Privacy CURE: Consent Comprehension Made Easy

Olha Drozd, Sabrina Kirrane

Privacy CURE: Consent Comprehension Made Easy

Olha Drozd[0000−0001−6551−6567] and Sabrina Kirrane[0000−0002−6955−7718]

Vienna University of Economics and Business, Vienna, Austria
{olha.drozd, sabrina.kirrane}@wu.ac.at

Abstract. Although the General Data Protection Regulation (GDPR) defines several potential legal bases for personal data processing, in many cases data controllers, even when they are located outside the European Union (EU), will need to obtain consent from EU citizens for the processing of their personal data. Unfortunately, existing approaches for obtaining consent, such as pages of text followed by an agreement/disagreement mechanism, are neither specific nor informed. In order to address this challenge, we introduce our Consent reqUest useR intErface (CURE) prototype, which is based on the GDPR requirements and the interpretation of those requirements by the Article 29 Working Party (i.e., the predecessor of the European Data Protection Board). The CURE prototype provides transparency regarding personal data processing, more control via a customization, and, based on the results of our usability evaluation, improves user comprehension with respect to what data subjects actually consent to. Although the CURE prototype is based on the GDPR requirements, it could potentially be used in other jurisdictions also.

Keywords: Consent request · Informed consent · GDPR · Usable privacy.

1 Introduction

In the European Union (EU) the General Data Protection Regulation (GDPR) came into force on May 25, 2018, modernizing the Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Both of these documents, however, suggest obtaining consent for data processing from data subjects. Although the GDPR defines several potential legal bases[1] for the lawful personal data processing[2], for instance for the provision of a contract, in order to fulfill a legal obligation, in the case of vital interest, in the case of public interest, or for reasons of legitimate interest, in many cases data controllers and processors, will need to obtain consent from data subjects for the processing of their personal data[3], for example in order to deliver personalized recommendations or to improve their services. According

[1] GDPR Art. 6(1)(b - f)
[2] For the lawful personal data processing data subject's consent is not required.
[3] GDPR Art. 6(1)(a)

to Art. 4(11)[4] of the GDPR, consent needs to be "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".

The de facto standard for consent requests is still ready-made, set in stone, static descriptions of current and future data processing in the form of privacy policies or terms and conditions. However, studies show that such policies and terms and conditions are rarely read and when they are, they are hard to digest [20]. Although there have been some attempts to give users more control and transparency regarding personal data processing [10,15], the cognitive limitation of data subjects in terms of understanding what exactly they consented to remains an open research challenge [1,6]. Considering that the GDPR in general, and GDPR Art. 4(11) in particular, is quite prescription when it comes to consent, we argue that consent request user interface (UI) designers should pay particular attention to consent requirements specified in the GDPR and the interpretation of said requirements, in the form of guidelines[5], by various expert groups, such as the European Data Protection Board, and its predecessor the Article 29 Working Party [6].

In this paper, we introduce our Consent reqUest useR intErface (CURE) prototype, based on said requirements and guidelines, which elicits greater involvement of data subjects when it comes to granting consent, affords them more control via customization, and provides high transparency with respect to personal data processing. Our evaluation results look very promising, not only in terms of usability, but also in terms of understandability. Our UI could be applied in different contexts, however, in this paper it is developed based on an exemplifying use case scenario, whereby an individual purchasing a new wearable appliance for fitness tracking needs to complete the consent request in order to activate the various features of the device. Also, although the requirements underpinning the design of the CURE prototype are based on the GDPR, the CURE prototype could potentially be used in other jurisdictions.

The remainder of the paper is structured as follows: we start by providing an overview of the state of the art; following on from this we highlight our exemplifying use case scenario, the general requirements and methodology that are used to guide our work; next we describe our CURE prototype and the corresponding usability evaluation; finally, we present our conclusions and describe future work.

[4] Art. 4(11) is complemented by Art. 7 that provides information on conditions for consent.

[5] Article 29 Working Party Guidelines on consent under Regulation 2016/6791 are available at https://bit.ly/2BdQs08.

[6] Article 29 Working Party was an independent European working party that dealt with data protection issues. On 25.05.2018 it was replaced by the European Data Protection Board under the GDPR.

2 Related work

Over the years there have been several papers tackling the problem of consent request design [21,27,28,30] and understandability of consent content [10,12,15,17,20].

As for types and formats of consent requests, Steinsbekk et al. [30] distinguish the following consent models: (i) no consent (i.e., all data usage is prohibited), (ii) specific consent (i.e., consent is tightly coupled with the purpose), (iii) broad consent (i.e., a framework whereby data are categorized according to type), and (iv) blanket consent (i.e.,virtually unlimited (including future) use of the data). Schaub et al. [28] survey the literature on privacy notices and identify four design dimensions of privacy notices, namely timing (i.e., when the notice is shown); channel (i.e., medium that delivers the notice); modality (i.e., how the notice is communicated); and control (i.e., what control options are available). Utz et al. [32] describe common UI properties of consent requests and their influence on people's consent behavior. They found that privacy notices located in the bottom left part of the screen have higher interaction rates. Additionally, the researchers show that user choices can be strongly influenced by the nudging and highlight the need for clear consent requirements to ensure that consent is informed and freely given.

In terms of comprehension of the consent request content, much of the focus to date has been on privacy policy visualization. McDonald et al. [21] assessed three formats of privacy policies: layered policies, conventional human-readable policies, and Privacy Finder privacy report[7]. In contrast to Utz et al. [32], the authors do not recommend regulating privacy policies. The evaluation showed that users disliked all three formats of privacy policies similarly, however, the authors do not provide an explanation with respect to what could have caused such a result. Kumar [17], in turn, analyzed 23 privacy policies putting a particular focus on the lack of clarity. Automatic assessment of the privacy policy completeness is proposed by Costante et al. [10]. Though they group privacy policy content into categories, the text of the privacy policy still remains the same as in a typical privacy policy and, as a result, is incomprehensible for users. The same issue concerns the cookie-watch tool for cookie management, developed by Friedman et al. [12]. Although it was designed to improve users' understanding of cookies, it still uses verbose cookie descriptions similar to the text of classical privacy policies. The consent requests in such a format would not provide for an informed consent. Kelley et al. [15] describe a process for constructing privacy policies based on labels and argue that their approach improves users' performance, however, they fail to visualize the full data processing flow. Therefore, such policies would lack full transparency regarding data processing. Reeder et al. [27] test an expandable grid in the context of setting permissions in the Windows operating system. However, the amount of information presented to a user in such a context is

[7] A Privacy Finder is a search engine service that informs users whether the privacy policies of the displayed search results coincide with users' privacy preferences. It also generates a privacy report for each search result, providing users with the core information from the privacy policy.

much smaller than in the general context of obtaining consent, hence cannot be applied to consent requests. Other literature, related to obtaining consent from the data subjects, analyzes privacy control UIs, such as mobile application (app) permissions [18,35]. When compared to a consent request, app permissions only provide users with an overview of the type of access the app requires, whereas no details are provided about the data processing, which makes permission settings not sufficient for a valid informed consent.

In terms of specific or dynamic consent, Mont et al. [22] propose a dynamic consent, policy enforcement and accountable information sharing platform. However, the focus is primarily on the architecture as opposed to the design of a usable and understandable user interface. Consent, compliance, and transparency systems [16,24,34], tools[8] and dashboards [26,5,2] are a related topic in the privacy literature as well as in industry, however, in this paper we focus primarily on the UI aspects of a consent request. Although consent request design features offered by Railean et al. [25] have some promising results, the authors received inconsistent outcomes concerning the comprehension of their "privacy facts" labels which indicates a need for a reevaluation.

New approaches for obtaining consent, such as Usercentrics' consent request [9] (or any other cookie consent request), try to categorize data and give users customization options, as opposed to all or nothing approach in classical privacy policies. However, they still provide a lot of textual information that causes information overload according to our evaluation results, which are presented later in this paper. According to a Norwegian Consumer Council report[10], Google and Facebook trick users into providing consent for the processing of more information and intentionally make it harder to customize users' consent by employing dark patterns. The report states, that both companies: (i) preselect settings to the least privacy friendly options; (ii) hide / obscure preselected settings; (iii) use confusing wording; and (iv) design complicated paths to make it difficult to manage users' data processing.

Unlike most of the current consent requests, that employ an all or nothing approach or provide pages of incomprehensible information about the data processing, in our CURE prototype we provide users with: (i) transparency with respect to personal data processing, (ii) understandable information about the actual data processing, and (iii) control over the data processing with the help of customization feature.

3 Background and Methodology

Before describing the CURE prototype and its usability evaluation, we provide the necessary background information with respect to the use case, the consent requirements and the methodology used to guide our work.

[8] Compliance tools are offered by various companies, e.g., ShareThis Inc., eccenca GmbH, etc.

[9] Usercentrics' consent request can be viewed at https://usercentrics.com.

[10] Norwegian Consumer Council Report is available at https://bit.ly/2N1TRRC.

3.1 Exemplifying Use Case Scenario

The following exemplifying use case scenario guided the development of the CURE prototype. Sue buys a wearable appliance for fitness tracking from BeFit Inc. In order to use the device's features, she first needs to grant consent for the processing of her personal data. She browses to BeFit's website and is presented with a consent request that describes which data need to be gathered, how they will be processed and shared in order to provide her with fitness-related information. For example, the consent request says that the device records heart rate parameters such as resting heart rate and activity heart rate; these data are stored on the device without sharing them with anyone; and processed to provide Sue with information about her all day heart rate. For the purpose of our research the content for the consent request was derived from our analysis of four smart devices (Fitbit, Apple Watch, Garmin Vivomove, and Garmin ForRunner) and two cloud-based analytics services (Runkeeping and Strava).

3.2 Consent Request UI Requirements

The CURE prototype requirements were derived both from the text of the GDPR and its interpretation by the Article 29 Working Party, that examined how the GDPR might influence data controllers in terms of consent request modifications. According to the Article 29 Working Party Guidelines on consent under Regulation 2016/6791, consent should be: (i) freely given, (i.e., it provides real choice and control for data subjects); (ii) specific, (i.e., it is separate from information about other matters, is tied to a purpose, and provides separate opt-in for each purpose); (iii) informed, (i.e., it includes elements that are crucial to understand processing of personally identifiable information and make a choice); and (iv) unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

3.3 Methodology

The Design Science Research (DSR) [23] methodology was the overarching methodology that guided the design of CURE prototype. DSR starts with the identification of the research problem and the justification of the solution necessity. Then the objectives are specified and the design and development of a research artefact begins. The evaluation of an artefact follows its development and the results of the evaluation are communicated to researchers and other stakeholders. DSR was complemented by Action Research (AR), as defined in [9], to allow for the iterative refinement of the prototype. AR is an iterative approach, that starts with a problem identification and a subsequent solution to it. In the end, the outcomes of the action taken to solve the problem are evaluated. The solution is improved if the evaluation outcomes are not satisfactory.

Given that we wanted to focus more on the why and how aspects of the user interaction, rather than on what, where, or when, an observational method was

Table 1: CURE prototype usability evaluation assignments.

Task #	Text of the task
T1	Give your consent to process your information to have health data on your device.
T2	Give your consent to process your information for your activities to be shown on a map.
T3	Give your consent to enable the fitness adviser.
T4	Give your consent to turn on the back-up of your data.
T5	Withdraw your consent to derive your cardio fitness score.
T6	Withdraw your consent to derive your race time predictions.
T7	Withdraw your consent to back up your data.
T8	Withdraw your consent to all the functionalities.
T9	Have a look at the detailed overview of the required data processing for the functionality "display route on map".

the methodology of choice for our usability testing [19]. The evaluation itself was done in an asynchronous remote way [3] using a think aloud method [8,29,33], where users recorded the video of their screen and the audio of their spoken thoughts. We combined the think aloud method with performance measurement (e.g., completion success rates, time spent on the tasks, errors, etc.) [14] and post-evaluation remote questionnaire[11] [13] containing single choice, multiple choice, rating scale and open-ended questions that provided us with participants' demographic data as well as their impression of the CURE prototype. In order to make our evaluation as realistic as possible (in contrast to usability evaluations performed in lab settings), we developed an online prototype, as it enabled the participants to give their consent from a place of their choosing. Additionally, we ensured ecological validity [7] by: (i) deriving the content for the consent from the popular wearable appliances for fitness tracking; (ii) developing a cross-platform prototype that allowed users to test it on any operating system and browser of their choice; and (iii) testing our prototype with broad segment of the population.

On commencement of the UI evaluation participants were asked to imagine themselves buying BeFit's wearable appliance for fitness tracking, and were presented with BeFit's information pertaining to activation and personal data processing practices. After the participants read this information, they were asked to activate the device, using the BeFit specific CURE prototype. During the usability evaluation, the participants first completed a set of predefined tasks (see Table 1) requiring them to grant and withdraw consent for specific features. After these predefined exercises, they were asked to simply give their own consent, as they would have done if they had bought the BeFit device. The former was used to enable us to assess the effectiveness of the UI, while, the latter was used to assess the users' comprehension in terms of what they had consented to. Additionally, the participants were also asked to visit Usercentrics' website and

[11] Our questionnaire is available at https://bit.ly/2DNOGC3.

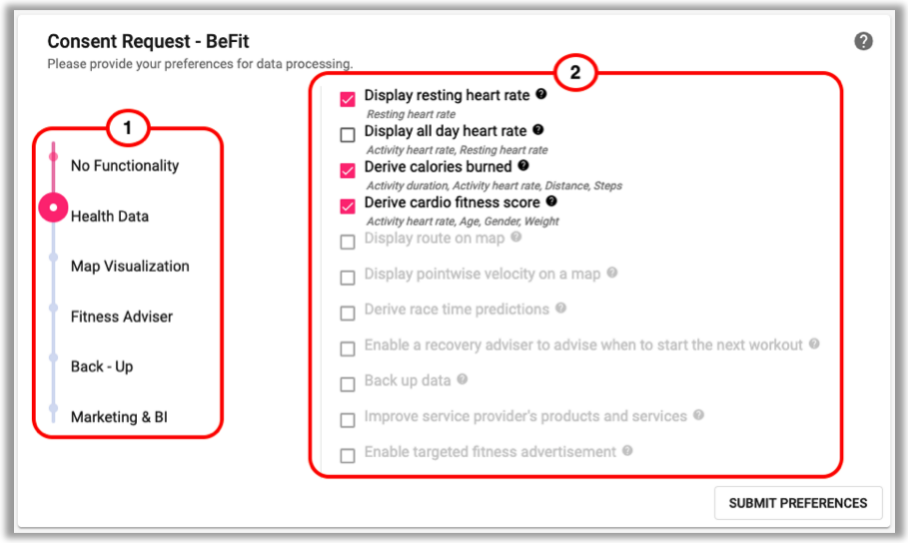

Fig. 1: The CURE prototype: (1) Slider. (2) Consent per purpose.

provide their consent for the personal data processing there, so that they could compare and contrast our prototype and Usercentrics' consent request approach. We selected Usercentrics' consent request for a comparative evaluation in our usability testing because Usercentrics describes itself as the market leader in the area of enterprise consent management platforms and is often referred to by data protection experts.

Usercentrics' consent request is an on-demand pop-up located in the bottom left corner of the screen that provides users with a list of data processors, several clickable icons (history, id, help) and a checkbox near each processor, so users can provide their consent per data processor. When users click on a "help" icon, they are presented with a more detailed consent request. In its detailed consent request, Usercentrics again groups information regarding data processing by data controller and offers users a possibility to give and withdraw their consent for each data controller. The data processing information of each controller is presented in a textual format and is divided into the following categories: processing company, data purposes, technologies used, data collected, legal basis, location of processing, retention period, data recipients, further information / opt-out, and history. The tasks where the participants gave their own consent to BeFit and Usercentrics were assigned in a random order to rule out the influence of the order on participants' evaluations. In the post-evaluation questionnaire the respondents were also asked to compare the CURE prototype with a classical verbose consent request followed by an "agree" button.

4 The CURE Prototype

As the CURE prototype was developed in an iterative manner, in this paper we describe its third version that achieved the best evaluation results and is

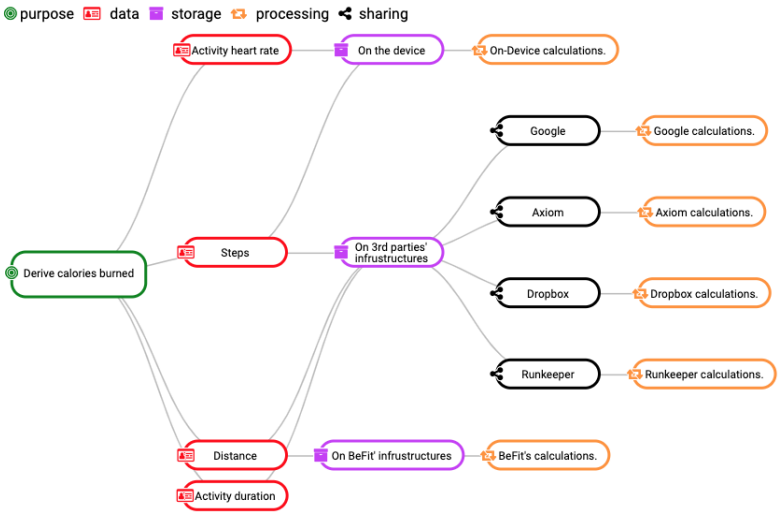

Fig. 2: Example of a detailed overview of the required data processing for the purpose "derive calories burned".

based on the usability evaluation outcomes of the first two versions. The first two prototypes and their evaluation results are presented in [11]. In contrast to the all-or-nothing approach, adopted by current consent requests, in the first version of the prototype we gave users *maximum control* over their data processing by providing them with an option to fully adjust their consent specifically to their needs. The results of the usability evaluation showed that the participants were overwhelmed with too much control over their data processing and there was a clear need to simplify the UI and to reduce the consent options. Based on the insights gained from the first usability evaluation, we developed a *simplified UI* prototype. This second version of the prototype reduced the customization options from full customization to just giving consent to data processing per device's functionality (i.e., purpose) with the possibility to customize third-party data sharing for each functionality. The evaluation of the second prototype indicated some improvement in terms of performance and comprehension. However, the users still complained about the amount of the information they had to digest and the lack of accelerators for giving and withdrawing consent.

Figure 1, which is split into two components: (1) slider, (2) consent per purpose, depicts final BeFit's CURE prototype. The fully functional prototype[12], which was developed for more realistic usability testing, as well as its source code[13] are both available online. From a technology perspective, Angular and D3.js were used for the front-end development and Java and PostgreSQL for the server side.

[12] The prototype is available in two languages: English (http://cr-slider.soft.cafe/en/) and German (http://cr-slider.soft.cafe/de/).

[13] The source code is available at https://bit.ly/2GErFC7.

4.1 The CURE Prototype Description

The CURE prototype offers the following features to the user. *Categorization.* The functionalities offered by the device equate to the purposes for personal data processing. We group these purposes into more general categories that can be browsed by just sliding the pointer up and down (see Figure 1 (1)). In the CURE prototype we order the categories in a way that when the pointer is at the top the users have maximum privacy with minimum device utility, and minimum privacy with maximum utility when the pointer is at the bottom. The ordering was done according to our own preferences. However, we envisage that companies will order those categories based on their device usage statistics. Additionally, the CURE prototype provides a detailed overview of the data processing separately for each purpose. This information is presented in a graphical form (see Figure 2) and is classified according to five categories, namely (i) purpose (i.e., functionalities offered by a service), (ii) data (i.e., what data are collected from the data subject), (iii) storage (i.e., where the data are stored), (iv) processing (i.e., how the personal data are processed) and (v) sharing (i.e., with whom the data are shared). These categories were derived from questions that were routinely asked by our legal colleagues in the context of the SPECIAL[14] project, which aims to assess the lawfulness of personal data processing according to the GDPR. Since the amount of information regarding the data processing is usually large, categorization ensures that the interface is both clean and not overwhelming [31].

Customization. One of the most important aspects of the CURE prototype is the possibility to customize the consent. The CURE prototype allows users to consent to general categories using a slider. By selecting a category, users automatically preselect all purposes that belong to that category. For example, if users want to receive information about their health, they can just slide the pointer to the "Health" category. Four purposes for data processing, that fall under this category (i.e., display resting/all day heart rate; derive calories burned; derive cardio fitness score), are automatically selected. Additionally, the CURE prototype allows more granular customization (see Figure 1 (2)), where the preselected consent can be further adjusted by selecting or deselecting checkboxes corresponding to specific purposes. From a design perspective checkboxes were selected for their simplicity and immediate choice visibility [31].

Understandability. In our CURE prototype we use plain language and short phrases to improve the understandability of the consent request content. Additionally, the CURE prototype provides feedback for every user action. For those users, who would prefer a detailed overview of the data processing, the CURE prototype contains the already mentioned comprehensive overview of the required data processing for each purpose. To reduce the amount of information that is shown immediately to the user, this comprehensive overview becomes available, on demand, upon clicking on a "?" symbol, placed after the description of each purpose. The understandability of this overview is enhanced with a graphical visualization of the data processing. Figure 2 shows an example of such

[14] Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compLiance (SPECIAL) project is described in detail on https://www.specialprivacy.eu/.

an overview graph that provides details of the data processing required for the "derive calories burned" purpose. Additionally, we incorporated color-coding and icons into the graph. Different organizational models (e.g., treemap, sunburst, chord, circle packing, etc.) were applied to represent the detailed overview of the data processing. The graph, however, proved to be the most suitable for our content.

Revocation. According to GDPR Art.7(3), the data subjects should be able to withdraw their consent at any time as easily as they gave it. In the CURE prototype, the consent revocation can be done in two ways, either by sliding up the pointer to withdraw the consent for multiple purposes at once or by deselecting a corresponding checkbox to withdraw the consent for each purpose separately. Although in our use case scenario the user is tasked with granting consent for the first time, the CURE prototype can be used as a control interface for the management of consent, which has already been given.

4.2 Results of the User Evaluations

In order to gain feedback regarding the effectiveness of our interface we conducted a usability evaluation of the CURE prototype. Thirty-five participants (69% - male, 31% - female) took part in our usability evaluation. The users belong to different age groups (51% - 16 to 25 years old, 23% - 26 to 35 years old, 17% - 36 to 45 years old, 6% - 46 to 55 years old, and 3% - 55 years old and over). Almost one third of the participants (31%) graduated from high school. The other 31% have bachelor's degrees. The rest have master's (14%) degrees, no degree with some college (12%), trade, technical or vocational training (6%), doctoral degrees (3%), and some high school education (3%). 63% of the participants come from Austria. Others come from Bosnia, Croatia, the United Kingdom, Italy, the Netherlands, Romania, and Serbia. The participants rated their Internet surfing skills as competent (43%), proficient (26%) and expert (28%). Most of them reported that they usually spend 3 - 6 hours (43%) or 1 - 3 hours (34%) on the Internet per day and preferably use a laptop (57%) or a desktop computer (23%) for the surfing. During the evaluation the participants, first, completed a set of predefined tasks that were outlined in the Methodology section. Then, they were instructed to imagine that they purchased BeFit's wearable appliance for fitness tracking and asked to give their own consent. The participants were also instructed to visit Usercentrics' website and provide their consent there. After finishing their assignments, the participants were asked to fill in a questionnaire about their experience with the CURE prototype.

Video recordings. The analysis of the 35 video recordings provided by our participants showed that the UI was very easy to use and the participants were able to complete the tasks with ease and with almost no errors. We did not observe any major confusion or misunderstanding of the UI. The users immediately noticed the slider and understood the usage of checkboxes for the adjustment of consent. The participants required, on average, 1 second to complete each of the tasks. The average time needed to give their own consent was 20 seconds.

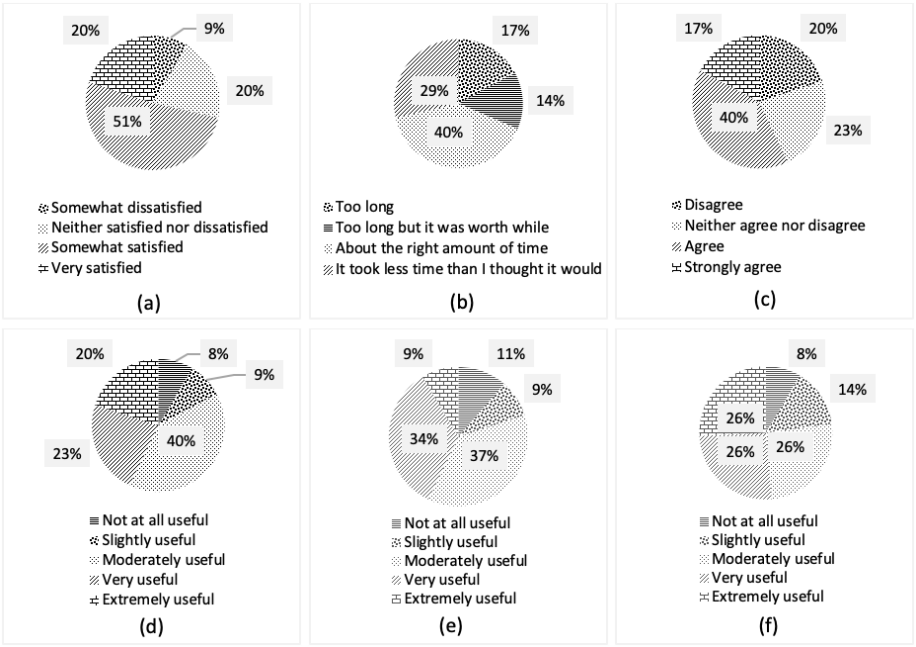

Fig. 3: (a) Overall satisfaction with the consent request. (b) Assessment of the time it took to give/withdraw the consent. (c) Perception of control over the data processing. (d) Usefulness of the detailed overview graph of the data processing. (e) Usefulness of the icons in the detailed overview graph of the data processing. (f) Usefulness of the color-coding in the detailed overview graph of the data processing.

Comprehension testing. We assessed the comprehension of the consent given to BeFit by presenting different possible consent variations in the questionnaire and asking the participants if they consented to that data processing. The answers of each user were compared with the actual consent given. More than a half of the participants answered all the questions correctly, and on average users got 86% of the questions correct.

Overall satisfaction. When we asked users if they were satisfied overall with the consent request, 71% of the participants reported satisfaction (51% - somewhat satisfied, 20% - very satisfied) with the consent request. 20% of the users remained neutral towards the consent request (see Figure 3 (a)). There were no very dissatisfied users and only 9% were somewhat dissatisfied with our UI. The high overall satisfaction can also be reflected in the answers to the question about the recommendation of the websites with the CURE prototype to a friend. 40% said that it was very likely that they would recommend a website with such a consent request to a friend and 29% replied that it was moderately likely. 11% of the respondents would be slightly likely and 3% would be extremely likely to advise a friend to use a website with our consent request. 17% of the participants would not recommend it to a friend. Since only 9% of the users were somewhat dissatisfied with our UI, this was somewhat surprising. Unfortunately, it was not possible to determine why this was the case.

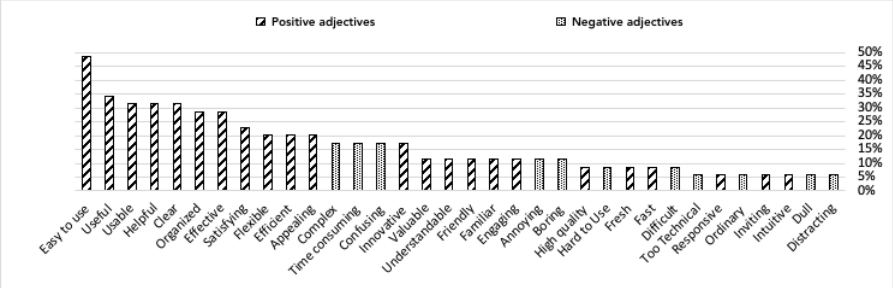

Fig. 4: Adjectives selected by the participants to describe the CURE prototype.

Ease of use. It was very easy for the participants to use the CURE prototype (e.g., the respondents stated that "...it was very clear", "I did not face any major difficulties"). A lot of the users said that the slider on the left side was the easiest part about using the UI (e.g., "the easiest part of this consent form was definitely the slider...", "the slider is extremely easy to navigate"). The respondents also spoke positively about the way the UI is organized (e.g., "the easiest thing was to understand the logic behind how the different settings are divided", "I liked the structure very much").

Adjective description. The users were asked to select adjectives that they would use to describe the UI they were testing. We used the list of adjectives from Microsoft Desirability Toolkit [4], which we adapted to our case. The adjectives that were selected support the results described above. The positive adjectives received most of the participants' votes. The users found this UI easy to use (50%), useful (34%), clear (32%), helpful (32%), usable (32%), effective (29%), organized (29%), satisfying (23%), appealing (20%), efficient (20%), flexible (20%), and innovative (17%). Some of the participants described the prototype with the following negative adjectives: complex (17%), time-consuming (17%), and confusing (17%). Figure 4 provides a detailed overview of the adjectives chosen by the respondents.

Time perception. When asked to provide their impression of the time it took to give or withdraw consent, 40% of the participants answered that it took them about the right amount of time (see Figure 3 (b)). 29% selected it took less time than they thought it would. 14% reported that it took too long, but it was worthwhile. For the rest of the users (17%), it took too long to give or withdraw the consent.

Being in control. We asked the participants, if they felt that they were in control of the processing of their data when they used our consent request. Figure 3 (c) depicts users' answers. More than a half of the participants agreed (40% - agree, 17% - strongly agree) that such a consent request gave them control over the data processing. 23% neither agreed nor disagreed that they were in control. 20% of the participants did not feel that they controlled the processing of their data. There were no users who strongly disagreed.

Overview graph. The graph that provided an overview of the data processing related to each purpose was found to be useful to a greater or lesser extent by

92% of the users (see Figure 3 (d)). 20% found it extremely useful, 23% - very useful, 40% - moderately useful, 9% - slightly useful. Only 8% of the users did not find the graph useful. The participants were asked two questions regarding the design features of the overview graph to find out if they liked the color-coding and the icons used in the graph. 26% of the participants found the color-coding to work extremely well in the graph (see Figure 3 (f)). Another 26% reported the color-coding to be very useful. This feature was rated as moderately useful by 26% of the participants. 14% found it to be slightly useful. The rest (8%) did not find color-coding useful. The icons helped 89% of users (37% - moderately, 34% - very, 9% extremely, 9% slightly) to understand the graph better (see Figure 3 (e)). However, for 11% of participants the icons were not useful.

Prototype vs existing consent requests. The CURE prototype was compared by the participants with two existing consent requests: (i) the classic consent request in the form of privacy policy and an "agree" button at the bottom of the web page, (ii) the consent request developed by Usercentrics. The respondents named four main reasons why they liked the CURE prototype better than traditional consent requests. Unlike classic consent requests, the CURE prototype provides: (i) choice (e.g., "...I have more opportunity to decide what happens with the data"), (ii) an understandable detailed overview of the data processing for each purpose (e.g., "...allows me to get a better image, especially with help of the diagrams for detailed overview, about who and how collects my personal data"), (iii) control over the data processing (e.g., "...helps control the way the data are used"), and (iv) usability (e.g., "it is very easy to use"). Although the consent request from Usercentrics is newly developed, the participants evaluated it similarly to the classic consent. Apart from appreciating customization, the users reported Usercentrics' consent request to be time consuming, overwhelming, not memorable and not user friendly. Only one out of thirty-five participants would choose this UI over the CURE prototype.

Prototype improvement suggestions. As users did not have any major problems while using the CURE prototype, they did not offer any improvements (e.g., "since I, literally, had no difficulties in navigating the UI, I do not have anything to say regarding the improvements", "I like the UI as it is"). One participant suggested to enhance the overview graph with links to third-party websites, wherever their names are mentioned.

5 Conclusion and Future Work

In this paper, we introduced our consent request user interface, which affords users more control over the processing of their personal data, by providing them with more transparency regarding personal data processing and giving them the opportunity to customize their consent. The UI was well received by the participants of our usability evaluation, who performed all tasks quickly, easily and almost without errors. Additionally, most of the adjectives used to describe the UI were very positive and the overall comprehension level of what the participants had consented to was very high. Our UI also performed better

in a comparison task, where users compared it to a classical consent request in the form of privacy policy or terms and conditions, and one of the new solutions on the market offered by Usercentrics. All the materials used in the evaluations are available online, so that other consent UIs can be benchmarked against ours.

So far we have concentrated on the prototype development for laptops and desktop computers, because most of the users still use these devices to surf the Internet [11]. In the future we plan to adapt the CURE prototype for mobile devices and conduct the evaluation of the adapted prototype.

Acknowledgments

This paper is supported by the European Union's Horizon 2020 research and innovation programme under grant 731601. We would like to thank our colleagues from SPECIAL and WU for their legal support and help with the user studies.

References

1. Acquisti, A., Adjerid, I., Brandimarte, L.: Gone in 15 seconds: The limits of privacy transparency and control. IEEE Security & Privacy **11**(4), 72–74 (2013)
2. Angulo, J., Fischer-Hübner, S., Pulls, T., Wästlund, E.: Usable transparency with the data track: a tool for visualizing data disclosures. In: Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems. pp. 1803–1808. ACM (2015)
3. Bastien, J.C.: Usability testing: some current practices and research questions (2010)
4. Benedek, J., Miner, T.: Measuring desirability: New methods for evaluating desirability in a usability lab setting. Proceedings of Usability Professionals Association **2003**(8-12), 57
5. Bier, C., Kühne, K., Beyerer, J.: Privacyinsight: the next generation privacy dashboard. In: Annual Privacy Forum. pp. 135–152. Springer (2016)
6. Borgesius, F.Z.: Informed consent: We can do better to defend privacy. IEEE Security & Privacy **13**(2), 103–107 (2015)
7. Brewer, M.B., Crano, W.D.: Research design and issues of validity. Handbook of research methods in social and personality psychology pp. 3–16 (2000)
8. Charters, E.: The use of think-aloud methods in qualitative research: An introduction to think-aloud methods. Brock Education Journal (2003)
9. Checkland, P., Holwell, S.: Action research. In: Information systems action research, pp. 3–17. Springer (2007)
10. Costante, E., Sun, Y., Petković, M., den Hartog, J.: A machine learning solution to assess privacy policy completeness:(short paper). In: Proceedings of the 2012 ACM workshop on Privacy in the electronic society. pp. 91–96. ACM (2012)
11. Drozd, O., Kirrane, S.: I agree: Customize your personal data processing with the core user interface. In: International Conference on Trust and Privacy in Digital Business. pp. 17–32. Springer (2019)
12. Friedman, B., Howe, D.C., Felten, E.: Informed consent in the mozilla browser: Implementing value-sensitive design. In: Proceedings of the 35th annual hawaii international conference on system sciences. pp. 10–pp. IEEE (2002)

13. Hartson, H.R., Castillo, J.C., Kelso, J., Neale, W.C.: Remote evaluation: the network as an extension of the usability laboratory. In: Proceedings of the SIGCHI. ACM (1996)
14. Ivory, M.Y., Hearst, M.A.: The state of the art in automating usability evaluation of user interfaces. ACM Computing Surveys (CSUR) **33**(4), 470–516 (2001)
15. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: A nutrition label for privacy. In: Proceedings of the 5th Symposium on Usable Privacy and Security. p. 4. ACM (2009)
16. Kirrane, S., Fernández, J.D., Dullaert, W., Milosevic, U., Polleres, A., Bonatti, P.A., Wenning, R., Drozd, O., Raschke, P.: A scalable consent, transparency and compliance architecture. In: European Semantic Web Conference. pp. 131–136. Springer (2018)
17. Kumar, P.: Privacy policies and their lack of clear disclosure regarding the life cycle of user information. In: 2016 AAAI Fall Symposium Series (2016)
18. Liccardi, I., Pato, J., Weitzner, D.J.: Improving mobile app selection through transparency and better permission analysis. Journal of Privacy and Confidentiality **5**(2), 1–55 (2014)
19. MacKenzie, I.S.: User studies and usability evaluations: From research to products. In: Proceedings of the 41st Graphics Interface Conference. pp. 1–8. CIPS (2015)
20. McDonald, A.M., Cranor, L.F.: The cost of reading privacy policies. ISJLP **4** (2008)
21. Mcdonald, A.M., Reeder, R.W., Kelley, P.G., Cranor, L.F.: A comparative study of online privacy policies and formats. In: International Symposium on PETs. Springer (2009)
22. Mont, M.C., Sharma, V., Pearson, S.: Encore: dynamic consent, policy enforcement and accountable information sharing within and across organisations. HP Laboratories. (2012)
23. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A design science research methodology for information systems research. JMIS **24**(3), 45–77 (2007)
24. Piras, L., Al-Obeidallah, M.G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., Bernard, J.B., Fiorani, M., Magkos, E., Sanz, A.C., Pavlidis, M., D'Addario, R., Zorzino, G.G.: Defend architecture: A privacy by design platform for gdpr compliance. In: International Conference on Trust and Privacy in Digital Business. pp. 78–93. Springer (2019)
25. Railean, A., Reinhardt, D.: 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. pp. 103–110. ACM (2018)
26. Raschke, P., Küpper, A., Drozd, O., Kirrane, S.: Designing a gdpr-compliant and usable privacy dashboard. In: Privacy and Identity Management. The Smart Revolution - 12th IFIP International Summer School, Ispra, Italy, September 4-8, 2017. pp. 221–236 (2017)
27. Reeder, R.W., Bauer, L., Cranor, L.F., Reiter, M.K., Bacon, K., How, K., Strong, H.: Expandable grids for visualizing and authoring computer security policies. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 1473–1482. ACM (2008)
28. Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F.: A design space for effective privacy notices. In: Eleventh Symposium On Usable Privacy and Security). pp. 1–17 (2015)
29. Seidman, I.: Interviewing as qualitative research: A guide for researchers in education and the social sciences. Teachers college press (2013)

30. Steinsbekk, K.S., Myskja, B.K., Solberg, B.: Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem? EJHG **21**(9), 897 (2013)
31. Tidwell, J.: Designing interfaces: Patterns for effective interaction design. " O'Reilly Media, Inc." (2010)
32. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (un) informed consent: Studying gdpr consent notices in the field. arXiv preprint arXiv:1909.02638 (2019)
33. Van Someren, M., Barnard, Y., Sandberg, J.: The think aloud method: a practical approach to modelling cognitive processes (1994)
34. Weitzner, D.J., Abelson, H., Berners-Lee, T., Hanson, C., Hendler, J., Kagal, L., McGuinness, D.L., Sussman, G.J., Waterman, K.K.: Transparent accountable data mining: New strategies for privacy protection (2006)
35. Wijesekera, P., Baokar, A., Tsai, L., Reardon, J., Egelman, S., Wagner, D., Beznosov, K.: The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. In: 2017 IEEE Symposium on Security and Privacy (SP). pp. 1077–1093. IEEE (2017)