to be transparent and understandable to people and to motivate them to be aware of the choices they make regarding their personal data.

In general, the suggestions and alternatives provided to the process of ensuring compliance of an online product are reasonable and understandable. However, the effectiveness of the approach used in this thesis is valid, as it was proved during the expert and end user evaluation.

7.2 Summary

This thesis outlines the approach to properly understand the General Data Protection Regulation, to design and evaluate the aid to support UX/UI designers in making compliant online products.

As the start point, we reviewed already existing approaches to achieving GDPR compliance in Chapter 2. We discovered the issue of user privacy on the web and defined advantages and disadvantages of existing solutions that can support businesses in achieving GDPR compliance.

We moved to the process of understanding the GDPR in Chapter 3. The results from the stage of examining the law (see Section 3.1) helped to define key issues of the GDPR such as its principles, terms ‘privacy policy’, ‘consent’, ‘cookies’, and rights of the data subject. In order to consolidate knowledge and to deepen an understanding of how to design privacy-friendly systems, we conducted the workshop with privacy and UX/UI design experts in Sections 3.2, 3.3. The findings of the workshop analyzed in Section 3.4, helped to define a set of dark and light patterns that could be used to explain key issues of the GDPR to designers. These findings also brought us closer to the understanding of the structure and content of the card deck.

Chapter 4 represented the paper prototype of the card deck ‘Designing for Privacy’ and its evaluation. Having started with defining what is a creativity card deck and design patterns, we extended our research by analyzing the existing toolkits. The results of the review provided us with relevant information about the structure and formation of toolkits, that further influenced the ideation process. Created in Section 4.4 paper prototype with 32 cards was then evaluated by two privacy experts in Section 4.5. The minor changes pointed by the experts were related to including a few new patterns, and to adjust some misleading once.

The following Chapter 5 described the process of designing the patterns. Initially, we set up the layout in Section 5.1. Then, in order to achieve the consistency in design of cards and significantly simplify the design process, the asset library for card deck ‘Designing for Privacy’ was created in Section 5.2. It included a collection of vectors, icons, images, color palettes, fonts, and other design elements. Ultimately, we suggested the style of the cards and designed 42 patterns in Section 5.3, and created an information sheet and a case in Section 5.4.

To understand if created design patterns work, two types of evaluation were conducted in Chapter 6. First evaluation included the deep review of cards by UX/UI designers in Section 6.1. The results of this evaluation demonstrated the validity and usefulness of the design patterns. They also delivered a range of ideas of how created design patterns can be improved in the future. For the usability testing in Section 6.2, participants were presented with the prototype of the privacy-friendly website. The aim of this evaluation was to define if end users could understand what was designed and could easily find necessary information about their privacy. The results of the user evaluation showed

that different users chose alternative scenarios to complete the same task. It means, that privacy-friendly systems should take into account different behavior patterns. This chapter concluded with making final improvements of the design patterns basing on the gathered experts' and end users' feedback in Section 6.3.

As a further step, in the following section we will discuss limitations of the project and highlight improvements for future work.

7.3 Limitations and Future Work

Although the designed card deck was positively evaluated by the privacy experts and UX/UI designers, and successfully tested by users, our work clearly has some limitations. Foremost, created design patterns represent recommendations and do not have legal force. They can be used as a guide during the design process, but not as an official document to refer to. Nevertheless, the card deck can be the first step in introducing the explanation to the law in an explicit and understandable way, with the use of visualized positive and negative examples.

The second limitation lies in the fact that this thesis aims to create GDPR compliant and privacy-friendly online systems, but does not enhance users' motivation to take more care about their privacy. From the one side, users are provided with all necessary information about storing and processing of their data; from the other side, it ensures that in spite users do not care about their privacy concerns, their rights will not be violated. In the future, it is necessary to gain more experience in understanding people's privacy decision-making process. The deeper study of user behavior would improve our understanding of how to design the systems that will increase users' awareness and trigger them to think about their decisions.

Design patterns suggested in this work, demonstrate how to design privacy-friendly websites for the desktop and do not take into account responsive design. Thus, some solutions that apply for the desktop could not work for the mobile version of the site. However, this limitation is expected to be examined and solved in future work.

Finally, despite the fact that each card is supported by visual examples, their number is limited to two. There are definitely situations in which more detailed examples could make more sense and explain the GDPR aspects better. This limitation, however, can be solved in future work by digitalizing hard copy of cards into an online format with an expanding number of examples. Another reason to consider an electronic version of the cards is that it can include a wiki community to discuss and improve the cards.

To sum up, there is always room for improvements, but we believe that our research will serve as a base for future studies on creating privacy-friendly online products.

List of Figures

3.1	Google Privacy & Terms	11
3.2	H&M Privacy Notice	11
3.3	Opt-in cookies bar	12
3.4	Newsletter form of H&M with an agreement consent	13
3.5	Separate consent for three different email lists	13
3.6	Subscription form with the information how a newsletter consent can be revoked	14
3.7	Opt-out cookies bar with the possibility to withdraw cookies anytime	14
3.8	Subscription and unsubscribe forms can be found in the same place on a web page	15
3.9	Amazon's recommendations based on cookies	16
3.10	Classic cookie hint bar without the possibility to decline to store cookies	16
3.11	Classic cookie hint bar without positive opt-in	16
3.12	Cookie bar with opt-in box to decline the use of cookies	17
3.13	A cookie bar with the option to choose the level of consent	17
3.14	Withdrawal of the consent from the same settings window where the consent was given	17
3.15	Information of third party cookies used at designmodo.com	19
3.16	Managing personal data at iCloud	20
3.17	Introduction pop-up with a short message about the privacy policy of H&M	22
3.18	Solution to introduction message	22
3.19	Short overview of user privacy, located in the footer of the web page	23
3.20	Representation of Privacy & Terms by Google	24
3.21	Privacy policy history	24
3.22	Privacy concerns	25
3.23	Non-compliant cookies bar that forces users to share their data if they do not want to pay for the browsing a website	25
3.24	Cookie bars	26
3.25	Cookie bar with a hidden configuration function	26
3.26	Solution to the compliant cookie bar	27
3.27	A sticky button with an option to change cookies preferences any time	27
3.28	Cookies configuration window with the cookie arrangement	28
3.29	Information about each third party is represented as an expandable box	28

3.30	Usage of pre-selected checkboxes for each third party and purpose	29
3.31	Solution to third party cookies declaration	29
3.32	Two-step subscription to a newsletter	30
3.33	Consent agreement with a link to full information	30
3.34	Configuration of newsletter topics	31
3.35	Unsubscribing from a newsletter in Profile Settings	31
3.36	Unsubscribing from a newsletter directly from email	32
3.37	Unsubscribing from a newsletter on the web page	32
3.38	Solution to unsubscribing form	32
3.39	Online form to access/change/erase user data	34
4.1	‘Superpowers Card Deck’	36
4.2	Examples of cards from ‘UI Pattern card deck’	36
4.3	IDEO Method Cards	37
4.4	Visualization of ‘Silk Method Deck’ card	38
4.5	Iconic visualization of ‘Roadblocks to innovation card deck’	38
4.6	Workshop using the MethodKit cards as headlines for sorting thoughts and ideas	39
4.7	Card with a visual example from ‘Design with Intent’ card deck	39
4.8	Grouped cards of ‘Zig Zag creativity card deck’	40
4.9	Manual how to use ‘Strategy Card Deck’	40
4.10	Card of ‘Group Works Card Deck’ with a list of related patterns	41
4.11	Concept design of a card with a privacy recommendation	43
4.12	Concept design of a card with a privacy principle	43
4.13	Prototype of a card (front and back)	44
4.14	Paper prototype with 32 design cards	44
4.15	Solution to the card with informed identification	46
4.16	Legal content limitation: users are asked to pay a PUR-Abo if they do not want to be tracked	47
5.1	Layout and measurements of a card	50
5.2	Asset library with the color palette, font hierarchy, and icons	51
5.3	Transforming a real user interface into abstract one	52
5.4	Design of the card ‘Accessibility’	53
5.5	Design of a card from the set ‘GDPR Principles’	54
5.6	Variations of the cards from the set ‘GDPR Aspects’	54
5.7	Light pattern with a user flow	55
5.8	Design of the Introduction Sheet	57
5.9	Design of the box	58
6.1	User flow of the ‘Cookie Settings’ case	63
6.2	User flow of the ‘Cookie Purpose’ case with 3 different scenarios	63
6.3	User flow of the ‘Privacy Concerns’ case with 2 different scenarios	64
6.4	User flow of the ‘Newsletter Subscription’ case with 2 different scenarios	64

6.5	User flow of the ‘Identification’ case	65
6.6	Visual prototype of GDPR compliant website	66
6.7	Usability testing process	67
6.8	Customize Cookies window with disabled toggle button for Necessary cookies	68
6.9	Part of Identification form with the privacy button and information text .	68
6.10	Icon labeling of the categories	69

List of Tables

2.1	Analysis of existing approaches to make an online product GDPR compliant	5
-----	--------------------------------------------------------------------------	---

Appendix

Appendix A: Use cases for workshop discussion

Use Case	Examples to discuss
Transparency	
1. Transparency via introduction message A user visits a web site.	Example A: at the beginning the light box with intro about transparency appears. It says: 'We care about your privacy'.
Privacy Policy	
2. Find a Privacy Policy (Location) A user is interested in privacy policy of the web site he visits. He or she wants to find the page that will tell him/her more information about privacy issues of the website.	Example A: A sticky button on the bottom of the page – fast access to the privacy policy any time. Example B: A user can barely find privacy policy in the footer. Example C: Quick privacy issues in a footer and links to Privacy and Cookie Policy.
3. Privacy Policy overload A user goes to the Privacy Policy page of the web site in order to find out more information about his or her privacy.	Example A: Privacy Policy as overlay. Example B: Privacy Policy as a new page of another web site. Example C: Privacy Policy structured. Example D: Privacy policy on the web page without Table of contents.

Cookies	
<p>4. Turn off cookies (opt-in) A user visits a web site. He or she does not want to share his or her cookies data with this web site, he or she wants to know how to turn cookies off.</p>	<p>Example A: Pop-up window with ability to accept/customize cookies. Example B: Pop-up window with ability agree/disagree all cookies. Example C: Classical cookies message with explanation how to turn off cookies in your browser.</p>
<p>5. Change a decision (opt-out) After turning off all cookies a user wants to share some of them to make an online service more personalized for him/her.</p>	<p>Example A: A sticky button opens the overlay where a user can set up cookies any time. Example B: Cookie settings are accessible from Cookies Notice page.</p>
<p>6. What cookies and who has access to them A user wants to know with whom (third parties), what data, how long, for which purpose this data is shared. He or she wants to set it up manually.</p>	<p>Example A: Giving a list of third parties with short info about each company. Example B: All purposes of data collection and third parties are selected by default. Example C: All info about each cookie that is collected.</p>
Consent	
<p>7. Subscribe for a newsletter A user is interested in news/updates about online resource he or she visits.</p>	<p>Example A: Two-step subscription. Huge text with privacy issue to consent directly near a checkbox. Example B: One-step subscription with a direct link from the startpage. Checkbox with a link to Data Privacy explanation that a user has to consent.</p>
<p>8. Newsletter settings A user would like to set up what information he or she would like to receive by email.</p>	<p>Example A: All categories are included automatically, no possibility to change it. Example B: A user can select topics he or she is interested in. By default, however, all topics are already selected. User has to uncheck every item he or she is not interested in.</p>

9. Newsletter withdraw

A user wants to unsubscribe from the newsletter.

Example A: (Indirect) withdraw of consent on the webpage Service – Newsletter – Newsletter unsubscribe.

Example B: Withdraw of consent direct from Newsletter or from settings in user account.

Manage Personal Data

10. Manage user data

A user wants to know what of his or her data is stored and get a copy of his or her data 'to go'.

Example A: Manage user data in icloud service. Get a copy of user's data within 1 week.

11. Erase user data

A user wants the company to remove all his or her data.

Example A: GDPR Data Request Form Template Online.

Example B: Delete my account/data: written and signed request template.

Appendix B: Asset Library

1. Color Palette



2. Font Hierarchy



3. Icons



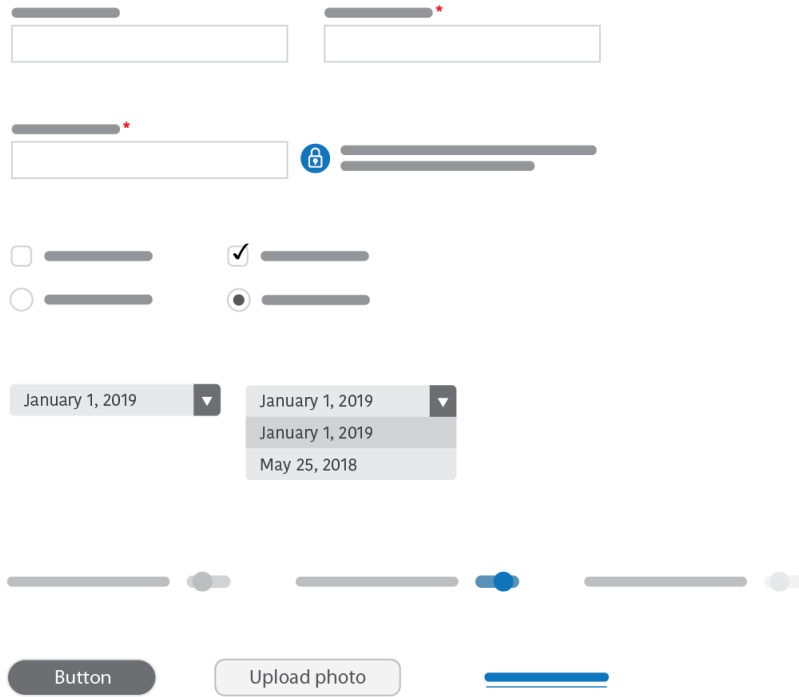
4. Frames



5. Content



6. Forms & Navigation



7. Additional Elements



Appendix C: Use cases for design patterns evaluation

Use Case	Task
Privacy Policy	
1. Privacy Policy Text You are given a 'Privacy Policy' text with a large volume of content to place on the web page.	Suggest changes in design of the page in order to make the privacy policy more readable for users.
2. Data Breach Your website was hacked, it is likely that all personal data such as emails and passwords of your customers were stolen.	Inform users about data breach. Suggest measures that can be taken to make users' data safe.
3. Redirected Privacy A user of your website would like to read more about privacy policy. He or she clicks the link 'Privacy Policy' and is redirected to the another web site.	Discuss the situation with redirected privacy link. Suggest a solution to how to make users aware where they are?
Cookies	
1. Cookie Consent Your web site uses different categories of cookies: essential, functional, marketing.	Inform users about cookies you use. Suggest a cookie banner, so users can configure their cookie choice.
2. Third Party Cookies Your website shares users' personal data with third parties.	Discuss given examples of 'third party cookies' representation. Suggest the solution to inform users about all third parties you share data with in a transparent and user-friendly way.
3. Withdrawable Cookies A user of your website firstly accepted the use of all cookies on your web site. Now, however, he or she would like to decline it.	Make it easy for users to find how they can withdraw given for cookies consent. Suggest a solution to where the withdrawal can take place in order user could easily find it.
Forms and Consent	
1. Informed Consent You are planning to provide your users with the possibility to request a DEMO of your system.	Suggest a privacy-friendly DEMO request form. Notify users what happens to their data provided during the request.

2. Question of Choice You are given 3 solutions to newsletter subscription form.	Discuss given solutions and suggest an optimal solution to the subscription form.
3. Withdrawable Consent A user of your website subscribed to your newsletter, but then moved out to another country. Receiving this newsletter is not more relevant for the user.	Suggest an easy way the user can unsubscribe or configure his or her newsletter settings.
<hr/> Manage Personal data <hr/>	
1. Privacy Concerns You are given 3 examples of Privacy Concerns provided by different web sites.	Discuss given solutions and suggest an optimal solution to the privacy concerns.
2. Data to take away A user would like to know what data about him or her is stored on your service.	Suggest and describe a flow how the user can get an overview of all data you store about him or her.
3. Identification A user of your website would like to change his or her contact data since it is not relevant anymore.	Suggest a simple identification process that the user have to complete in order to send a 'data change' request.

Appendix D: Interview questions for the design patterns evaluation

Block 1: Understanding of patterns

- How clear and understandable are patterns? Did you have any problems while reading design patterns?
- Would it be easy for you to design a GDPR compliant website with the help of these design patterns?
- What do you think about the explanation text of the design patterns? Does it help to understand them better?
- How do you find idea to have bad and good design patterns?

Block 2: Navigation

- How easy it is to navigate via different categories? Is the structure of the card deck clear?
- How would you start to use them? Reading one after each other or by selecting cards that answer your concrete questions?
- Would you use reference to the Article to read more information about some aspects? Do you find these references useful?

Block 3: Visual language

- What do you think about visual language of the patterns in total (fonts, icons, colors)? Have you noticed some design problems, inconsistency etc.?

Block 4: Feelings and Improvements

- What are your feelings about using these patterns while designing an online product? Do you find it useful?
- Is there something that can be improved?

Appendix E: Wireframing of the Visual Prototype of the GDPR Compliant Website

Figure E1: Use Case 1: Cookie Settings

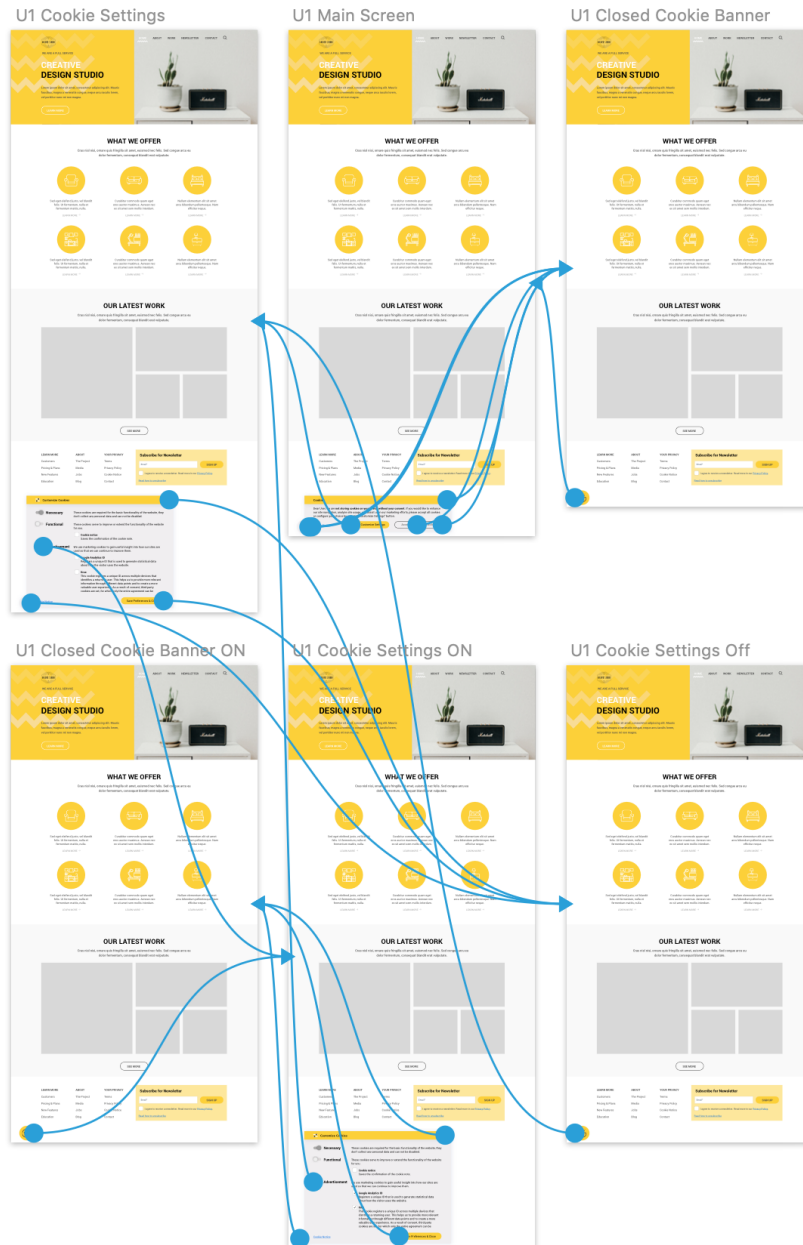


Figure E2: Use Case 2: Cookie Purpose



Figure E3: Use Case 3: Privacy Concern

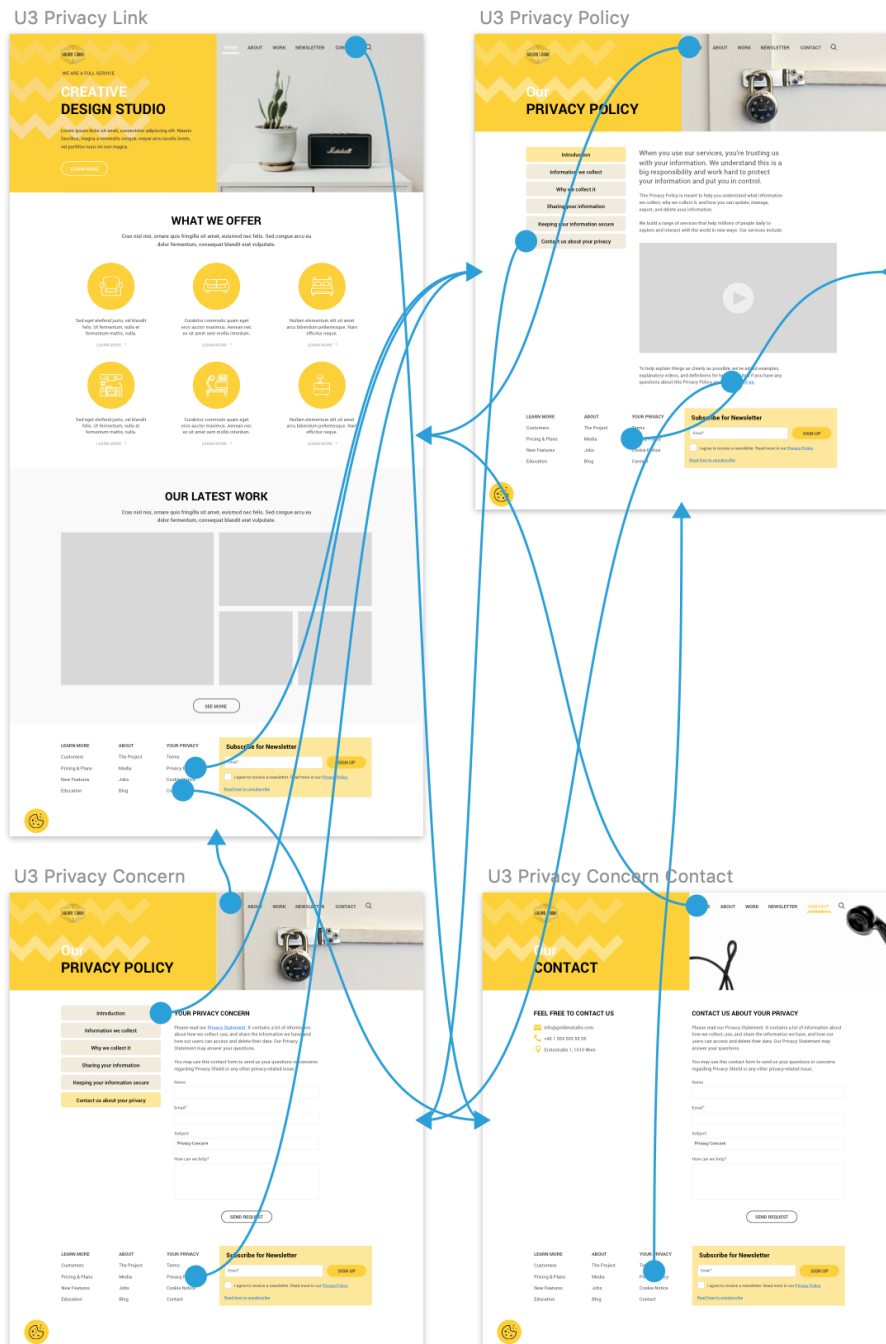


Figure E4: Use Case 4: Newsletter Subscription

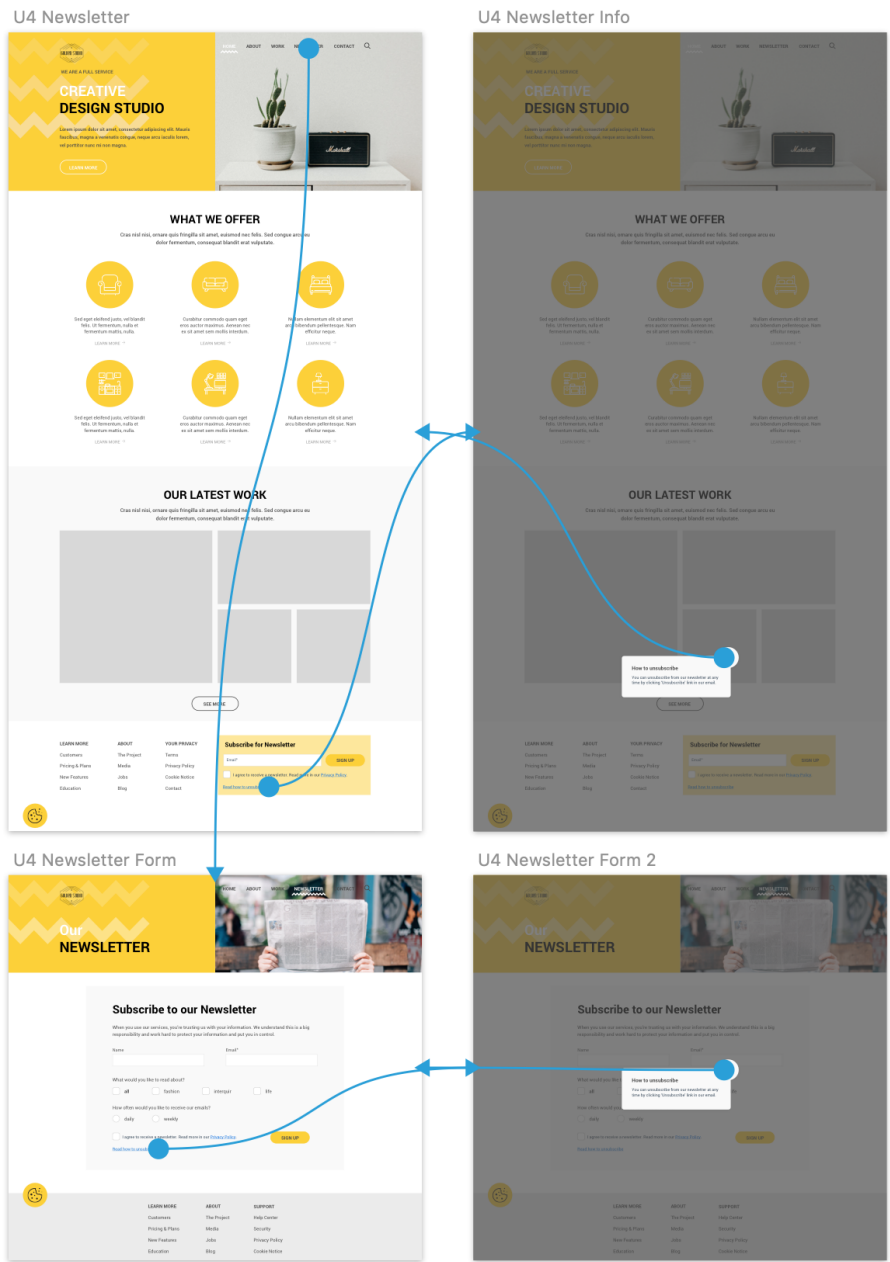
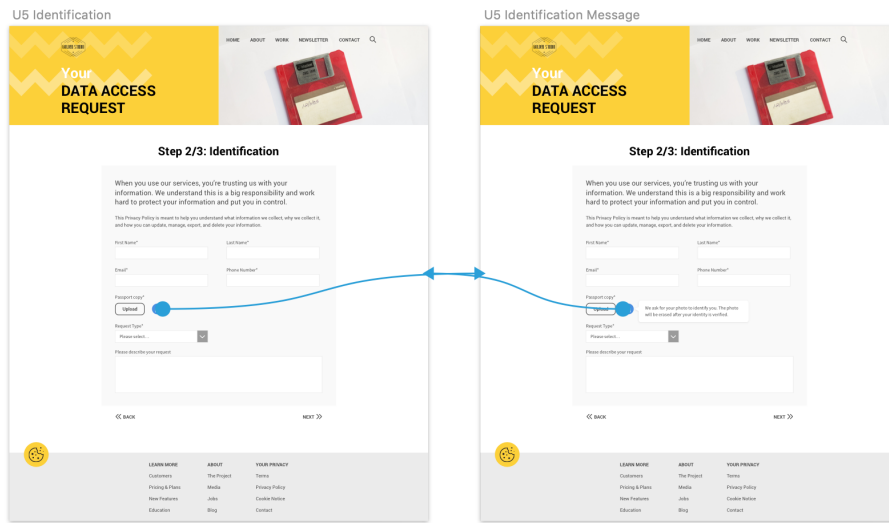


Figure E5: Use Case 5: Identification



Appendix F: Interview questions for usability testing

Block 1: Cookie Settings

- What do you think about a pop-up cookie banner? Would you ever set up your cookie choice? How notable do you think this feature should be?
- What do you usually do with information on cookie banner?

Block 2: Cookie Purpose

- Were you ever interested in how long and for which purpose websites are storing and using cookies? Would you like to know more about this?
- What are your thoughts about tab navigation inside Cookie Policy? Is it easy to find what you are searching for in that way?

Block 3: Privacy Concern

- What is the easiest way for you to communicate with a web service about privacy issues? Would you prefer to have a request form or other information to contact a service?

Block 4: Newsletter Subscription

- While subscribing to a newsletter, do you pay attention to how unsubscribe from this and what you are subscribing for?
- Do you check how provided by you personal data will be used after subscription?

Block 5: Identification

- Have you ever tried to delete your data/account? Could you share your experience? Was it easy or difficult?
- Have you ever experienced an online identification process (to restore your account, data, etc.)? Can you remember any complicated examples?

Block 6: Feelings and Thoughts

- How would you define privacy-friendly websites?
- What are your feelings about using privacy-friendly websites? Would you trust them more?

Overall, how difficult or easy did you find each task? Evaluate each task from 1 to 5, where 1 is 'very easy', 5 is 'very difficult'.

	Very easy			Very difficult	
	1	2	3	4	5
1. Cookie Settings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. Cookie Purpose	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. Privacy Concerns	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. Newsletter Subscription	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. Identification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Appendix G: Card Deck 'Designing for Privacy'

Accessibility



1. Accessible Content

Make your web content more accessible to people with disabilities.

Pay attention to accessibility of your content when designing an online product. Ensure people with disabilities can visit, understand and interact with your website.



Where to find this
WCAG 2.0 (W3C)



Subscribe for Newsletter


```
...  
<input type="text" aria-label="name">  
<input type="email" aria-label="emailRequired">  
<input type="submit" aria-label="submit">  
...
```

Accessible form where each of the inputs has a related aria-label. Assistive technologies, such as screen readers, use labels to announce the purpose of inputs to users.



1. Lawfulness, Fairness, and Transparency

Process user data in a transparent and fair way.

Identify valid grounds under the GDPR for collecting and using personal data. Be clear, open and honest with users from the start about how you will use their personal data.



Where to find this
Article 5(1a)



What?

██████████
██████████
██████████
██████████

Why?

██████████
██████████
██████████
██████████

How?

██████████
██████████
██████████
██████████

On the website, users are provided with a privacy policy explaining in clear and transparent ways what type of data you collect, the reason you are collecting it and how it will be processed.



2. Purpose Limitation

Collect personal data for specified and legitimate purposes.

Process all user data for specific purposes. You must gain consent from users for this.



Where to find this
Article 5(1b)



1

✓ I agree to give the **Company A** permission to send me messages

2

Unread Messages
Company B Special offer for you... Today

After giving their consent to emailing from one company (1), users also receive special offers (2) from a partner-company, for which no consent was obtained.



Cookie

Cookie	Name	Purpose
██████████	██████████	██████████
██████████	██████████	██████████
██████████	██████████	██████████

The purpose of each cookie used by the website is clearly identified and explained to users.



3. Data Minimization

Limit the amount of user data you process.

Review all data you hold: what is it and why do you have it?
Only collect and retain data that is required.



Where to find this
Article 5(1c)

GDPR Principles



For credit, invite some people

From:

Your name:

Send to emails:

[+ Add from address book](#)

To invite new people, users have to import their address book to select whom to notify about a product.



Registration

Name:

Email:

Password:

Delivery Address:

The registration form of a delivery company only contains necessary data for the customer-company relationship.



4. Accuracy

Keep user data up to date.

Ensure all data you store about your users is accurate, up to date and accessible. Ideally, users can securely update or delete their data by themselves.



Where to find this
Article 5(1d)

GDPR Principles



1

My Profile

Name:

Phone:

Email:

Delivery address:



Save Changes

2

Customer Information

Name:

Phone:

Email:

Delivery address:

Confirm Changes

After a user changes the address in his or her profile (1), the company updates their records for customers' changes (2) so that goods are delivered to the correct location.



5. Storage Limitation

Only keep user data for as long as you need it.

You should also periodically review the data you hold, and erase or anonymize it when you no longer need it.



Where to find this
Article 5(1e)

GDPR Principles



Applicant Data

Name: _____
Surname: _____
Age: _____
Phone: _____
Email: _____



The employer keeps recruitment records for unsuccessful applicants after the process has been ended and applicant's data is not needed anymore.



Customer Data

Name: _____
Surname: _____
Provided services: _____

A company keeps some personal data about a previous customer in case they will have to deal with any complaints the customer might make about the services they provided.



6. Integrity and Confidentiality

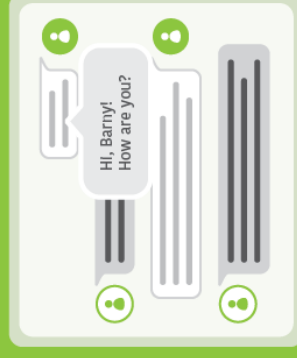
Protect user data.

You must protect user data against unlawful processing or loss; encryption and privacy by design are required.



Where to find this
Article 5(1f)

GDPR Principles



Online service provides end-to-end encryption for user-to-user text messaging. Encrypted messaging prevents anyone from monitoring text conversations of their customers.

Part 1. Privacy Policy



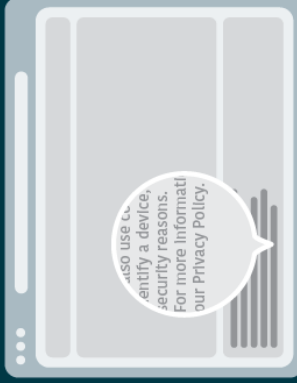
1. Go to Privacy Policy

Place a link to the privacy policy in a way users can easily find it.

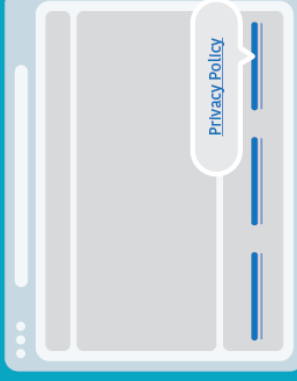
Make it easy for users to find a link to your privacy policy by placing it in the place most expected by them.



Where to find this
Article 5(1a), Recital 58



The privacy policy link is hidden in a long paragraph so it's hard to find it.



The privacy policy link is placed in the footer.

Part 1. Privacy Policy



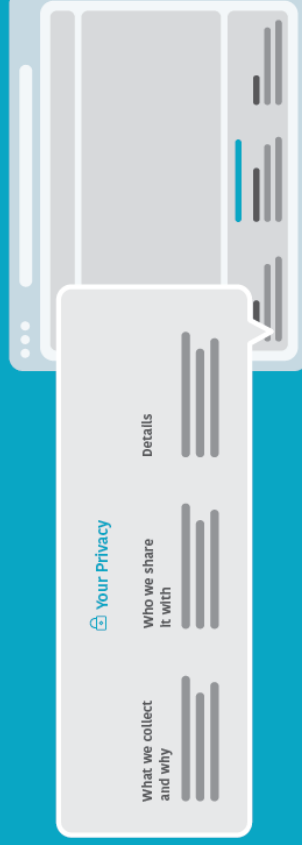
2. Privacy Overview

Notify users about the transparency of your web site.

Tell users in a few words what data you are collecting from them, who you share it with and why. Make users aware of privacy issues in a glance.



Where to find this
Articles 12-14, Recital 58



Short introduction message about users' privacy placed in the footer.

Part 1. Privacy Policy



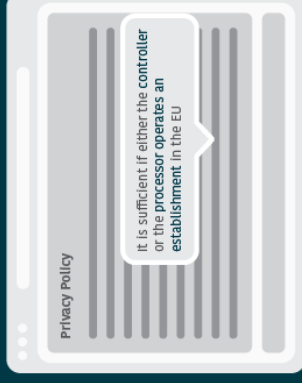
3. Privacy Language

Write your privacy policy in a clear and understandable language.

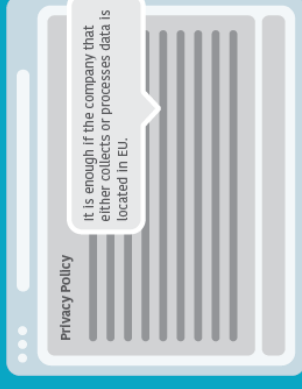
Don't overload users with hard-to-read text written by lawyers for lawyers. Simplify legal terminology to understandable phrases.



Where to find this
Article 12(1), Recital 58



Hard-to-read text with legal terminology.



Simple explanation of users' privacy.



4. Privacy Visualization

Visualize your privacy policy.

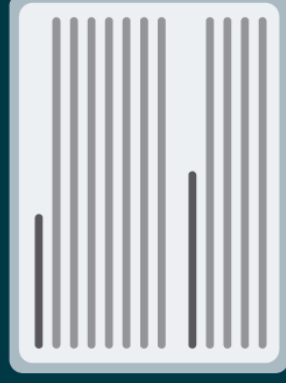
Break up large amounts of text with short videos or/and images about privacy issues that may concern your users.



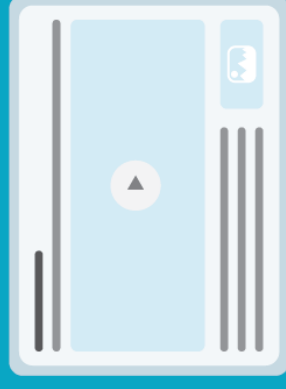
Where to find this
Article 12(1), Recital 58



UX
advice



Large volume of continuous text that is hard to read.



Instead of using a wall of text, illustrations or videos are used to explain privacy issues.



5. Privacy Structure

Structure and group the privacy issues.

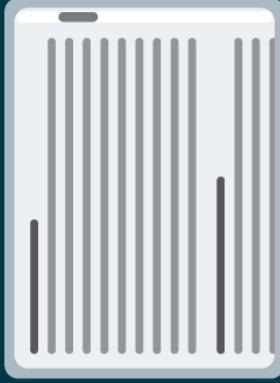
Make it easy for users to navigate through your privacy policy by structuring and grouping privacy issues. Provide users with a table of content and fast navigation to the privacy issues they are searching for.



Where to find this
Article 12(f), Recital 58



UX
advice



Large volume of continuous text, navigation via scrolling.



Privacy issues are grouped using tab navigation.



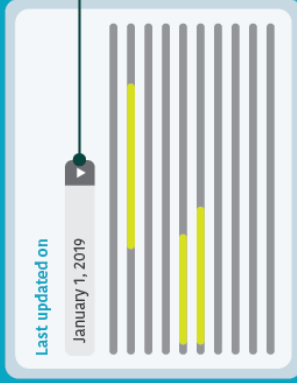
6. Privacy History

Inform users whether your privacy policy changes.

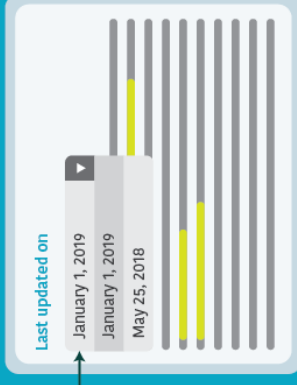
Tell users that something changed in the privacy policy since their last visit. Provide a history of changes so users can clearly see what has been changed.



Where to find this
Article 5(1d)



The privacy policy history with highlighted changes.

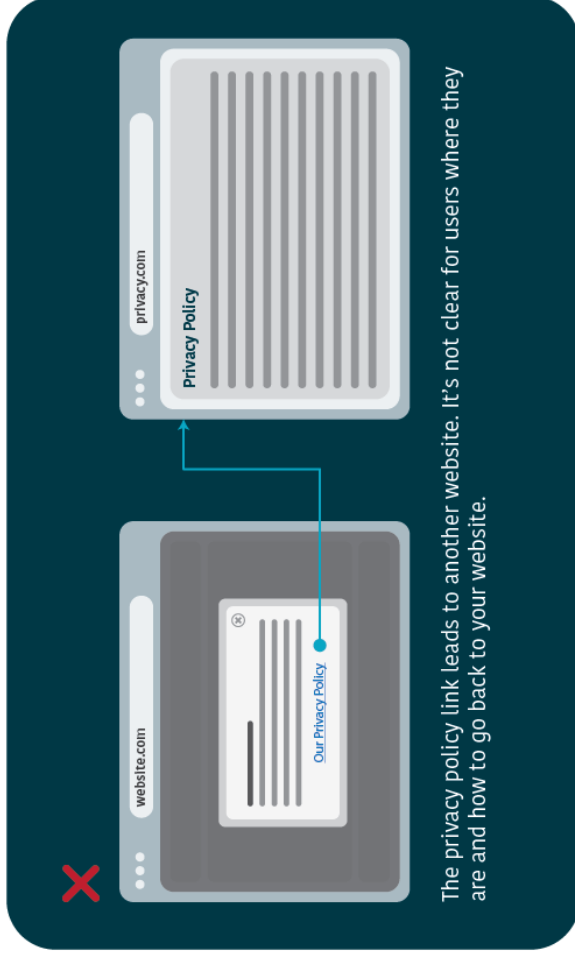




7. Redirected Privacy

Don't bring users to another place.

Don't send users for reading your privacy policy to another web resource.



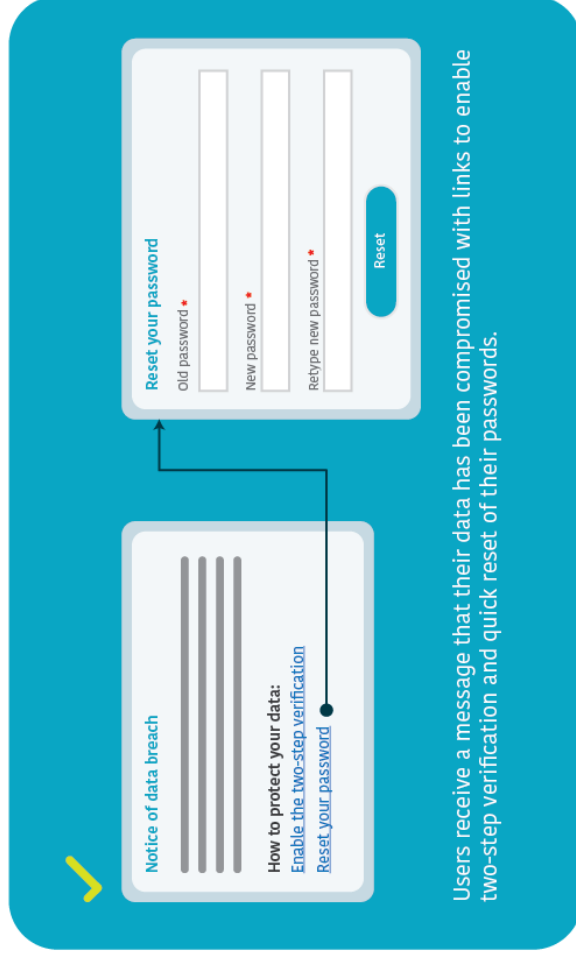
The privacy policy link leads to another website. It's not clear for users where they are and how to go back to your website.



8. Data Breaches

Inform users if their data might have been compromised.

Communicate personal data breaches to your users. Tell them how they can protect their data.



Users receive a message that their data has been compromised with links to enable two-step verification and quick reset of their passwords.

Part 2. Cookies



1. Transparent Cookie Policy

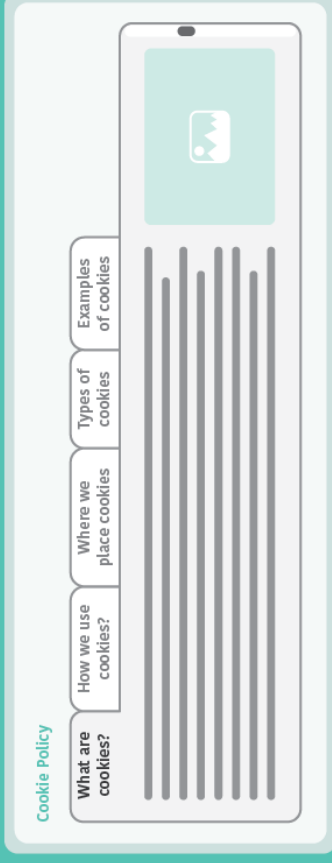
Give users insight into how their data are being used.

Tell users in a clear and plain language what, how, for which purposes and how long cookies are used.



Where to find this
Articles 12-15, Recitals 58, 60

Part 2. Cookies



Structured information about cookie policy answering all necessary questions.



2. Find Cookie Consent

Don't hide your cookie consent from users.

Make it easy for users to find the cookie consent at the beginning of their visit.

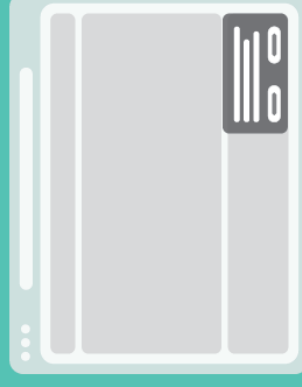


Where to find this
Article 15, Recital 58

Part 2. Cookies



Classical cookie banner is hidden inside the content of the page.



Cookie banner as a sticky overlay that can't be overseen.



3. Compliant Cookie Banner

Make your cookie banner compliant.

Implied consent and consent given simply by visiting your website is not enough. Provide users with the possibility to refuse to give their consent for cookies.



Where to find this
Article 7, Recital 32



Cookies
This website uses cookies. By continuing to use this site, you agree to the use of all cookies.

OK

Classical cookie banner with default agreement to all cookies.



Cookies
This website uses cookies to enhance browsing experience and provide additional functionality. [Details](#)

Agree Disagree

Cookie banner with the possibility to agree/disagree to the use of all cookies and a link to cookies details.



4. Cookies by Default

Assure users that no their data is used without their consent.

Make it clear to your users that before they give their permission to the use of cookies, no their data is collected and stored by your website.



Where to find this
Article 25, Recital 78



Cookies help us to deliver our Services. By using our Services or clicking I agree, you agree to our use of cookies.

[Learn more](#)

I Agree

Classical cookie banner that informs users about the constant use of all cookies.



Cookies
We don't use cookies without your consent. If you would like to enhance the functionality of our website, please configure your cookie choice in settings.

[Cookie Notice](#) [Cookie Settings](#)

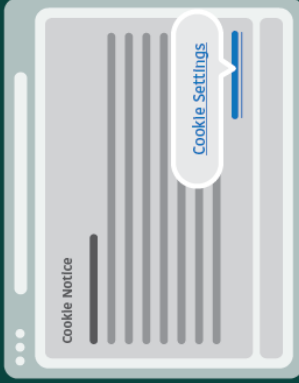
Cookie banner with a message that no cookies are used without user's consent.



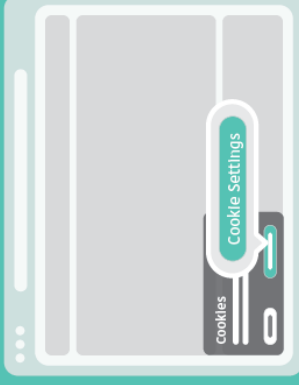
5. Cookies Configuration Link

Make it easy and clear for users where they can set up their cookies choice.

Don't hide the possibility to configure cookie choice from your users. Don't bundle it with the Cookie Policy.



Cookie configuration is bundled in Cookie Notice.



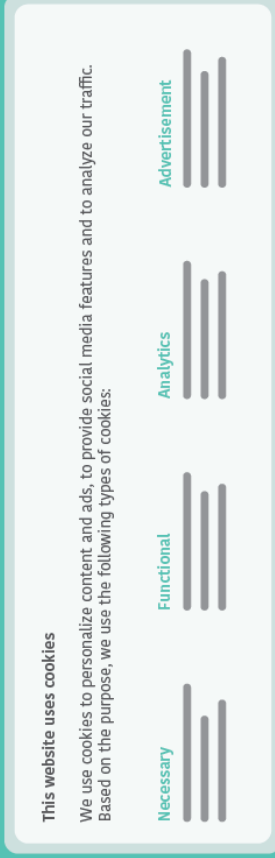
Direct link to the cookie configuration window from the cookie banner.



6. Cookie Grouping

Arrange cookies into intelligible categories.

Explain to users which categories of cookies you use, for which purposes do you use them. Make it clear that some cookies that don't contain personal data may be used without user's consent.



Cookies are grouped into 4 categories with a short explanation of each of them.



7. Cookies Choice

Allow users to set up their cookies choice (opt-in).

By clicking on an opt-in box or choosing settings from the menu, users should be able to select which cookies they would like to use. Pay attention not to have pre-ticked agreement on the consent form.



Where to find this
Article 7, Recital 32



UX
advice



Cookies
This website uses cookies:

- ✓ Necessary
- ✓ Functional
- ✓ Advertisement

Decline Accept all

Users can either accept or decline all cookies.



Cookie Settings
Please set up your cookie choice.

Necessary don't store personal data

Functional

Advertisement

[Cookie Notice](#) Save Preferences

Users can configure their cookie choice in Cookie Settings.



8. Third Party Cookies

Provide users with a declaration of all third parties your website shares cookies with.

Users should be able to get all necessary information about third party cookies (e.g. name, provider, purpose, expiry, type) in a structured and clear way.



Where to find this
Articles 7, 15



Cookie Declaration

Necessary (10)	Functional (15)	Analytics (22)	Advertisement (132)	
			Provider	Purpose
Name	Expiry	Type		

Overview of all third party cookies with important information about each of them.



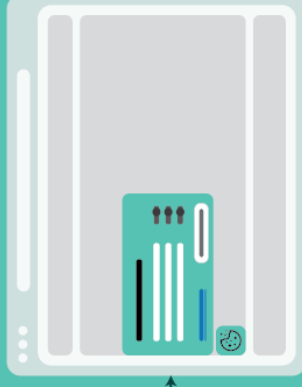
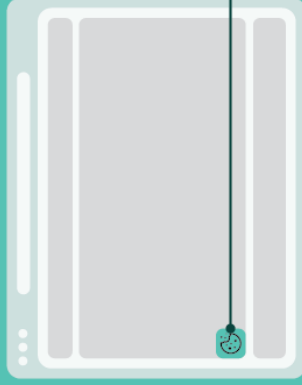
9. Withdrawable Cookies (Opt-out)

Give users the possibility to withdraw their consent at any time.

Make sure that users have access to their current consent state at all times and can change the settings or withdraw their consent in the same way as it was given.



Where to find this
Articles 7(3)



Sticky 'cookie' button brings users to the box with cookie configuration where they can revoke consent at any time.



10. User-Friendly Dialogue

Don't impose users with a "right" decision.

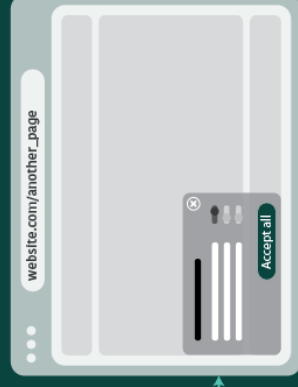
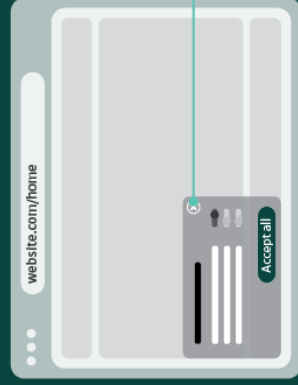
Don't bother users who didn't give you consent by constantly asking if they would like to change their preferences. Provide users with a possibility to have a true choice.



Where to find this
Recital 32(1)



UX
advice



A pop-up with cookie request appears on every page a user visits until he or she accepts all cookies.



1. Asking for Data

Collect only necessary data.

Don't force users to provide huge volumes of personal data that is not required for the service to be used.



Where to find this
Article 5(1c)



Users are required to fill in their home address while subscribing to the newsletter.



Email field is required as a service will send a reply by email.



2. Positive Consent

Provide consent forms with a positive opt-in.

Consent must be freely given. Don't use pre-ticked boxes or any other techniques that may influence user choices.



Where to find this
Recital 32



Overseen pre-ticked box with signing up for a newsletter during the registration.



Positive consent with a link related to the privacy concern.



3. Informed Consent

Inform users about what will happen to their data.

Provide users with a clear explanation of how the data they submit is going to be stored and used.



Where to find this
Recital 32

The illustration shows a form with several input fields. Each field is highlighted with a blue padlock icon, indicating that each field is protected and its data will be stored and processed. A callout box points to one of the fields with the text: "We ask for your birth date to verify your age. This data will be erased after approval." A "Continue" button is visible at the bottom of the form.

Each field of the form is provided with information about how the data will be stored and processed.



4. Separate Consent

Separate newsletter consent from your general Privacy Policy.

Provide a separate privacy policy for the newsletter; hiding your subscription's terms and conditions in some 50-page long general terms and conditions does not cut it anymore.



Where to find this
Recital 32(5)

The illustration is split into two panels. The left panel, marked with a red 'X', shows a "Privacy Policy" document with a callout box labeled "Newsletter consent" pointing to a section of text, indicating that newsletter consent is bundled with the general privacy policy. The right panel, marked with a green checkmark, shows a form with a callout box containing the text: "I would like to sign up to receive Website Newsletter. I have read and accepted the [Terms & Conditions](#)." Below the callout is a "Subscribe" button, indicating that newsletter consent is separate and placed directly on the form.

Newsletter consent text with a link to Terms & Conditions is placed directly on the newsletter form.

Newsletter consent is bundled with Privacy Policy.



5. Redirected Subscription

Avoid two-step subscription.

Make it clear to users what is waiting for them after they provide their data.



Confusing two-step subscription: after filling out their email addresses, users are sent to the page with a large number of additional fields and consent.



6. Question of Choice

Allow users to decide what they want to subscribe to.

Provide users with options to choose categories of content and how often they would like to receive your newsletters.



Newsletter form with auto subscription for all partners' newsletters.

Newsletter settings to set up what users would like to subscribe to.



7. Double Opt-In

Offer users to confirm their consent.

After filling out a signup form, send your subscribers a confirmation email where they have to confirm their signup. This process will let you know the email address is valid.



Join our Newsletter

Subscribe

Hello User,
Thank you for subscribing for our Newsletter.
To confirm your email, click the button below.

Confirm my address

After online subscription to the newsletter, users receive an additional email asking them to confirm the subscription.



8. Withdrawable Consent (1/4)

Give users the possibility to withdraw consent easily.

Provide users with a quick and convenient option to withdraw consent. The withdrawal must be as easy as giving consent.



Where to find this
Article 7(3)

Sign in to unsubscribe

Unsubscribe

If you are not interested in receiving our newsletter anymore, you can [unsubscribe](#) from this list.

Account Settings
Receive Newsletter

Save

Users are required to log in before they can unsubscribe.

Users can unsubscribe directly from the email as well as in Account Settings.



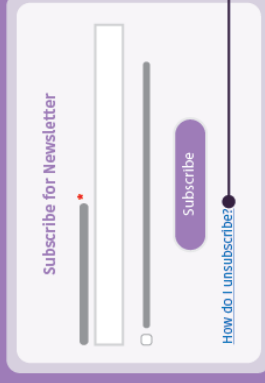
9. Withdrawable Consent (2/4)

Tell users how they can withdraw the given consent.

Make sure users are informed about their right to withdraw their consent at any time.



Where to find this
Article 7(3)



How do I unsubscribe?

You can either click on the unsubscribe link at the bottom of the email or change the settings in your account.

Subscribe form contains a link to information about how users can withdraw their consent to receiving a newsletter.



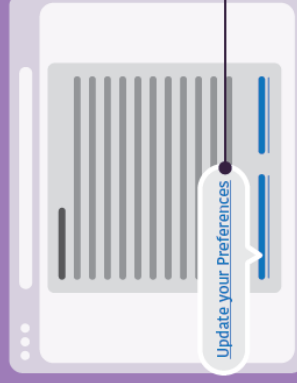
10. Withdrawable Consent (3/4)

Allow users to decide what to withdraw.

If a website offers its users the option to set up their preferences while subscribing for newsletters, then users should be able to have the same option when they are unsubscribing from them.



Where to find this
Article 7(3), Recital 32(6)



Email Preferences

What would you like to receive?

Exclusive offers.

The latest fashion news.

Offers from our [Partners](#).

How often?

daily

weekly

Update

Update your Preferences

Users are given the possibility to update their email preferences instead of unsubscribing from all emails.



11. Withdrawable Consent (4/4)

Inform users about the consequences of withdrawing their consent.

Make it clear to users what will happen after they revoke their consent with their personal data stored on your server.



Where to find this
Recital 39(5)



UX
advice



Unsubscribe from all emails

Please note that in this case you will also not receive emails with offers for you anymore.

Unsubscribe

Note

Unsubscribing from our emails doesn't cause deletion of your account. You can customize or delete your data in your [Account Settings](#).

Users are informed what will happen to their data after they unsubscribe from all emails.

Part 4. Manage Personal Data

Part 4. Manage Personal Data



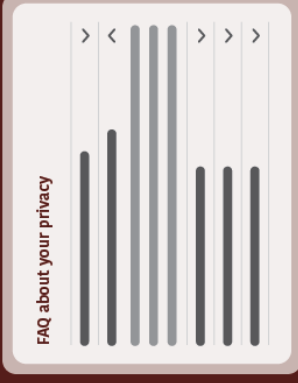
1. Privacy Concern

Give users the possibility to contact you about their privacy.

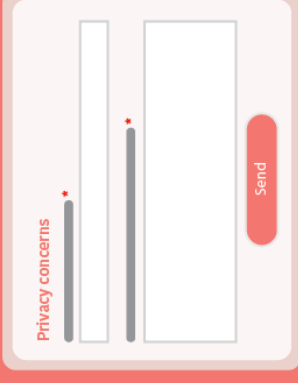
Provide users with contact information so they can easily contact your service when they have privacy-related questions.



Where to find this
Article 15



Users have to search for answers to their questions in the FAQ.



Users are provided with a contact form to send questions about their privacy concerns.

Part 4. Manage Personal Data



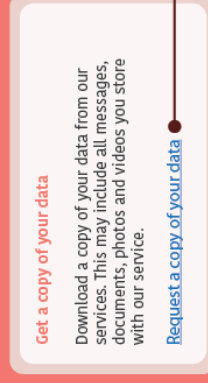
2. Data to Take Away

Show users what data you store.

Make it possible for users to get a copy of their data. This will provide users with a transparent overview of what data, files and documents are stored.



Where to find this
Article 15, Recital 63



Users are given the option to get a copy of all personal data that the online service stores about them.





3. Data Change/Erase Request

Give users the possibility to change or delete their data.

Allow users to change or delete their data in a user-friendly way. Inform users about when their data will be completely deleted from the system.



Where to find this
Articles 16-17, Recitals 65-66



Erasure Request

If you wish, we will remove your contact info from the system.

Please download the form below, then print, complete, sign and submit the form to gdpr@website.com.

Download a request form

Users have to download a form, then print, complete, sign and submit it per email.

The screenshot shows a web form titled "Erasure Request". It has two input fields at the top, each with a red error indicator. Below them is a larger text area. At the bottom right is a "Submit" button.

Users are provided with a simple online request form to change or delete their data.



4. Simple Identification

Simplify the process of user identification.

Don't make the process of data access/change/erase more complicated than the process of creating an account.



Where to find this
Article 11, Recital 64



Your Identification

Step 2/5

Upload photo

Back

Next

Users are required to complete the 5-step identification process before they send a request.

The screenshot shows a web form titled "Your Identification" at "Step 2/5". It has an "Upload photo" button, a "Back" button, and a "Next" button. There are three input fields, each with a red error indicator. A "Confirm" button is at the bottom right.

Simplified identification of a user by name, email, and phone number.





5. Informed Identification

Tell users what happens to their personal data after passing the identification.

Inform users how you will deal with their personal data provided during the identification process.



Where to find this
Article 12, Recital 60



Your Identification

Upload photo

We ask for your photo to identify you. The photo will be erased after your identity is verified.

Confirm

Users are informed what will happen to their data after the identification process is completed.



6. Final Erase

Make users aware that they have the right to erase and what are the consequences of their full data (account) removal.

Users should be aware of what will exactly happen once their accounts are deleted in order to avoid future surprises.



Where to find this
Article 17



Delete your Account

Please confirm the removal of your account.

Confirm

Note

By deleting your account, your documents photos, videos, and messages will be deleted. Irretrievably. You will not be able to receive or send any message.

Not sure yet? You can also [deactivate your account](#) for 14 days.

Message with an explanation of what will happen is given to the user before the data is erased.

Bibliography

- [1] European Parliament and Council of European Union. *Regulation (EU) 2016/679 on the protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Official Journal of the European Union, 2016.
- [2] EU GDPR Information Portal. The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. <https://www.eugdpr.org>, 2018. [Online, accessed 12-February-2019].
- [3] Armen Ghazaryan. UX design and GDPR: Everything you need to know. <https://designmodo.com/ux-gdpr/>, 2018. [Online, accessed 12-February-2019].
- [4] Website Monitoring Evidon – Digital Governance, Privacy Compliance. How to make your website compliant with the GDPR. <https://www.evidon.com/wp-content/uploads/2017/10/Evidon-How-to-Make-your-Website-GDPR-Compliant.pdf>, 2017. [Online, accessed 12-February-2019].
- [5] Ety Khaitzin, Roe Shlomo, and Maya Anderson. Privacy enforcement at a large scale for GDPR compliance. In *Proceedings of the 11th ACM International Systems and Storage Conference, SYSTOR '18*, pages 124–124, New York, NY, USA, 2018. ACM.
- [6] Jody Gilbert. Time is running out on GDPR compliance: Find out if you're affected. <https://www.techrepublic.com/article/time-is-running-out-on-gdpr-compliance-find-out-if-youre-affected/>, 2018. [Online, accessed 12-February-2019].
- [7] Solix. GDPR compliance. <https://www.solix.com/data-management-solutions/compliance/gdpr/>, 2018. [Online, accessed 12-February-2019].
- [8] GOV.UK. Cyber security breaches survey 2018: Preparations for the new Data Protection Act. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018-preparations-for-the-new-data-protection-act>, 2018. [Online, accessed 12-February-2019].

- [9] Johanneke Siljee. Privacy transparency patterns. In *Proceedings of the 20th European Conference on Pattern Languages of Programs*, EuroPLoP '15, pages 52:1–52:11, New York, NY, USA, 2015. ACM.
- [10] Michael Colesky, Julio C. Caiza, José M. Del Álamo, Jaap-Henk Hoepman, and Yod-Samuel Martín. A system of privacy patterns for user control. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, SAC '18, pages 1150–1156, New York, NY, USA, 2018. ACM.
- [11] Sarah Spiekermann. The challenges of privacy by design. *Commun. ACM*, 55(7):38–40, July 2012.
- [12] B.J. Keeton. How to make your website compliant with the GDPR. <https://www.elegantthemes.com/blog/tips-tricks/how-to-make-your-websites-gdpr-compliant>, 2018. [Online, accessed 12-February-2019].
- [13] Website Monitoring Evidon – Digital Governance, Privacy Compliance. Evidon's Trackermap. <https://www.evidon.com>, 2018. [Online, accessed 12-February-2019].
- [14] The Contract Shop. GDPR compliant terms & conditions + privacy policy for your website. <https://thecontractshop.com/products/terms-conditions-privacy-policy-for-your-website?ref=zoelinda>, 2018. [Online, accessed 12-February-2019].
- [15] WPBeginner. The ultimate guide to WordPress and GDPR compliance – everything you need to know. <https://www.wpbeginner.com/beginners-guide/the-ultimate-guide-to-wordpress-and-gdpr-compliance-everything-you-need-to-know/>, 2018. [Online, accessed 12-February-2019].
- [16] Consultancy.uk. Six privacy principles for General Data Protection Regulation compliance. <https://www.consultancy.uk/news/13487/six-privacy-principles-for-general-data-protection-regulation-compliance>, 2017. [Online, accessed 12-February-2019].
- [17] European Commission. Data protection in the EU. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en, 2018. [Online, accessed 12-February-2019].
- [18] Luke Irwin. The GDPR: Understanding the 6 data protection principles. <https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles>, 2018. [Online, accessed 12-February-2019].
- [19] Information Commissioner's Office. Principle (a): Lawfulness, fairness and transparency. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation->

- gdpr/principles/lawfulness-fairness-and-transparency/, 2018. [Online, accessed 12-February-2019].
- [20] Information Commissioner's Office. Principle (b): Purpose limitation. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/>, 2018. [Online, accessed 12-February-2019].
- [21] Information Commissioner's Office. Principle (c): Data minimisation. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>, 2018. [Online, accessed 12-February-2019].
- [22] Information Commissioner's Office. Principle (d): Accuracy. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>, 2018. [Online, accessed 12-February-2019].
- [23] Information Commissioner's Office. Principle (e): Storage limitation. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/>, 2018. [Online, accessed 12-February-2019].
- [24] Monique Magalhaes. The 6 GDPR privacy principles you must know — now. <http://techgenix.com/6-gdpr-privacy-principles/>, 2018. [Online, accessed 12-February-2019].
- [25] Information Commissioner. Data protection by design and by default. <https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/gdpr-in-depth/accountability/data-protection-by-design-and-by-default/>, 2018. [Online, accessed 12-February-2019].
- [26] Webfinance. Privacy policy. <http://www.businessdictionary.com/definition/privacy-policy.html>, 2011. [Online, accessed 12-February-2019].
- [27] A&L Goodbody. The GDPR: A guide for businesses. <https://www.algoodbody.com/media/TheGDPR-AGuideforBusinesses1.pdf>, 2018. [Online, accessed 12-February-2019].
- [28] Alexandr Railean and Delphine Reinhardt. Let there be lite: Design and evaluation of a label for iot transparency enhancement. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, MobileHCI '18, pages 103–110, New York, NY, USA, 2018. ACM.

- [29] Intersoft Consulting. GDPR consent. <https://gdpr-info.eu/issues/consent/>, 2018. [Online, accessed 12-February-2019].
- [30] i SCOOP. Consent under the GDPR: valid, freely given, specific, informed and active consent. <https://www.i-scoop.eu/gdpr/consent-gdpr/>, 2018. [Online, accessed 12-February-2019].
- [31] Emilia. GDPR friendly subscription forms – what mistakes to avoid. <https://www.getanewsletter.com/en/blog/gdpr-friendly-subscription-forms/>, 2018. [Online, accessed 12-February-2019].
- [32] Manuel Grenacher. GDPR, the checklist for compliance. <https://www.forbes.com/sites/forbestechcouncil/2018/06/04/gdpr-the-checklist-for-compliance/#4d29e5945bec>, 2018. [Online, accessed 12-February-2019].
- [33] Kris Jamsa. *.NET Web Services Solutions*. John Wiley & Sons, 2006.
- [34] June Jamrich Parsons and Dan Oja. *New Perspectives on Computer Concepts 2012: Introductory*. Cengage Learning, 2011.
- [35] Laura Vegh. Cookies consent under the GDPR. <https://eugdprcompliant.com/cookies-consent-gdpr/>, 2018. [Online, accessed 12-February-2019].
- [36] Cookiebot. GDPR and cookies. What do I need to know? Is my use of cookies compliant? <https://www.cookiebot.com/en/gdpr-cookies/>, 2018. [Online, accessed 12-February-2019].
- [37] Designmodo. Cookies Policy. <https://designmodo.com/cookies-policy/>, 2018. [Online, accessed 12-February-2019].
- [38] Danny Palmer. What is GDPR? Everything you need to know about the new General Data Protection Regulations. <https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/>, 2018. [Online, accessed 12-February-2019].
- [39] Source Making. Design patterns. https://sourcemaking.com/design_patterns, 2018. [Online, accessed 12-February-2019].
- [40] UI Patterns. UI patterns card deck. <https://shop.ui-patterns.com/product/ui-patterns-card-deck/>, 2018. [Online, accessed 12-February-2019].
- [41] Ola Möller. 81 creativity card decks. <https://methodkit.com/research-method-cards/>, 2016. [Online, accessed 12-February-2019].

- [42] IDEO. Method cards. <https://www.ideo.com/post/method-cards>, 2018. [Online, accessed 12-February-2019].
- [43] Social Innovation Lab kent. SILK method deck. <https://socialinnovation.typepad.com/silk/silk-method-deck.html>, 2018. [Online, accessed 12-February-2019].
- [44] LPK. Overcome the 50 roadblocks to innovation. <https://roadblocks.lpklab.com>, 2017. [Online, accessed 12-February-2019].
- [45] MethodKit. How to use methodkit. <https://methodkit.com/how-to-use/>, 2018. [Online, accessed 12-February-2019].
- [46] Dan Lockton. Design with Intent. <http://designwithintent.co.uk>, 2015. [Online, accessed 12-February-2019].
- [47] Keith Sawyer. The Zig Zag creativity card deck: A brilliant ideation tool. <http://chuckfrey.com/the-zig-zag-creativity-card-deck-review/>, 2015. [Online, accessed 12-February-2019].
- [48] Behavior & Design The Brains. Strategy Cards. <http://www.brainsbehavioranddesign.com/kit.html#reference>, 2018. [Online, accessed 12-February-2019].
- [49] Group Works. The Group Works Card Deck. <https://groupworksdeck.org/deck>, 2018. [Online, accessed 12-February-2019].
- [50] Carolyn Snyder. *Paper prototyping: The fast and easy way to design and refine user interfaces*. Morgan Kaufmann, 2003.
- [51] Todd Zaki Warfel. *Prototyping: a practitioner's guide*. Rosenfeld media, 2009.
- [52] Max Schrems. "Pay or Okay" bei derStandard.at? <https://noyb.eu/derstandard-einwilligung/>, 2018. [Online, accessed 12-February-2019].
- [53] W3C. The W3C Web Accessibility Initiative (WAI). <https://www.w3.org/WAI/>, 2019. [Online, accessed 12-February-2019].
- [54] W3C. Web Content Accessibility Guidelines (WCAG) overview. <https://www.w3.org/WAI/standards-guidelines/wcag/>, 2019. [Online, accessed 12-February-2019].
- [55] Jim Krause. *Color for designers: ninety-five things you need to know when choosing and using colors for layouts and illustrations*. New Riders, 2014.
- [56] John-Paul Ballard. What is an asset library? <https://www.lynda.com/Sketch-tutorials/What-Asset-Library/496908/530324-4.html>, 2016. [Online, accessed 12-February-2019].

- [57] IBM Knowledge Center. Managing the asset library. https://www.ibm.com/support/knowledgecenter/en/SSWU4L/GetStarted/imc_GetStarted/08_Asset_Library.html, 2018. [Online, accessed 12-February-2019].
- [58] Dempsey Chang, Laurence Dooley, and Juhani E Tuovinen. Gestalt theory in visual screen design: a new look at an old subject. In *Proceedings of the Seventh world conference on computers in education conference on Computers in education: Australian topics-Volume 8*, pages 5–12. Australian Computer Society, Inc., 2002.
- [59] VISSCOM. Principle of repetition & pattern. <https://visscom.wordpress.com/2013/04/16/principle-of-repetition-pattern/>, 2013. [Online, accessed 12-February-2019].
- [60] Agnieszka Kitkowska. Should I paint my house pink? Decisions are difficult... extra difficult when we talk privacy! <https://akitkowska.com/2017/11/26/should-i-paint-my-house-pink-decisions-are-difficult-extra-difficult-when-we-talk-privacy/>, 2017. [Online, accessed 12-February-2019].
- [61] Simone Mora, Francesco Gianni, and Monica Divitini. Tiles: a card-based ideation toolkit for the internet of things. In *Proceedings of the 2017 Conference on Designing Interactive Systems*, pages 587–598. ACM, 2017.
- [62] Kasper Hornbæk, Rune Thaarup Høegh, Michael Bach Pedersen, and Jan Stage. Use case evaluation (UCE): A method for early usability evaluation in software development. In *IFIP Conference on Human-Computer Interaction*, pages 578–591. Springer, 2007.
- [63] Joost Ouwerkerk and Alain Abran. An evaluation of the design of use case points (UCP). In *Proceedings of the International Conference on Software Process and Product Measurement MENSURA*, pages 83–97, 2006.
- [64] Antti Salovaara, Antti Oulasvirta, and Giulio Jacucci. Evaluation of prototypes and the problem of possible futures. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2064–2077. ACM, 2017.
- [65] Robert D Atkinson and Daniel Castro. Digital quality of life: Understanding the personal and social benefits of the information technology revolution. 2008.
- [66] Jan Philipp Albrecht. How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, 2:287, 2016.
- [67] Paul Voigt and Axel Von dem Bussche. *The EU General Data Protection Regulation (GDPR)*, volume 18. Springer, 2017.
- [68] Alan Calder. *EU GDPR: a pocket guide*. IT Governance Publishing Ltd, 2018.

- [69] Saul Greenberg. Toolkits and interface creativity. *Multimedia Tools and Applications*, 32(2):139–159, 2007.
- [70] Jenifer Tidwell. *Designing Interfaces*. O’Reilly Media, Inc., 2010.
- [71] Saul Greenberg, Sheelagh Carpendale, Nicolai Marquardt, and Bill Buxton. *Sketching User Experiences: The Workbook*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1st edition, 2011.