SPECIAL

Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance

Deliverable D4.5

Transparency dashboard and control panel release final release

Document version: 1.0

SPECIAL DELIVERABLE

Name, title and organisation of the scientific representative of the project's coordinator:

Ms Jessica Michel t: +33 4 92 38 50 89 f: +33 4 92 38 78 22 e: jessica.michel@ercim.eu

GEIE ERCIM, 2004, route des Lucioles, Sophia Antipolis, 06410 Biot, France

Project website address: http://www.specialprivacy.eu/

Project	
Grant Agreement number	731601
Project acronym:	SPECIAL
Project title:	Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance
Funding Scheme:	Research & Innovation Action (RIA)
Date of latest version of DoW against which the assessment will be made:	17/10/2016
Document	
Period covered:	M9-M35
Deliverable number:	D4.5
Deliverable title	Transparency dashboard and control panel release final release
Contractual Date of Delivery:	30-11-2019
Actual Date of Delivery:	30-11-2019
Editor (s):	
Author (s):	Philip Raschke (TUB), Olha Drozd (WU), Bert Bos (W3C)
Reviewer (s):	Rudy Jacob (PROX), Martin Kurze (DT)
Participant(s):	TUB, WU, PROX, DT
Work package no.:	4
Work package title:	User Interaction & Permission
Work package leader:	TUB
Distribution:	PU
Version/Revision:	1.0
Draft/Final:	Final
Total number of pages (including cover):	83

Disclaimer

This document contains a description of the SPECIAL project work and findings.

The authors of this document have taken any available measure in order for its content to be accurate, consistent and lawful. However, neither the project consortium as a whole nor the individual partners that implicitly or explicitly participated in the creation and publication of this document hold any responsibility for actions that might occur as a result of using its content.

This publication has been produced with the assistance of the European Union. The content of this publication is the sole responsibility of the SPECIAL consortium and can in no way be taken to reflect the views of the European Union.

The European Union is established in accordance with the Treaty on European Union (Maastricht). There are currently 28 Member States of the Union. It is based on the European Communities and the Member States cooperation in the fields of Common Foreign and Security Policy and Justice and Home Affairs. The five main institutions of the European Union are the European Parliament, the Council of Ministers, the European Commission, the Court of Justice and the Court of Auditors (http://europa.eu/).

SPECIAL has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731601.

Table of Contents

1 Introduction

The goal of work package four (WP4) is to provide data subjects with a so-called "Transparency dashboard and control panel" (in the following referred to as privacy dashboard) that serves as a control panel for them to access and assess their personal data a controller and possible additional processors, they are concerned with, process for a variety of purposes. Furthermore, data subjects shall be able to rectify or erase inaccurate data, review given consent, or withdraw it. All these actions require interaction and communication with the respective controller. The privacy dashboard is supposed to ease this interaction and communication by defining concrete tasks and actions that can be triggered by the data subject or controller and by structuring information required by the controller to act upon the data subject's requests. This way data privacy concerns can be easier expressed, transmitted, processed, and automated by defining business processes in accordance with existing laws.

New legal requirements imposed by the European Union's General Data Protection Regulation (GDPR)[1], which came into effect in May 2018, emphasize the significance of privacy-enhancing technologies such as privacy dashboards. Article 5 of the GDPR defines multiple personal data processing principles such as *lawfulness* and *fairness*[2], *purpose limitation*[3], *data minimization*[4], *accuracy*[5], *storage limitation*[6], *integrity and confidentiality*[7], and *accountability*[8]. We argue that the transparency principle[9], which is newly introduced in Article 5 of the GDPR, requires innovative approaches to realize this personal data processing principle. Due to its vague expression in the legal text, controllers and processors are left in uncertainty when it comes to required actions that need to be taken to be compliant with this principle. Moreover, it is not possible to provide data subjects with transparency by simply showing them all their personal data the controller processed of them. The vast amount of information and the frequency in which it is processed will overwhelm the majority of data subjects. To provide data subjects with the right information they require to express reasonable data privacy decisions is the key challenge of WP4.

For this reason, activities in WP4 address research and user studies in particular in the fields usable privacy, data visualization, consent management including alternatives for privacy policies and innovative consent interfaces, policy expression of access and usage policies, and the general research fields privacy-enhancing technologies (PETs) and transparency-enhancing tools (TETs).

WP4 started at M9 of the project, i.e. September 2017, and this final version of the deliverable is written and submitted in month 35 of the project, i.e. November 2019. The first version of this

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88 [hereinafter GDPR]

[2] GDPR art. 5(1)(a)

[3] GDPR art. 5(1)(b)

[4] GDPR art. 5(1)(c)

[5] GDPR art. 5(1)(d)

[6] GDPR art. 5(1)(e)

[7] GDPR art. 5(1)(f)

[8] GDPR art. 5(2)(a)

[9] GDPR art. 5(1)(a)

deliverable (**D4.1 Transparency dashboard and control panel release V1**) was submitted in M16 of the project, i.e. April 2018. Version 2 (**D4.3 Transparency dashboard and control panel release V2**) of the deliverable extends the first version and documents our efforts taken since the beginning of WP4 until M25 (i.e. March 2019). With **D4.5 Transparency dashboard and control panel final release** we extend the second version of this report, document our efforts taken between M25 and M35, present and discuss our final results, conclude, and provide and outlook for future work.

2 Goals and scope of the dashboard

This target of this chapter is to extend the introduction by formulating, defining, and narrowing the objectives of the dashboard, which embody the overall scope of WP4. The following subsection gives details on how these objectives are addressed and approached in WP4. Last, the scope of the individual deliverables will be defined.

2.1 Overall scope of WP4

Figure 1 depicts a mind map of the *privacy dashboard* derived from the SPECIAL proposal. Therefore, keywords used in the proposal have been extracted and classified into functional components of the dashboard (colorized green) and general attributes or requirements of the dashboard (depicted in red squares). Based on Figure 1, the objectives of the dashboard are discussed in the following individually.

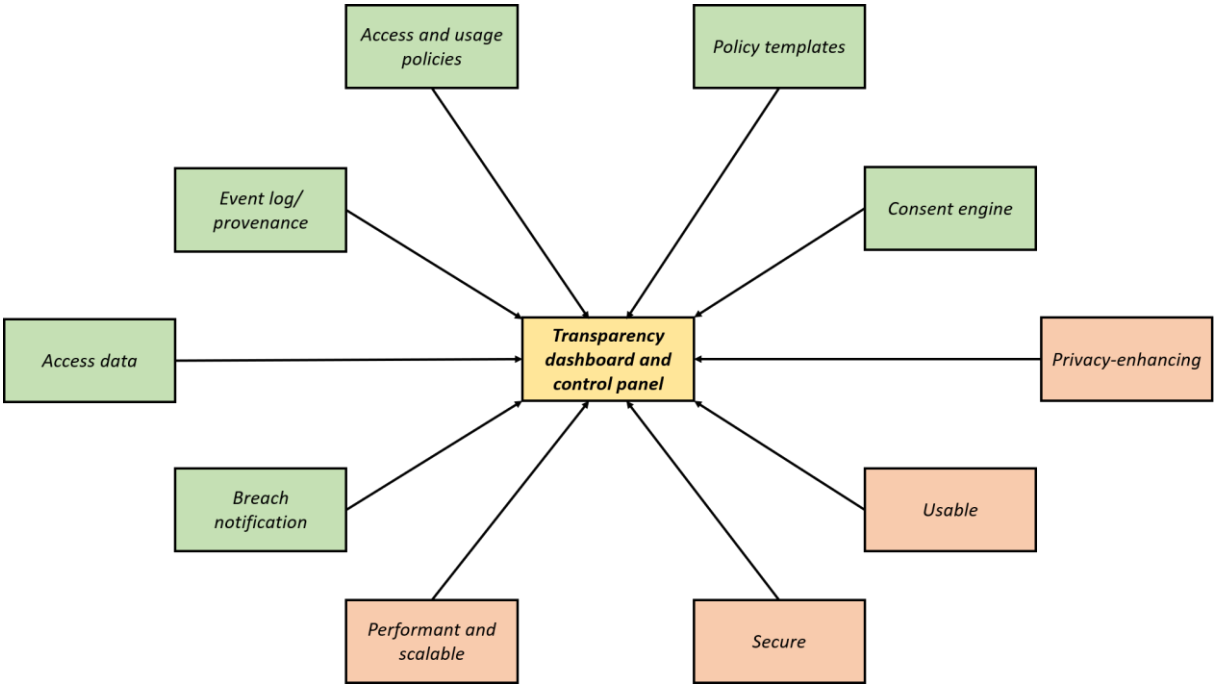

Figure 1: A mind map of the transparency dashboard and control panel derived from the SPECIAL proposal.

2.1.1 Functional components

ACCESS DATA

The privacy dashboard's main purpose is to offer data subjects an interface to access and assess their personal data that is processed by a single or multiple controllers and processors that act on behalf of them within a specific context for one or multiple purposes. We argue that, in order to be compliant with the GDPR, controllers must introduce, develop, or adapt privacy dashboards. Biere et al. (Biere et al. 2016) formulate the same assumption. Data privacy rights like the right to rectification or the right to erasure require data subjects to access and assess their personal data. This includes in particular all personal data not just the information that the data subject deliberately and fully aware disclosed to the controller, but also data obtained from other sources like third parties (such as advertising networks for example), data measured by sensors (in particular Internet of Things devices), information provided by the data subject in publicly available online profiles (Facebook, LinkedIn, and

suchlike), and inferred information gained from Big Data applications. While all this information needs to be made accessible to the data subject, it is also of importance to make it digestible for the data subject. Providing access to the data does not necessarily imply transparency, thus a strong focus on usability needs to be laid.

EVENT LOG/ PROVENANCE

In addition, meta information and provenance data are needed to provide full transparency to the data subject. This includes the purpose and the legal basis of the processing, involved processors, context information like time and the physical location of the processing servers, and which safeguards are applied to protect the data subject's personal data. In deliverable **D1.3 Policy, transparency and compliance guidelines V1** (Section 3.1) a complete list of provided information can be found. The specification of the event log's data format is part of work package two (WP2) and is described in deliverable **D2.3 Transparency Framework V1** and **D2.7 Transparency Framework V2** in detail. The event log's visualization and the identification and presentation of the relevant and necessary information are major challenges addressed in WP4.

ACCESS AND USAGE POLICIES

The expression of access and usage policies by data subjects is a further functionality the privacy dashboard can offer. The underlying policy language SPECIAL introduced in WP2 (see deliverables **D2.1 Policy Language V1** and **D2.5 Policy Language V2**) shall be used for these policies. Legal requirements of the GDPR shall be expressed and formulated with it. This way, SPECIAL aims to enable automated compliance checking with the GDPR. Violations of the GDPR could be prevented in real-time during the processing of personal data. WP4 will offer data subjects an interface to express policies in various forms. For example, a withdrawal of consent for a specific purpose will be reflected with the policy language, so the data subject's withdrawal can be applied (almost) immediately. The same applies for the right to rectification and erasure. WP4 will avoid complex interfaces with many options, so data subject's will not be required to understand the policy language at all, while still using it.

POLICY TEMPLATES

To reduce complexity, policy templates are offered to data subjects. Research (Liu et al. 2016) shows that users can benefit from so-called privacy recommendations in order to enhance their data privacy. The definition of those privacy recommendations depends heavily on the context of the controller, the purpose of the processing, and the data subject's privacy preferences. Thus, the definition of reasonable policy templates is a challenge of WP4.

CONSENT ENGINE

The consent engine is another core component of SPECIAL. It is supposed to allow data subjects to review consent that was previously given, to give informed consent for additional purposes offered by the controller, and to withdraw consent if necessary. WP4 pursues two main goals: (i) designing and implementing consent interfaces that make consent actually (and measurably) informed, (ii) and furthermore, find mechanisms to prevent data subjects being "scared away" by consent requests, for example by informing about the risks and highlighting the benefits of the data disclosure.

BREACH NOTIFICATION

The breach notification is a legal requirement of the GDPR obliging controllers to properly inform data subject's in case of a data breach. Its significance is emphasized by recent data breach incidents like

the Equifax case[10] or the Cambridge Analytica and Facebook scandal[11]. As stated in the introduction, the dashboard's intention is to ease and structure interaction and communication between data subject and controller. In case of a data breach, data subjects can be provided with the most relevant and urgent information and recommendations to react upon data breaches. Controllers might benefit from a standardized, uniform, and automated mechanism enabling them to be compliant with the GDPR. WP4 aims to identify the relevant information data subjects need and how this can be presented in a usable and user-friendly way.

2.1.2 General requirements

PERFORMANT AND SCALABLE

The dashboard must be performant and scalable, this means, it must be capable of handling a vast amount of data, while keeping response times within a reasonable time range. To achieve this, stress tests with unrealistic amounts of data could be conducted. Additionally, mechanisms will be implemented that limit the amount of data displayed. This also contributes to the usability of the dashboard. An asynchronous execution environment enables the application of techniques like lazy-loading to optimize response times on a fine-grained level.

SECURE

The dashboard must be secure since it is used to access sensitive personal data. The security risk involved by introducing the privacy dashboard (as an additional mean to access personal data) must be limited to an absolute minimum. The highest degree of security can be achieved by deploying the dashboard within the controller's domain, this way, the data subject's personal data remains in its entirety within the controller's infrastructure. Only small chunks that the data subject wants to review are transmitted to his or her local machine. For this transmission state-of-the-art encryption techniques are used that offer the highest possible security. Data retrieved by data subjects will be deleted after every session or encryption at rest[12] is applied to secure the data on the data subject's machine from access by possible malicious software.

PRIVACY-ENHANCING

It must be privacy-enhancing to an extent that the introduction of a new security risk is justifiable. Data subjects must be able to use it to fulfil tasks that actually enhance their data privacy. These tasks do not only have to be fully implemented, but also the definition of these tasks is crucial. What tasks within the context of their data privacy do data subjects expect and need in order to make decisions that positively affect their data privacy?

USABLE

It must be usable by a variety of user groups and types in order to serve the purpose as a transparency-enhancing tool and privacy-enhancing technology. As already stated above, providing transparency is not trivial. Transparency is enabled by granting access to the data, but still requires a usable and user-

[10] Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed - Bloomberg. https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed, last accessed: 04/16/2018.

[11] Facebook and Cambridge Analytica face class action lawsuit - The Guardian. https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit, last accessed: 04/16/2018.

[12] Encryption at Rest | Google Cloud. https://cloud.google.com/security/encryption-at-rest/, last accessed: 04/26/2018.

friendly presentation so data subjects can interpret and comprehend the impact of the presented information on their data privacy.

2.2 Scope of D4.1, D4.3, and D4.5

To narrow the scope of this deliverable, the description of **D4.1**, **D4.3**, and **D4.5** in the proposal is used, besides the above given explanation of WP4. The deliverables are described in the proposal as follows:

"*This release will include policy and event data visualisation (T4.1) and system interaction (T4.2).*"

- Description of D4.1 in the proposal

"This release includes improvements to the policy and event data visualisation (T4.1) and system interaction (T4.2) and new visualisations to support the transparency and compliance functionality (T4.1 & T4.2)."

- Description of D4.3 in the proposal

"The final release will incorporate all feedback from the inhouse robustness testing (T4.4), pilot evaluations (T5.1, T5.2), and hacking challenges (T5.3)."

- Description of D4.5 in the proposal

It might be helpful to cite the descriptions of the above-mentioned tasks: **T4.1 Transparency dashboard and control panel, T4.2 Consent engine and feedback mechanism**, and **T4.4 Front end usability testing.**

"An interactive dashboard will provide end users with a digestible log of what happened with the data based on the provenance/event data. In the context of our use cases, the dashboard will be specifically tailored to cater for these Big Data traits. The tool will also enable users to verify that data processors and data controllers are complying with both access and usage policies and with the data protection legislation. Given the volume of data involved, the dashboard will be highly intuitive and flexible, making it easy for the user to pull data based on different contexts. Particularly, the dashboard will allow for checking policy templates in terms of legal requirements (cf. T2.2) but also other easy to understand and re-use "canned" policies in the form of policy templates, developing a kind of "Creative Commons" scheme for end-user policies."

- Description of T4.1 in the proposal

"One of the challenges faced by our use case partners is the fact that much of the data they currently possess can't be used because they do not have the consent to do so. The consent engine feedback mechanism, which will be embedded into the dashboard, will provide the data subject with the ability to highlight data that is inaccurate and to specify new or update existing access/usage policies."

- Description of T4.2 in the proposal

"This task will be dedicated to testing the robustness of the transparency dashboard. The objective of the task is threefold: (i) to stress test the individual components and the dashboard both in terms of performance and scalability; (ii) to validate the usability of the dashboard; and (iii) as per T3.6, to expose the front end to open penetration/hacking challenges in WP5."

- Description of T4.4 in the proposal

The tasks T3.6, T5.1, T5.2, and T5.3 will not be addressed in this deliverable as they are addressed in the following deliverables of the corresponding work packages. See:

- **D3.5 Scalability and Robustness testing report V2** for **T3.6**
- **D3.6 final release** for **T3.6**, **T5.1**, **T5.2**, and **T5.3**

3 Concepts & design decisions

This chapter presents and discusses theoretical concepts for the privacy dashboard and the consent interfaces with the aim to make the designs and different approaches more comprehensible.

3.1 Concepts for the privacy dashboard

As stated above, the visualization of data is a major challenge for the design of the dashboard and a central concern of WP4. The main question is, whether a uniform design for a user interface for all kinds of controllers and data subjects is realistic or not. An alternative would be to build a specific privacy dashboard for every controller and for every user group or type. So, in a first step it is reasonable to identify factors that the appearance of the privacy dashboard depends on. See Figure 2 for an overview.

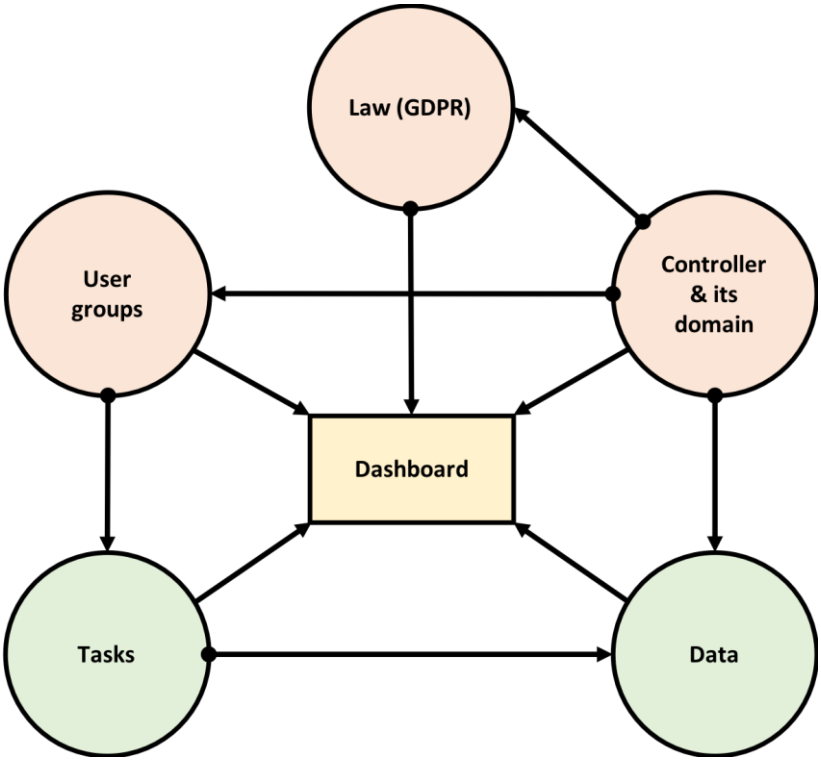

Figure 2: Identified factors that the privacy dashboard's appearance depends on including principle requirements like usability, legal, or business requirements.

In general, the appearance of the privacy dashboard depends heavily on the controller and its domain. Most controllers have a dedicated branding that customers expect to see whenever they interact with the controller. The so-called corporate design is a central building block of the corporate identity, that helps users identifying and verifying the controller's *"identity"* in application scenarios in which no real persons are present (like the Web). The branding is an important requirement that should be taken into consideration when developing the prototypes because it massively influences the appearance of the privacy dashboard.

Legal requirements are derived from the legislation, which to some extent depends on the domain of the controller, since different business domains are subject to different regulations. However, WP4 only considers legal requirements from the GDPR.

Data subjects influence the privacy dashboard's design, since their experience with computers and the Internet is a key factor for the usability of the privacy dashboard. In addition, data subjects vary in terms of age, education, and attitudes (towards privacy in particular), thus their priorities of relevance of information provided by the tool heavily differs. Furthermore, the user groups and types partially depend on the controller and its domain. Considering that Google, for example, concerns potentially all kinds of users including minors, whereas controllers like Tinder are only used by data subjects of legal age. These two user groups do not only differ in age but also in multiple other characteristics.

The tasks that the privacy dashboard is intended to fulfil is another key factor that its appearance depends on. The tasks and how they are executed determine whether a component like a button is needed or in which order components have to be aligned. These tasks also depend on the addressed user groups, since different users may execute different tasks more often than others or execute some tasks not at all, while others on a more frequent basis.

The personal data in question massively influences the appearance of the privacy dashboard. Its subject, context, and domain determine what is displayed and how. What kinds of data categories are displayed also depends on the controller and its domain. The tasks and how they are executed mainly influence the way the data is displayed. For example, if data subjects just want to review location data the address in plain text may be sufficient, whereas the rectification of a location information may be easier for data subjects to realize on an interactive map with a marker.

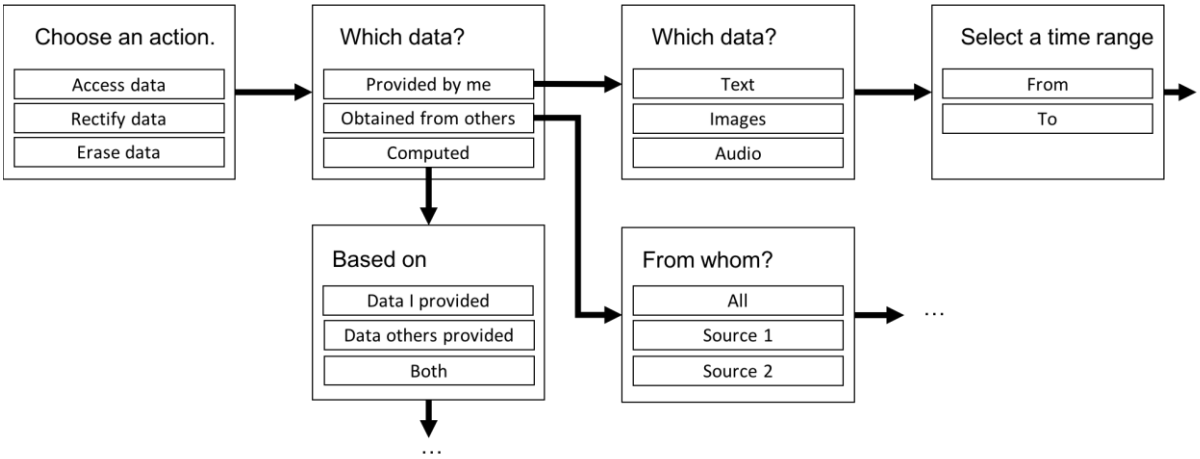

Figure 3: A wizard-like design that guides data subjects through a series of questions leading them to the desired information or action.

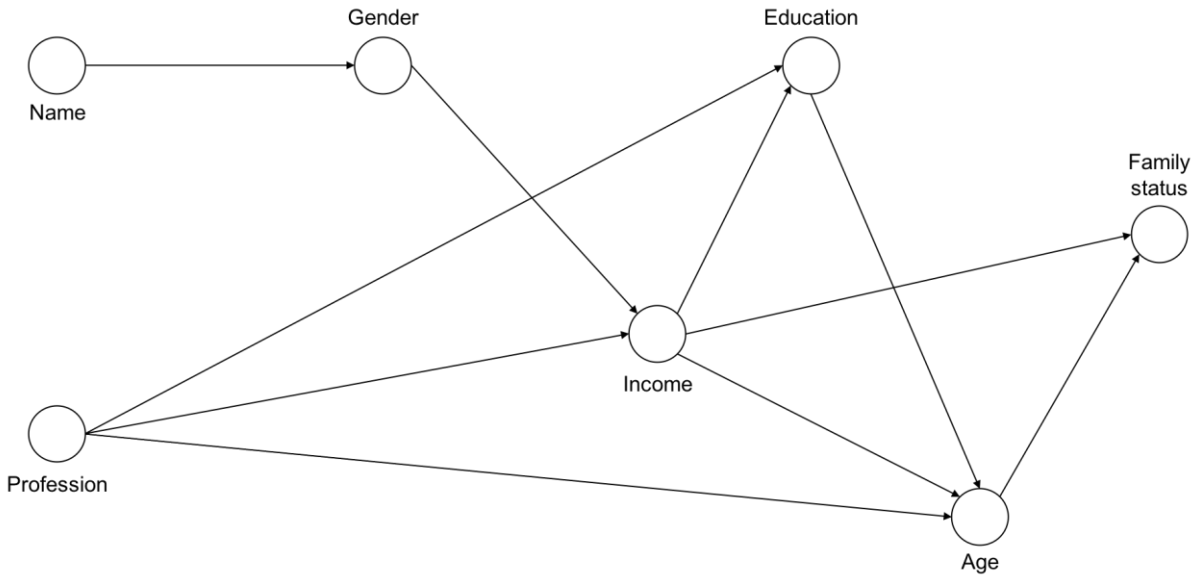

Figure 4: A graph visualizing what information was processed and combined and what information has been derived from that combination.

The identified factors shall help to classify different design approaches. We designed examples for task-centric design approaches (see an example in Figure 3) that put the focus on the tasks data subjects want to fulfil and data-centric design approaches (like depicted in Figure 4) that lay focus on the data itself and emphasize meta information within the context of the processing. User-centric design approaches analogously address the data subject's needs, while controller-centric design approaches are very controller-specific designs that address particular privacy matters of a controller and its data subjects. Controller-centric designs could be realized within existing user interfaces of the data controller's service, without introducing a new and dedicated component for privacy matters.

3.2 Consent interfaces

SPECIAL aims to design and implement new and innovative consent interfaces that enable data subjects to give actual informed consent, while at the same time strengthening their confidence in data disclosure and information sharing with controllers and processors. This appears to be a contradiction intuitively. User studies (Lai et al. 2006) confirm that users, when asked, tend to disagree with data disclosure for purposes like tracking or profiling. However, studies addressing the extensively researched privacy calculus theory (Dinev and Hart 2006) suggest that data subjects are willing to share their information when offered something in return.

Our goal is to better inform users about what they are agreeing to, while simultaneously providing them with more options to choose from to express a consent statement that is acceptable for them and to a certain extent represents their privacy preferences. On the other hand, we want to design consent interfaces that controllers would use in practice. Therefore, the design of these consent interfaces should not lead to users blindly disagreeing.

During the project, we identified four main approaches to improve the process of obtaining consent: (i) broad consent with reduced complexity, (ii) privacy plans, and (iii) customized consent, and (iv) dynamic consent, which will be discussed in the following individually.

3.2.1 Approach: Broad consent with reduced complexity

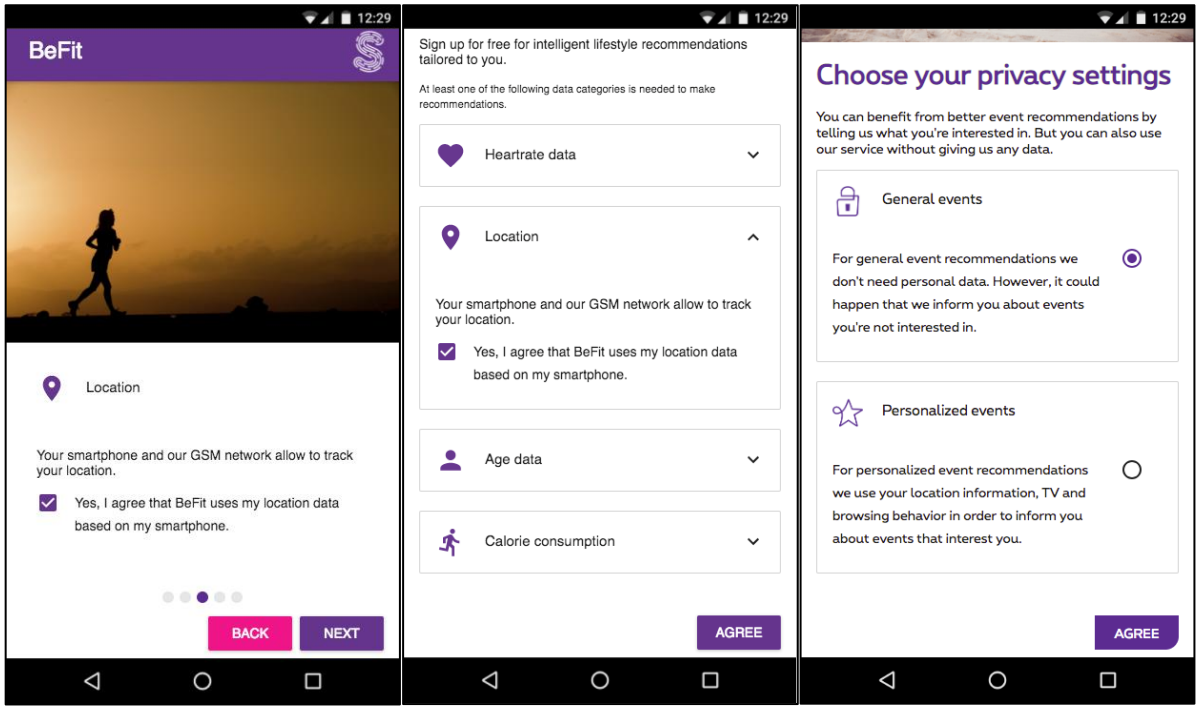

Figure 5: Examples for broad consent with reduced complexity

Today's main problem with consent is not the required user interaction but what this interaction supposedly represents, namely that the user read, understood, and entirely agrees with the privacy policy of the controller for a particular service (or multiple services) at the moment consent is given and valid for all subsequent scenarios in which the user's personal data is processed in any given context the user may be at that moment.

It appears obvious that such a statement cannot be made by simply ticking a checkbox right before the service was ever used and often without any background knowledge of the technology or even the controller. Yet, this is today's modus operandi and users developed a habit to blindly agree with whatever they are supposed to agree with in order to use the service. It could be argued that consent obtained from interfaces that force users to read an excessive amount of text, to entirely agree with its content, and without any means that help users to understand its content, is not legally valid, since a vast number of studies show that users do not read privacy policies. Thus, consent obtained through such interfaces is not informed. It can be further argued that this consent is also not freely given, since users are left with no choice other than to agree and use the service or disagree and do not use the service. There are many scenarios in which users are pressured into using a service and agreeing with the personal data processing implied by it, for example services, which are employed in working environments.

Figure 5 shows alternative approaches to conventional text walls, namely interactive UI elements that are supposed to explain the user: (i) which data is processed, (ii) for which purposes, (iii) stored where and for how long, (iv) and with whom it might be shared. In addition to the interactivity, users are offered more options to express their preferences, i.e. users are given the choice to agree or disagree with certain personal data processing practices (for example which data category they want to share with the controller and which not). This unavoidably requires controllers (service providers) to adhere

to their users' choices and to forward these choices onto all levels of their software stack. This challenge is addressed by the SPECIAL policy language and the compliance checker.

3.2.2 Approach: Policy templates or privacy plans

Purposes of processing personal information can be categorized into two categories: (i) user-beneficial and (ii) controller-beneficial.

The first category consists of personal data processing for purposes that data subjects can benefit from. Any kind of service (for which processing of personal data is required), which is perceived as added-value by the data subject, falls into this category. Examples for this category are: messaging applications, navigation services, location sharing, social networks, and suchlike.

The second category contains purposes that primarily serve the data controller such as profiling for targeted advertising, tracking to improve profiling techniques, or requesting additional external data sources for information of the data subject. Consenting to one of the above-listed purposes does not imply a direct benefit for the data subject. Thus, users tend to not consent to those kinds of personal data processing practices unless they get something tangible in return.

Giving consent to the personal data processing practices of a particular service of a data controller is usually realized by ticking a checkbox labeled with a text that is somewhat similar to *"I've read and agree to the privacy policy"*. Ticking the checkbox is supposed to imply that the data subject has read, understood, and entirely agrees with the privacy policy of the controller. The privacy policy itself contains relevant information about the types of data processed, for what purposes it is processed, and with whom it is shared. The GDPR binds given consent to a specific purpose, thus emphasizing the significance of the purpose. This design approach, presented in Figure 6, addresses the significance of the purpose.

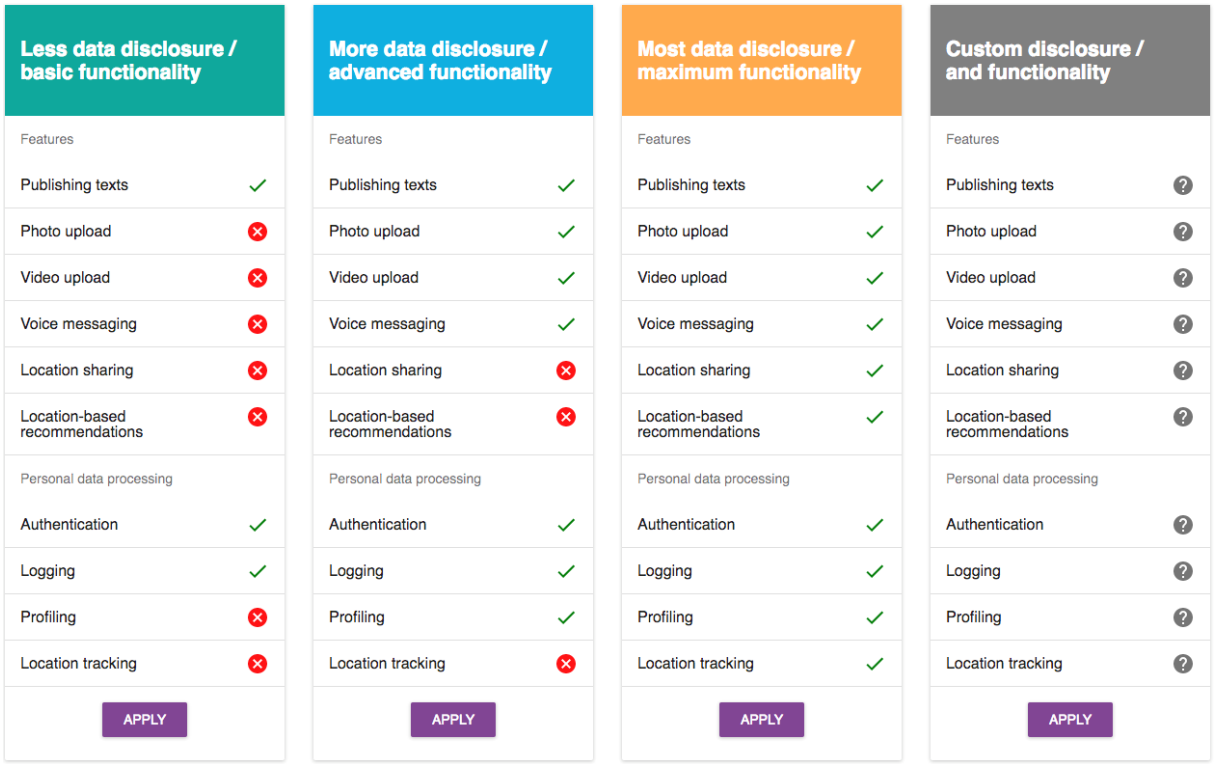

Figure 6: Data privacy plans to easily and quickly choose a privacy setting that reflects the privacy preferences of the data subject.

Figure 6 shows three data privacy plans and a forth option to customize a plan on a finer-grained level. The three plans are in this case: ***less data disclosure/ basic functionality***, ***more data disclosure/ advanced functionality***, and ***most data disclosure/ maximum functionality***. These plans are supposed to be predefined by the data controller who is aware of technical requirements that need to be considered at this point but also is given the chance here to formulate acceptable compromises. For example, the controller cannot offer the data subject location-based recommendations without processing the physical location of the data subject. Or the controller is only willing to provide the data subject with user-beneficial features (here photo and video upload and voice messaging) only if being allowed to profile the data subject.

These privacy plans are supposed to be easy to understand by the users and should represent a clear and simple statement: "This is what you get, if you give us this". Users can safely choose the most privacy-preserving option and later change their mind when they gained more trust towards the service or its provider. This approach however, has some challenges from a legal point of view. First, it's lacking information that are required to be disclosed in a privacy policy. This information must be incorporated without destroying the readability of the individual plans. Second, users could be easily nudged into tolerating more data disclosure for the sake of a single feature they want to use. Even worse, this feature could be a core functionality of the service. It is debatable, whether consent obtained from such an interface is "freely" given from a legal point of view or not.

3.2.3 Approach: Customized consent

If the data subject has chosen to configure a customized data privacy plan, he or she could be presented the consent interface depicted in Figure 7. The idea is that data subject and controller enter

a negotiation process, which results in a consent statement of the data subject, which is acceptable by both parties.

Consenting to controller-beneficial purposes could "earn" the data subject points that can be "spent" to acquire user-beneficial service features. The values are supposed to be predefined by the controller. This way, more control can be offered to the data subject but limited by the individual values for the purposes to implicitly address the controller's interests.

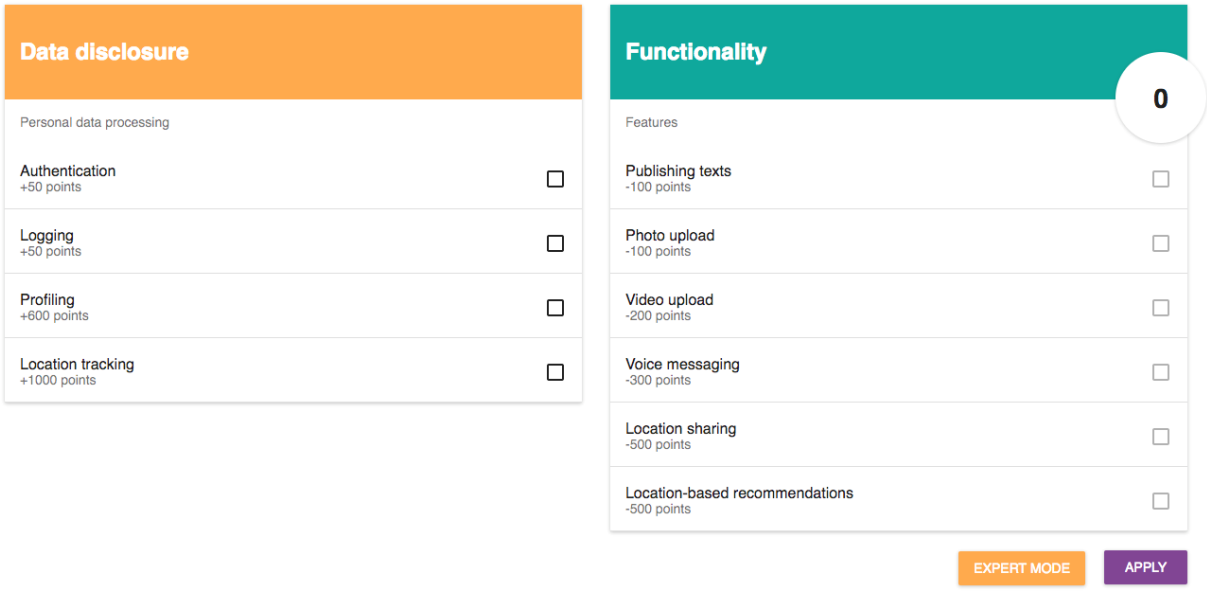

Figure 7: Consenting to purposes (that the controller benefits from) allows data subjects to "get" features they desire.

This prototype does not meet the legal requirements and would need to be extended to meet legal requirements of the GDPR. However, it is conceivable that this design encourages more data disclosure (with reference to one of the goals of WP4). Figure 8 shows a configuration with "unspent" points that the data subject might consider using (by consenting to ***Photo upload*** for example). This design approach gives personal data a concrete counter value. However, it would have to be carefully evaluated whether data subjects perceive this interface and the interaction with it as giving consent. Reviewing the situation in Figure 8 again, it is questionable whether all data subjects understand that they implicitly allowed the data controller to obtain and process their physical location by "acquiring the purpose ***Location sharing*** (despite not consenting to the purpose ***Location tracking***).

This is a very experimental approach with open expectations for results. However, it seems very promising and worthwhile pursuing to investigate this approach. The controller's interests to get explicit and informed consent for privacy-critical purposes like profiling and location tracking are considered and addressed in this design. On the other hand, data subjects have actual control on a finer-grained level. The current modus operandi is *"all-or-nothing",* i.e. data subjects either must agree with the privacy policy and use the service or disagree with the privacy policy and not use the service at all, although they might agree with the majority of personal data processing practices of the data controller (Steinfeld 2016). It is furthermore imaginable, that this approach leads to more informed consent since data subjects will aim to maximize what they can get for their "earned" points, thus being aware what they consented to and what not.

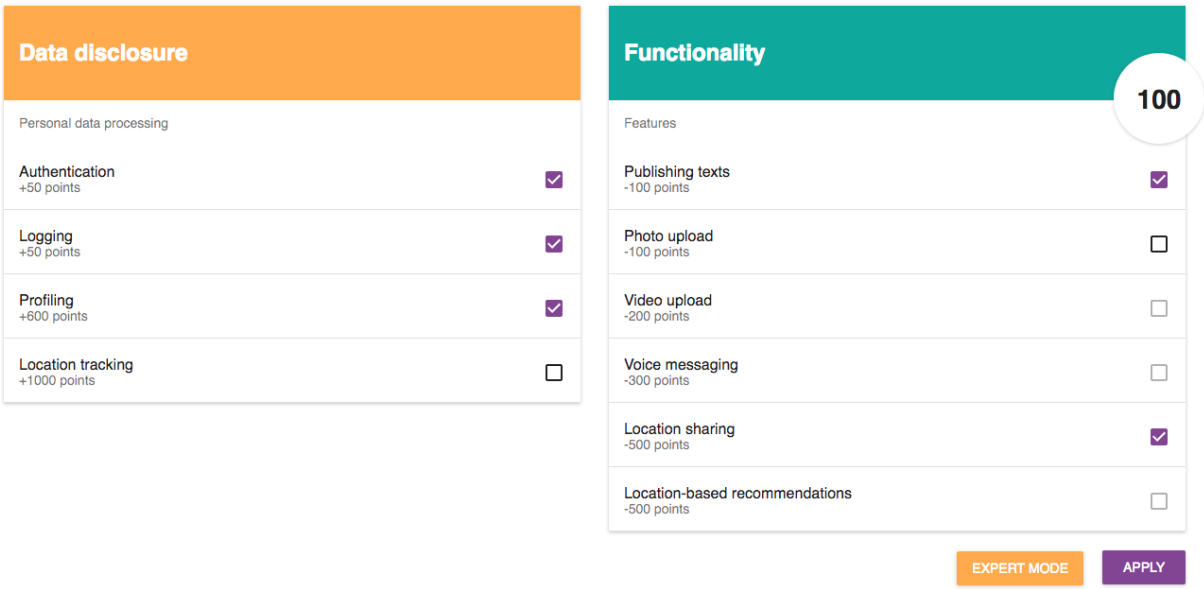

Figure 8: A custom configuration allowing data subjects to consent to the processing of their physical location without allowing the controller to track their location or give location-based recommendations.

3.2.4 Dynamic consent

One goal of SPECIAL is to rethink and redesign giving consent to personal data processing entirely. In Section 3.2, we described concepts for innovative consent interfaces that keep the general approach of asking for consent during the service subscription. This approach has many disadvantages, which lead to users giving uninformed consent. Besides the sheer amount of text that privacy policies consist of, the contemporary irrelevance of most of its content hinder users from carefully reading through the privacy statement. Moreover, even if doubts arise from reading the privacy policy, there is no mean to express, communicate, or negotiate them with the controller.

Privacy policies cover all data processing scenarios, however, not all scenarios are equally relevant to all users. Often it is also dependent on the user's usage of the service. A user, for instance, might not use a certain feature of a service at all. Therefore, one might argue that it is more reasonable to ask for consent when the processing of personal data becomes necessary in order to fulfil the user's requests. Similar to how the mobile operating systems iOS and Android ask users for permission to access certain resources of their smartphone, when the user is about to use a certain feature that makes access to a certain resource necessary.

We introduce our concept of dynamic consent in SPECIAL. See Figure 9[13], for an exemplary application of dynamic consent in an event recommender use case. We identified three phases around the concept of dynamic consent: *notice*, *transparency*, and *control*. Dynamic-consent-enabled services need to communicate this novel approach to their users during the subscription for the service. Otherwise, the constant sending of consent requests would collide with the user's expectations. Therefore, the first phase should focus on giving notice.

[13] Access online via http://dashboard.specialprivacy.eu/Storyboard.png for full size.

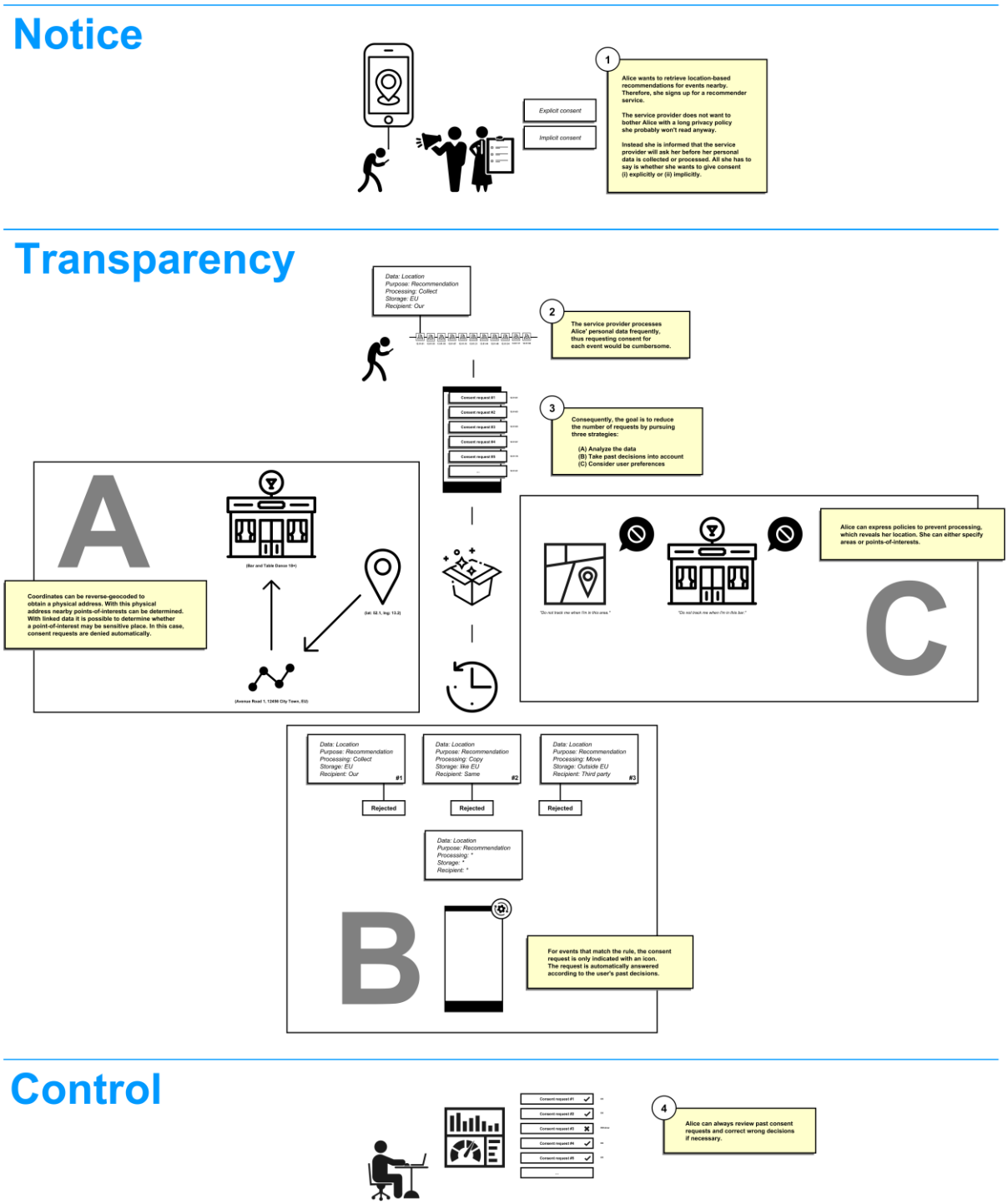

Figure 9: Storyboard for the concept of dynamic consent regarding the user interface

The main phase is called transparency, since the user should be aware (or at least able to be aware) of any data processing during that phase. Despite the user benefitting from enhanced transparency, we found this phase as a challenge for the user. We assume personal data processing to occur often and in a high frequency. Thus, consent requests would be sent to the user at the same rate. Likely, users are not willing to undergo such cumbersome process only to protect their privacy. For this reason, we designed strategies to massively reduce the number of consent requests to a minimum.

The main strategy is assuming consent is given, when the user does not respond to a consent request. This is not really conforming with the privacy-by-default paradigm but does not differ too much from today's reality of personal data processing. However, our approach only behaves in the described way, if the user is in a privacy-sensitive context (e.g. the user is in a table dance bar). This requires the system to detect such a privacy-sensitive context. To achieve this, linked data and semantic web technologies are used. When the user is in such a situation, all consent requests that are sent to the user during that time are rejected by default. Additionally, users are able to define certain situations (in our case areas or locations) by themselves in which consent requests are rejected by default.

Another strategy is to learn from past user decisions. The system can remember user decisions and with the help of statistical analysis determine certain combinations, which always led to a certain decision. For example, could a user always reject consent requests that involve location data stored outside of the EU. Or users consent to almost anything that involve a specific purpose. For such occasions, the consent request could be hidden and only indicated with an icon. This way the user would be able to see that personal data is currently processed, but, if concerned with other things, not be bothered with it.

Apparently, both approaches hold potential for errors. Therefore, the user must be able to make corrections when necessary. For this reason, we introduce the phase control. There needs to be a user interface the user can address privacy concerns to. Here, the user must be able to review all consent requests and their decisions (whether there were done by the user or the system). Withdrawing consent must be fast and easy, since the user might want to make multiple corrections.

4 Privacy Dashboard

This chapter presents the different states of the privacy dashboard developed during the last 27 months since the begin of WP4 in month 9. The prototype has been developed as a Web application realized with Hypertext Markup Language (HTML), Cascading Style Sheets (CSS), and JavaScript using the JavaScript framework *React*[14]. To adapt state-of-the-art design principles for such kind of applications and to ease the process of styling, *Google's Material Design*[15] guidelines were followed. Therefore, the React library *material-ui* [16] has been used. In the following screenshots and corresponding descriptions will be given to describe the prototype textually. All versions of the privacy dashboard (source code and a demonstration) are published on GitHub.

4.1 Privacy Dashboard V1

This section presents the first version of the privacy dashboard as of **D4.1 Transparency dashboard and control panel release V1**, which was submitted in month 16 (April 2018). It can be accessed via https://specialprivacy.github.io/D4.1-Privacy-Dashboard-DEMO/ and the source code is available at https://github.com/specialprivacy/D4.1-Privacy-Dashboard.

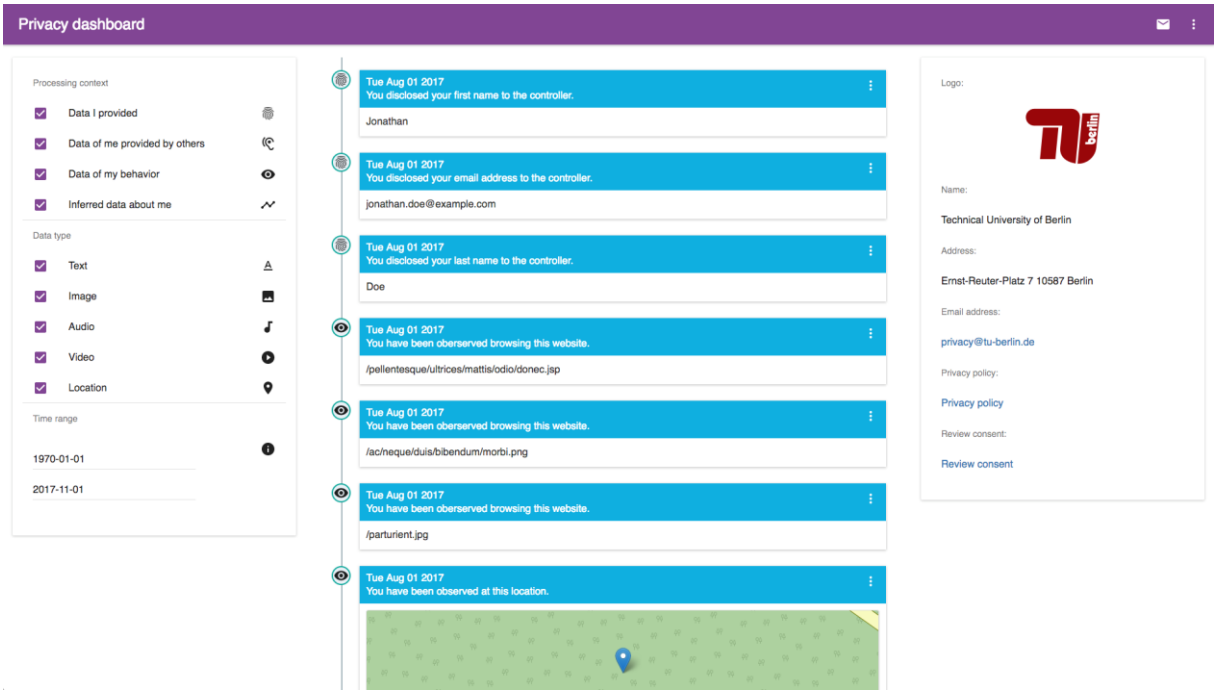

Figure 10: The previous version of the privacy dashboard structured into three-columns.

As it can be seen in Figure 10, we have decided to follow a rather user-centric (and data-centric) design approach. In the left sidebar (see Figure 14 for a bigger image), data subjects find filter options to reduce the amount of presented data. Its intention is to ease the navigation through the data subject's personal data, which is assumed to be extensively large. Besides filtering personal data based on its data type and time of its processing, we consider the context of its processing. We therefore defined

[14] React - A JavaScript library for building user interfaces. https://reactjs.org/, last accessed: 04/16/2018.

[15] Material Design. https://material.io/, last accessed: 04/16/2018.

[16] Material-UI. http://www.material-ui.com/, last accessed: 04/16/2018.

data categories that have been derived from Bruce Schneier's data taxonomy (Schneier 2010), which he defined for online social networks. Here follows a short description of Schneier's data taxonomy:

- **Service data** is any kind of data that is required in order to provide the service in question (name, address, payment information).
- **Disclosed data** is any data that the data subject intentionally provides on their own profile page or in their posts.
- **Entrusted data** is any data that the data subject intentionally provides on other users' profiles pages or in their posts.
- **Incidental data** is any kind of data provided by other users of the service about the data subject (a photo showing the data subject posted by a friend).
- **Behavioral data** is any kind of data the service provider observes about the data subject while he or she uses the service (browsing behavior).
- **Derived data** is any kind of data derived from any other category or data source (profiles for marketing, location tracks, possible preferences).

To adapt this data taxonomy for all kinds of domains, we removed the social network context. Based on the results of a user study, we merged the data categories *Service data*, *Disclosed data*, and *Entrusted data* into a single data category (***Intentional data***). Our resulting data taxonomy is presented below:

- **Intentional data** is any piece of data the data subject deliberately discloses to the controller fully aware of the disclosure.
- **Incidental data** refers to information relating to the data subject shared by another entity with the controller.
- **Behavioral data** is any data obtained from monitoring the data subject's behavior regardless of his or her awareness of the monitoring.
- **Derived data** is any information derived, inferred, or obtained from the other categories or combination of them.

The data is presented in the middle of the screen ordered chronologically beginning with the "oldest" entry from the top to the bottom. Each data item has its own visual representation, which gives information on the time of its processing, a description and explanation of the processing, the data category it belongs to (represented by an icon) and the data itself. As it can be seen in Figure 11, for each data entry a submenu can be opened with one click, which reveals the purpose of the processing and offers possibilities to withdraw consent for the purpose and rectify or erase the data in question.

Withdrawing consent, requesting rectification, or erasure are actual legal requests that have to be responded by the controller within a certain time according to the GDPR[17]. Although it is a goal of SPECIAL to automate the application and realization of these requests, a formal notice is sent to the controller, which documents the request and the deadline for the controller to respond to the request (see Figure 12 for an example of such a message). The deadline is determined in an automated way. The dashboard can help data subjects to manage deadlines of their data privacy requests enabling them to keep track of pending requests and identify lapsed deadlines. This requires an overview of messages sent to the controller, which can be seen in Figure 13. Messages are categorized into pending and answered requests. Here, the data subject can review sent messages and the answers of the

[17] GDPR art. 12(3)

controller to his or her request. Further requests and responses to answers from the controller can be sent as well.

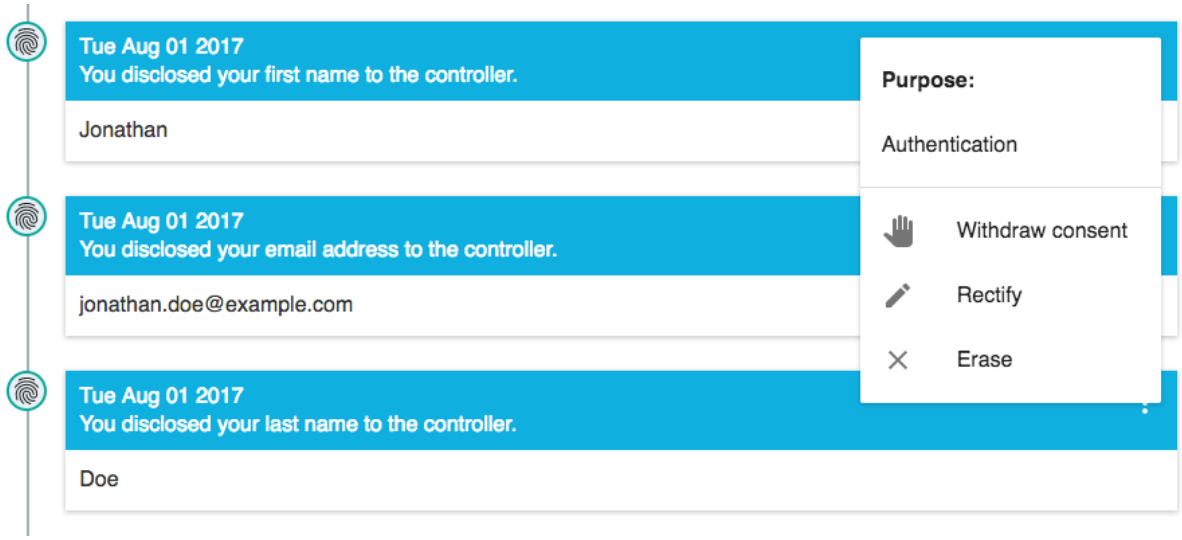

Figure 11: Representation of each data item by a visual component that gives context information on the processing.

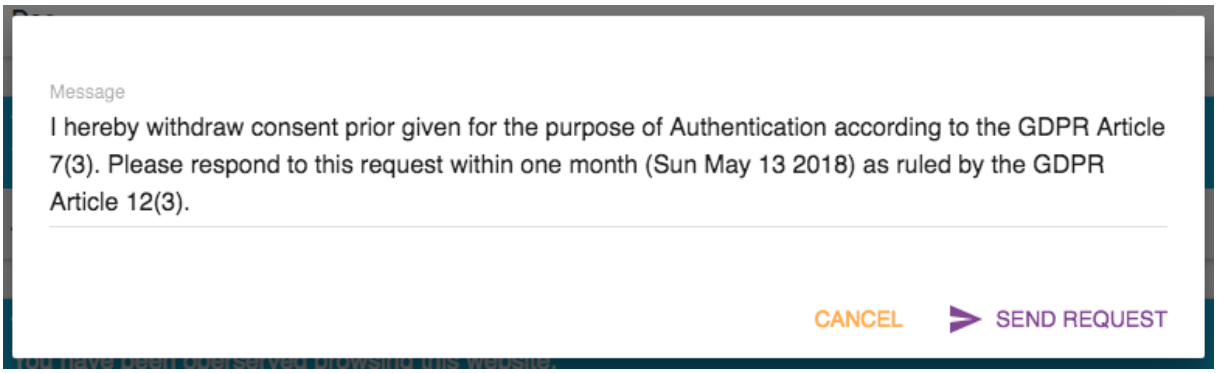

Figure 12: The withdrawal of consent is represented through a predefined written notice that is sent to the controller. The message can be edited by the data subject.

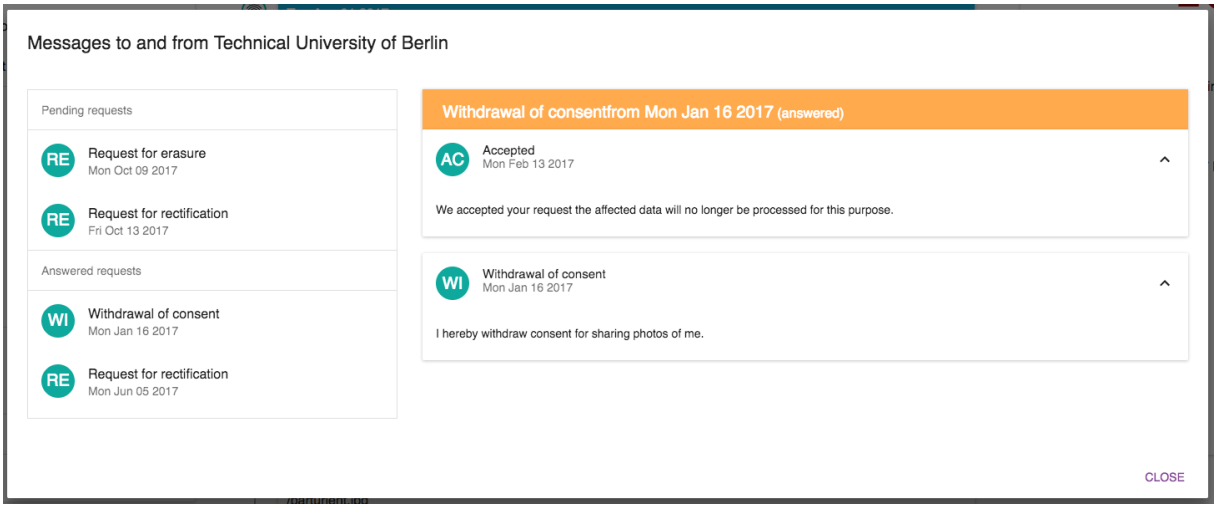

Figure 13: A message section gives an overview of pending and answered requests.

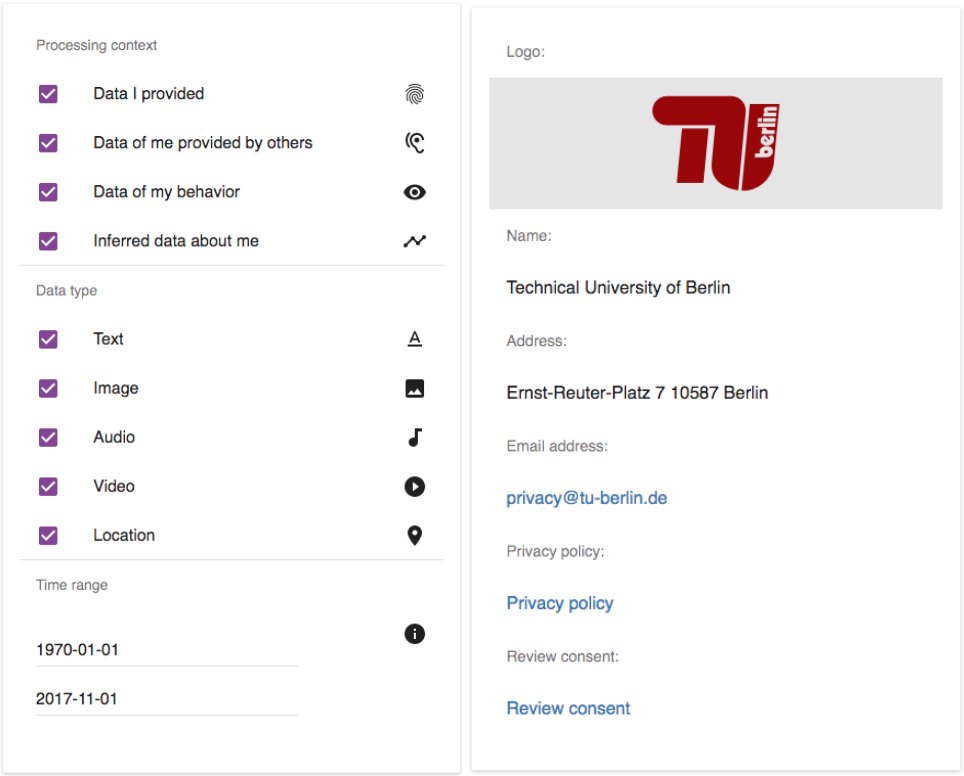

Figure 14: The left sidebar offers data subjects to filter the presented personal data. The right sidebar gives information on the controller in question.

Figure 14 shows the right sidebar that gives general information on the respective controller. General information to contact the controller either physically (name and address) or digitally (email address) are given. A link to the controller's privacy policy might help data subjects to even find the privacy policy (they probably consented to, when registering for the service). The controller component of the dashboard needs further attention in the next iteration to identify, which information is relevant to data subjects with regard to the data controller.

This first version of the privacy dashboard addressed several challenges: (i) the data subjects privacy rights granted by the GDPR (namely right to access, rectification, and erasure), (ii) the handling of a vast amount of heterogenous data, and (iii) the categorization of this data according to its processing context (i.e. the data subject provided the data, it was obtained from other sources, etc.). This version neglected the underlying event log and policy format of SPECIAL, since the log and policy language were not fully specified at that time. We used synthesized data for this prototype, which proofed beneficial for the user tests we conducted on this version.

4.2 Privacy Dashboard V1.1

This section presents the enhanced version of the privacy dashboard as of **D4.2 Usability testing report V1**, which was submitted in month 18 (June 2018). It can be accessed via https://specialprivacy.github.io/D4.2-Privacy-Dashboard-DEMO/ and the source code is available at https://github.com/specialprivacy/D4.2-Privacy-Dashboard. We adapted the feedback gathered in the early user tests to improve the usability of the privacy dashboard's first version.

Adjustments had been made to test how users respond to a more abstract view. See Figure 15, in which the actual data items are concealed per default and an option to display a certain data item is offered to the user (see Figure 16). Moreover, data items are aggregated over a certain time period (for example a day) to reduce entries in the timeline. This way the privacy dashboard is less overloaded, and data can be shown on demand.

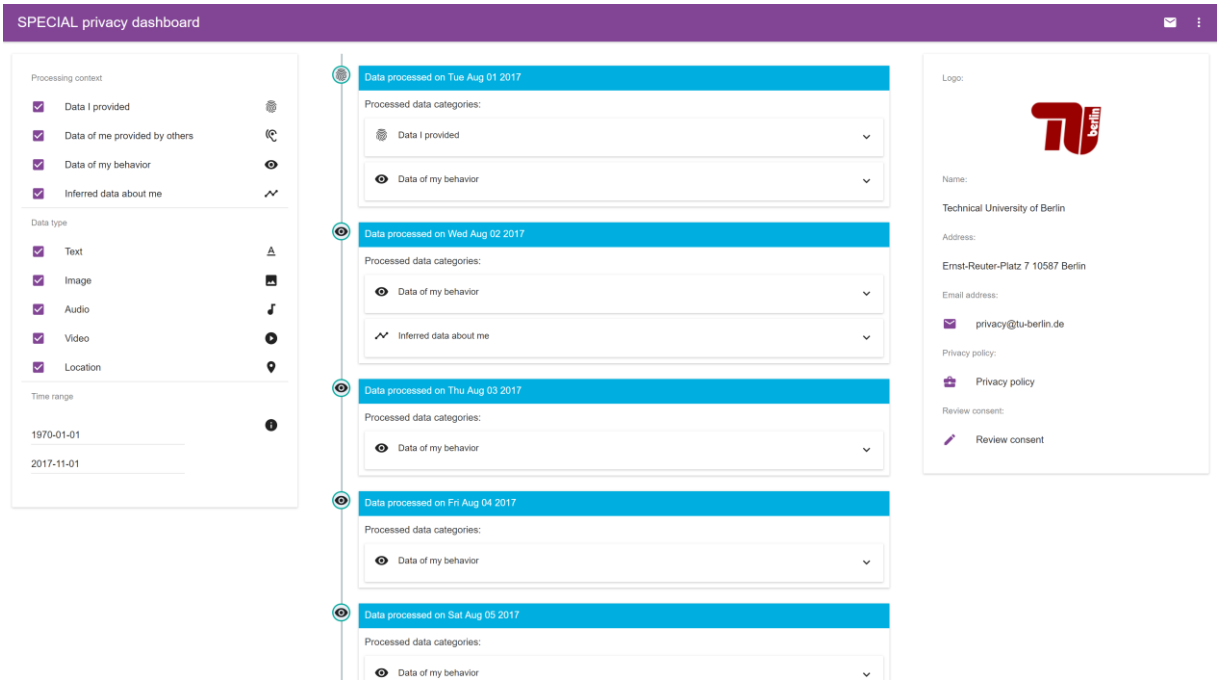

Figure 15: Aggregated data processing items to reduce complexity

This small adjustment was made based on the feedback retrieved in the first iteration of the conducted usability tests. The main goal of this attempt was to offer users (fewer) summaries of their personal data instead of the bulk of personal data at the beginning. This way, redundant or irrelevant information can be hidden and relevant aspects easier identified. For the categorization we used our personal data taxonomy. The interval in which "events" were grouped into one timeline event was determined dynamically based on the frequency of processing events occurring in the log.

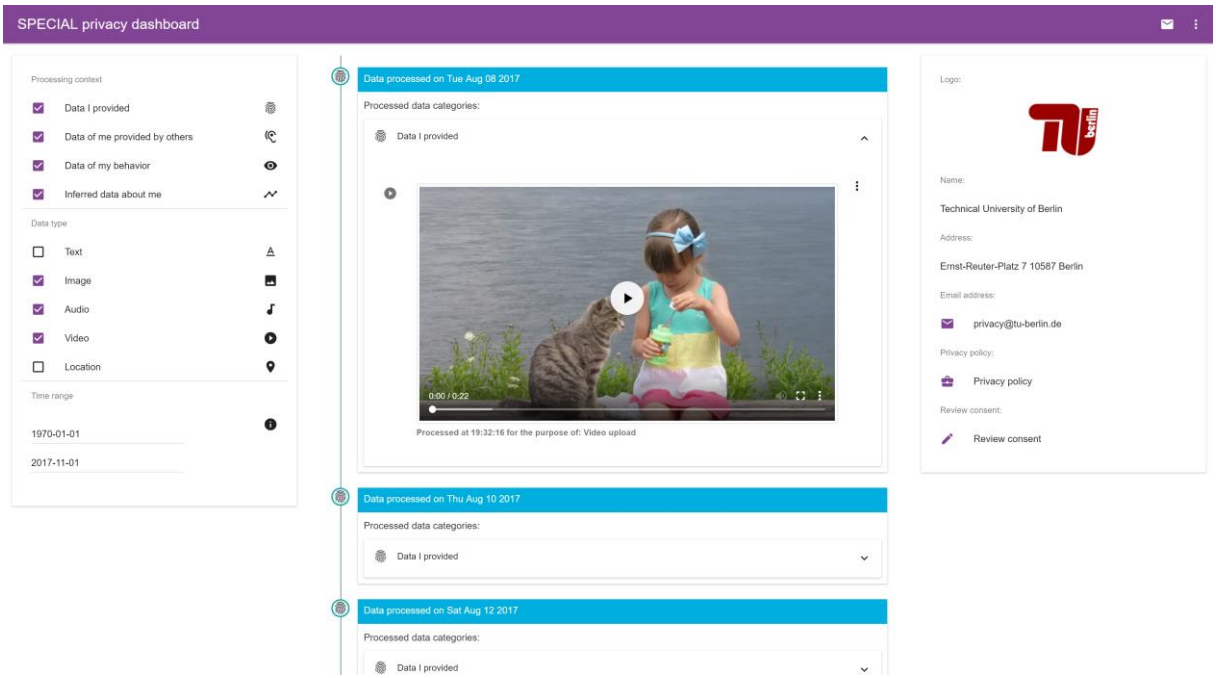

Figure 16: Aggregated data processing items with expanded data item

4.3 Privacy Dashboard V2

This section presents the second version of the privacy dashboard as of month 25 (January 2019). With the second release of the privacy dashboard we enhance the event log visualization and address the functional components: access and usage policy, policy template, and consent engine (see 2.1.1). Besides visual improvements version two also aims to give users a broader view on the data the controller processes, the kind of processing that is executed, the processors involved, and the physical location of the controller's and processor's servers. This version was also published on GitHub and can be accessed via https://specialprivacy.github.io/D4.3-Privacy-Dashboard-DEMO/ and the source code is available at https://github.com/specialprivacy/D4.3-Privacy-Dashboard.

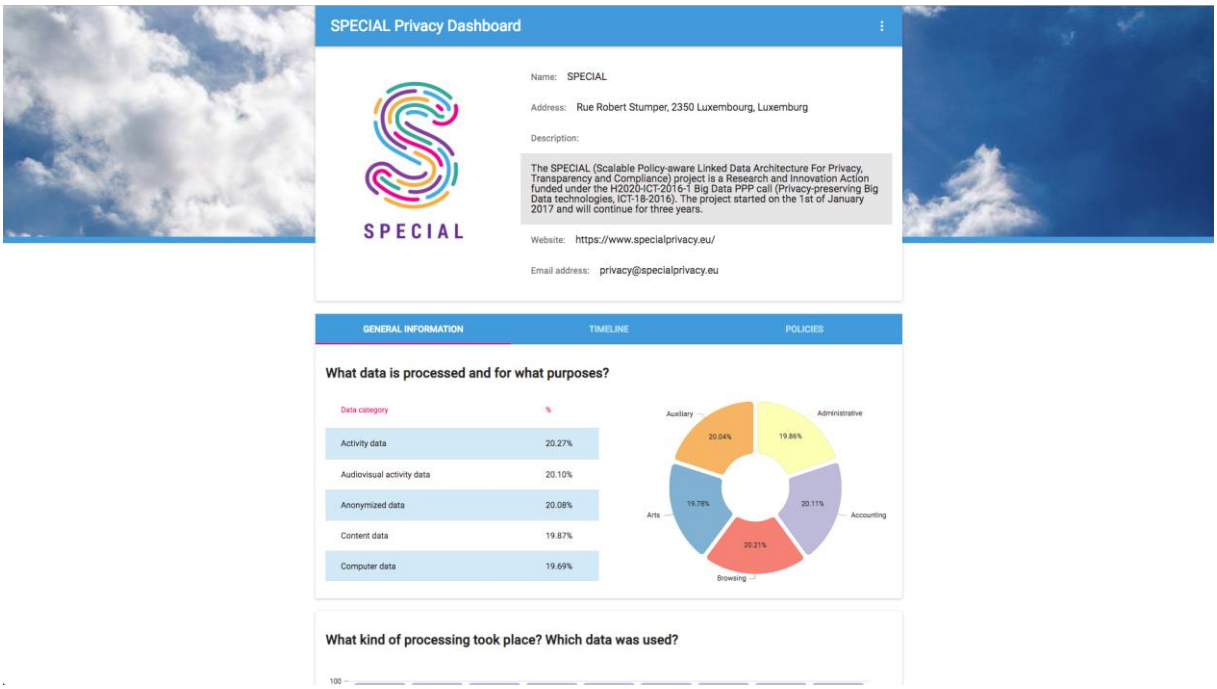

Figure 17: A screenshot giving an overview of Version 2 of the privacy dashboard.

As it can be seen in Figure 17, we abandoned the simple three column approach, and give the most relevant information on the controller (including the controller's logo, the name, a description, an email address, and the controller's website) at the top of the page. The timeline of processing events was moved to another tab to directly present the user with statistical information on the controller's processing practices. Tables and (rather) simple charts are used to provide the user with an overall picture of the controller's personal data processing practices. We therefore define the following four questions, we consider most important for users, who use the privacy dashboard:

1. What data is processed and for what purposes?
2. What kind of processing took place and which data was used?
3. Where is data stored and with whom was it shared?
4. Where is which data stored?

Each question is supposed to be answered separately in a so-called card with the help of tables and charts. The statistics shall provide an overall picture without being too specific. Therefore, the

relatively broad data categories of the SPECIAL vocabulary suit well. The cards are supposed to confirm (or not confirm) user expectations. Users might expect that a location-based service, for instance, processes location data predominantly, while processing no health data at all.

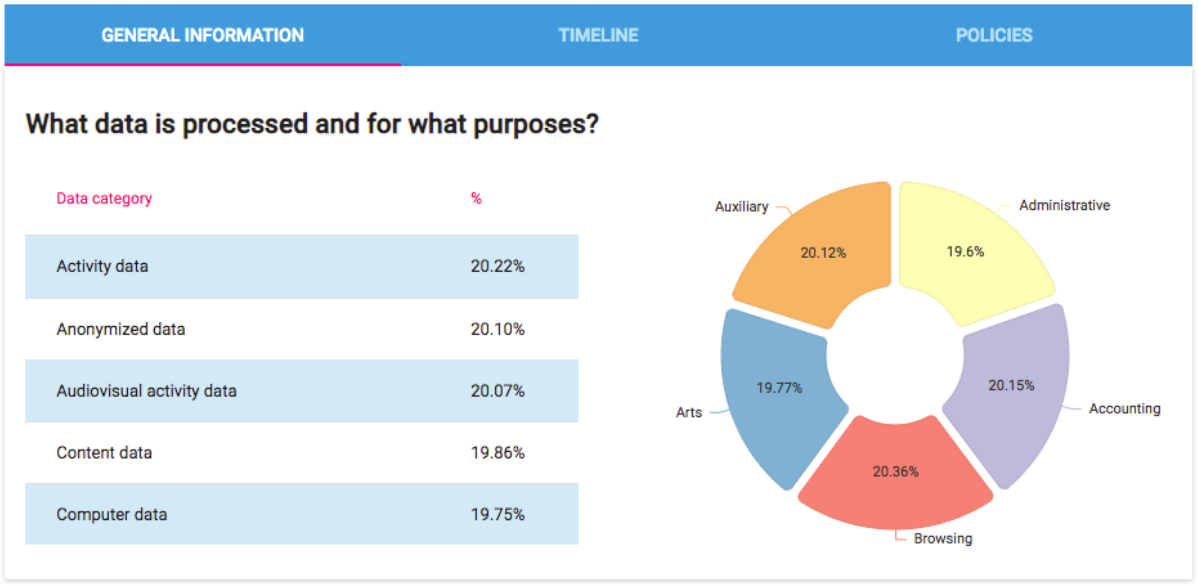

Figure 18: A card to give the user general information on processed data and for which purposes it is processed.

Figure 18 shows the first card, which gives information on the kind of data that is processed by the controller and the purposes for which the controller processes personal data. On the left-hand side, the top five processed data categories are listed in a table sorted by their amount of the total processing logs. On the right-hand side, a pie chart is given to visualize the amounts of processing logs with regard to the processing purpose. Here, all purposes that appear in the processing events logs are visualized regardless of how small their overall amount might be. It is important to note, that there is no correlation between both visualizations, i.e. there can be, for example, no statement made on whether the (roughly) 20% of activity data (in Figure 18) are evenly used for all purposes or only used for one of the purposes.

In contrast to that, Figure 19 shows correlations between processing types and data categories used for the processing. For each processing category, the corresponding data categories are stacked according to their amount of processing events with that specific processing type. From that diagram it can be for instance inferred that more than one fifth of the data that is anonymized is activity data or that approximately one fifth of the data that is aggregated is audio-visual activity data.

Figure 20 and Figure 21 are similar to Figure 18 and Figure 19. They aim to provide the user with information on the physical location of servers on which the user's personal data is stored. Besides the physical location the SPECIAL vocabulary also addresses the sovereignty of these servers. Is the controller fully in charge or are other parties involved? Who retrieves my personal data and which privacy practices do these third-parties have? These questions are not answered by the card (Figure 20) but a general tendency is given. When in doubt because the chart does not address the user's expectation, then the user is able to further navigate in the privacy dashboard to answer those questions.

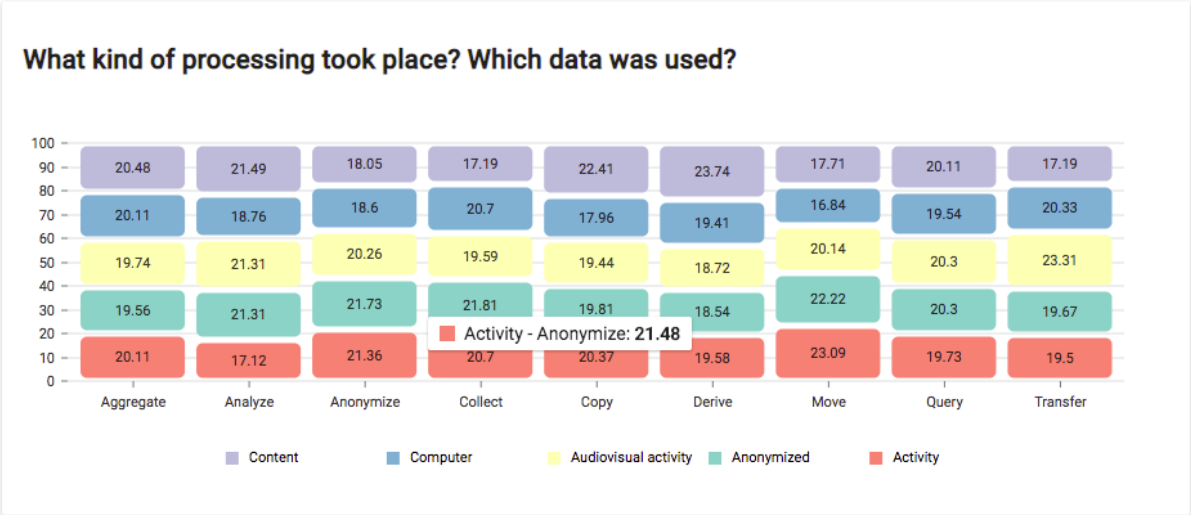

Figure 19: A bar chart to visualize correlations between kinds of processing and categories of data.

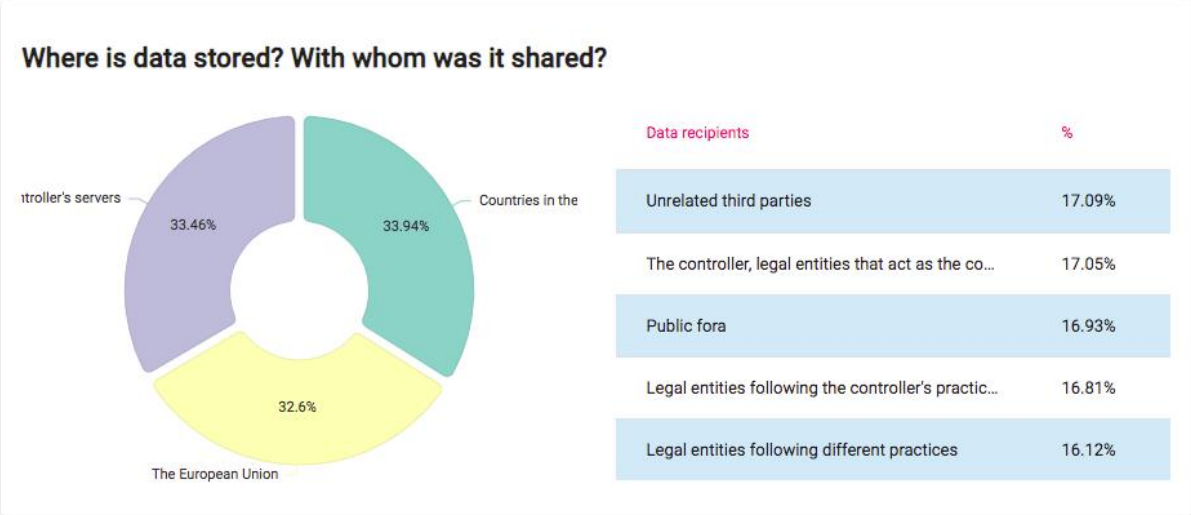

Figure 20: A card to give users an impression of where their data is stored and what kinds of third parties retrieve it.

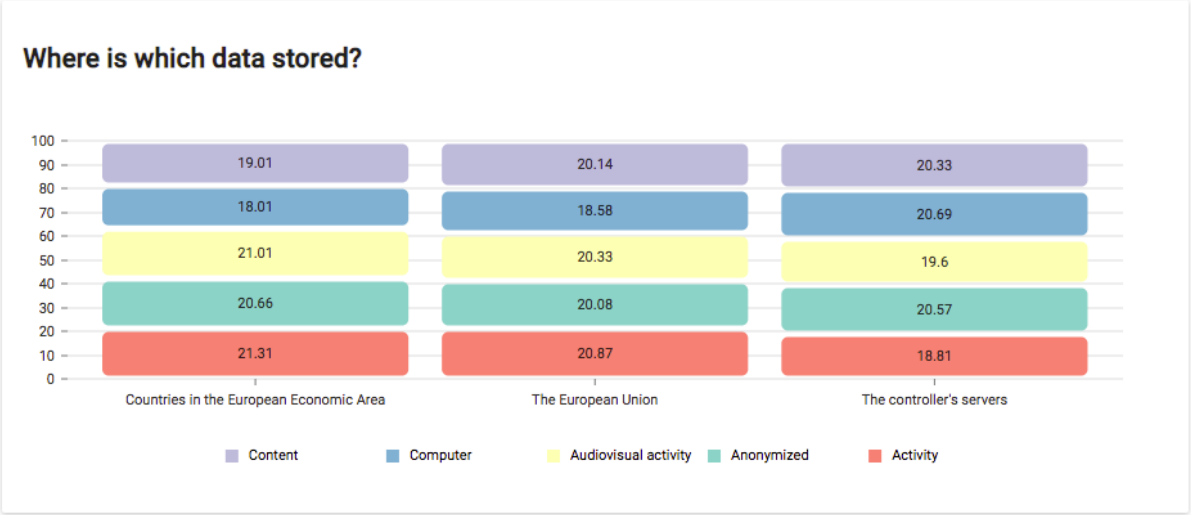

Figure 21: This chart gives information on where which kind of data is stored.

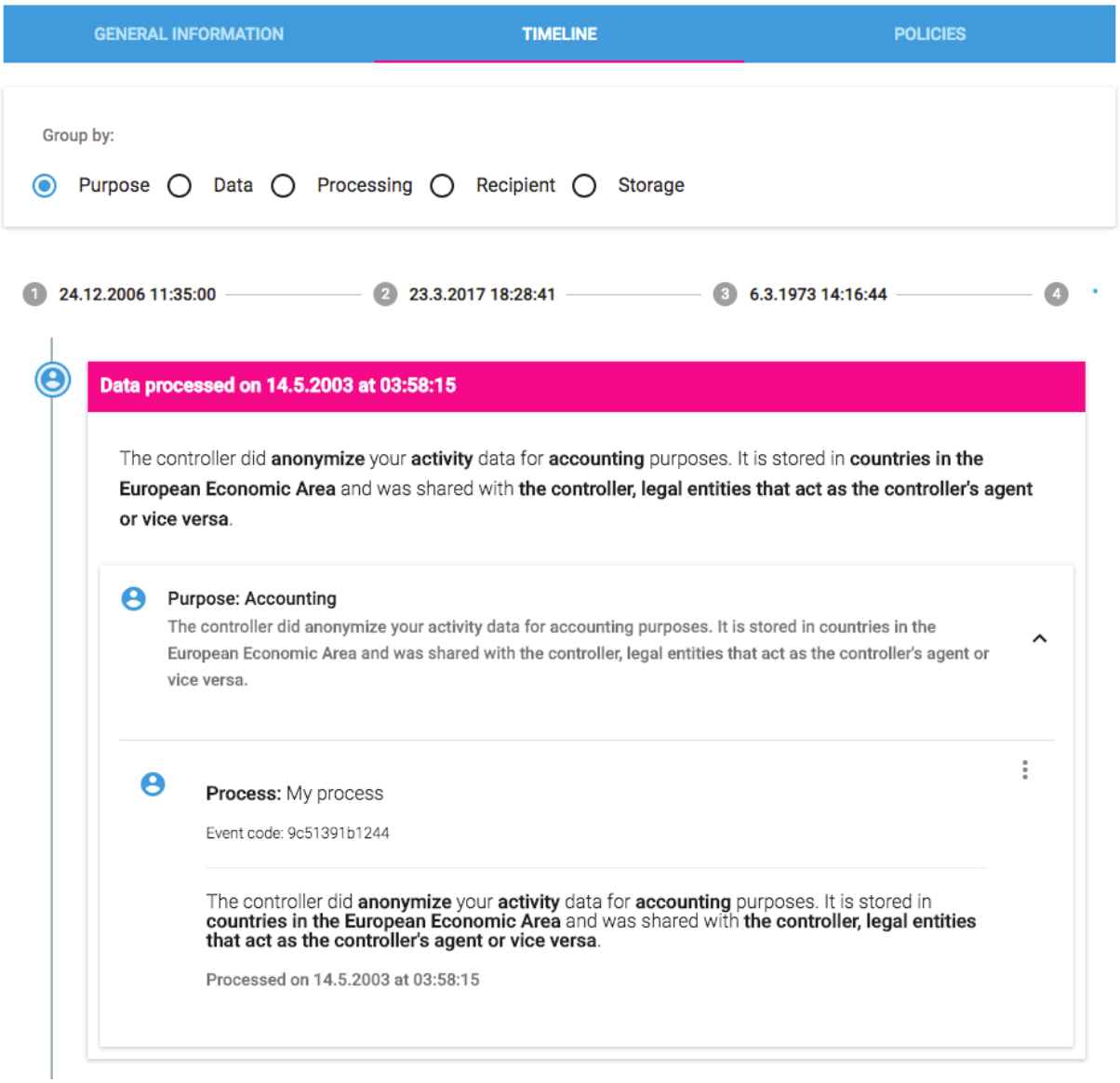

Figure 22: Improved visualization of processing events in the timeline.

In the previous version of the privacy dashboard there was a processing event log entry foreseen for each data item that was processed. This led to many visual repetitions of timeline entries, which are interdependent (see Figure 10 and Figure 11). Moreover, we expect the frequency of processing events in some use cases to be very high, thus many events need to be considered. Therefore, further grouping of those events is desirable (see also **D4.2 Usability testing report V1**). The data categories of Section **Fehler! Verweisquelle konnte nicht gefunden werden.** are not compatible with the SPECIAL vocabulary, hence the filter options of the previous version were removed. Now, events can be grouped by **purpose**, **data** category, kind of **processing**, the **recipient**, or the **storage location**.

Each timeline entry (card with pink header as in Figure 22) gives information on personal data processing within a certain time range. A textual summary is given to list which data categories were processed for which purposes, where stored, and with whom shared. Depending on the grouping criteria another card (within the timeline card) is given to give more specific information. This card can be extended to see the corresponding processing events for which a textual visualization is given. The submenu of the previous version (see Figure 11) is also included in the most recent version.

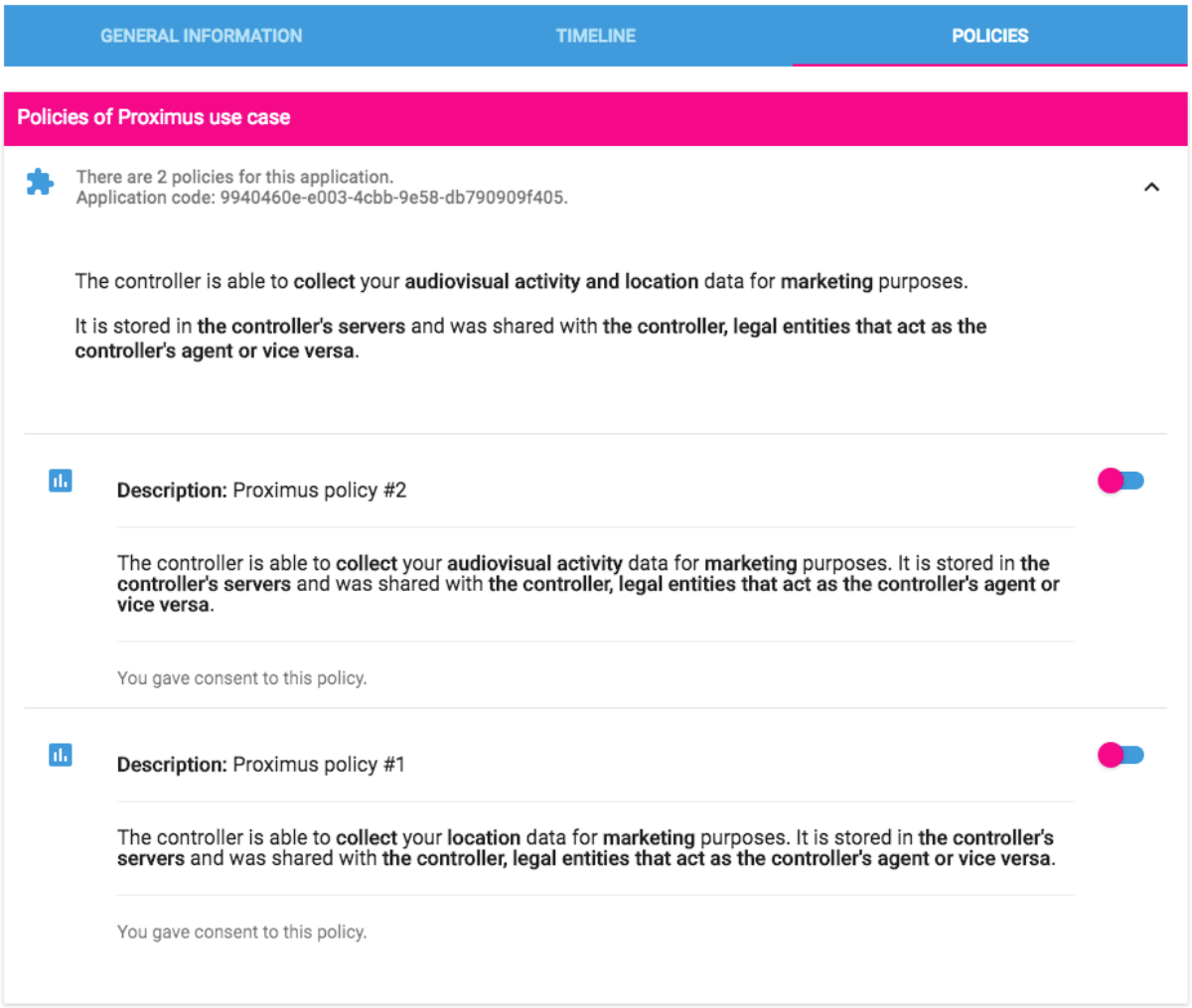

Figure 23: Under the policies tab the user can view the controller-specified policies and update consent to them.

By opening the policies tab, the user is able to see all controller-specified policies. Furthermore, the user is able to see to which policies he or she consented to and if necessary is able to withdraw consent for a single or multiple policy. Policies are in relation to an application of the controller; therefore, policies are grouped by their respective application. One problem of this view is that if a policy is in relation to multiple applications it would be visualized multiple times. However, it is thinkable that the user might give consent to a policy for a certain application but not for another. Figure 23 also shows the textual representation of a single policy or a set of policies.

When clicking on a data category, a purpose, a kind of processing, a storage location, or a recipient (in the charts or in the tables), a view (so-called modal) opened (see Figure 24) in which correlations between the selected attribute and the other attributes of the event log format are visualized. This way, users could answer questions like: “For which purposes was location data processed?”, “Where is location data stored?”, or “With whom was location data shared?”.

Figure 24: View to identify correlations between event attributes in the event log.

This version of the privacy dashboard incorporated SPECIAL's event log format. At the time of deliverable **D4.3**, the log format did not include a reference to the personal data (the corresponding log entry is about) nor the personal data itself. Thus, only limited statements could be made by the privacy dashboard: "At that particular time, your data was processed for this purpose stored at this location and shared with this entity". These events had to be expressed with the SPECIAL vocabulary, which was very limited at that time. Thus, the results of user tests conducted on this version of the privacy dashboard (see **D4.4)** are sobering.

While this version is capable of expressing even complex correlations in the event log and offering data subjects almost maximum insights on their processed personal data, it is not usable. Users expect a data-centric design to a certain extent. Privacy dashboards of popular services provide access to "all" the data they have about the user and this is what users expect when they assess their data privacy with regard to a certain service or service provider. This version of the privacy dashboard underlined the significance of the actual data in privacy and transparency-enhancing tools. We found, that users need it as means for self-identification and reflection. This user requirement was communicated into the consortium and the event log was adapted.

4.4 Privacy Dashboard V3

This section presents the third and final version of the privacy dashboard as of month 35 (November 2019). After the clear direction set by the results of the user tests conducted in the context of D4.4, we completely redesigned the privacy dashboard. In fact, we returned to the data-centric approach. Thus, synthetic data was generated and used for this version of the privacy dashboard. We have also adapted an application-centric design over a controller-centric design, i.e. that the privacy dashboard shows users' personal data that is processed within the context of a particular service. This version was published on GitHub and can be accessed via https://specialprivacy.github.io/D4.5-Privacy-Dashboard-DEMO/ and the source code is available at https://github.com/specialprivacy/D4.5-Privacy-Dashboard.

After D4.4 there were only eight months left to address the issues of the privacy dashboard's second version. The first action, we have taken was to generate synthetic user data in order to enable the visualization of personal data in the privacy dashboard. This synthetic data was encoded in the SPECIAL log format. Figure 25 shows the redesigned privacy dashboard. The privacy dashboard is fully responsive and is optimized for handheld devices. We reintegrated the message section from the first version of the privacy dashboard. See Section 4.5 for a detailed presentation. The menu on the left-hand side consists of the following entries:

- "My Profile", a page to show intentional and derived personal data of the data subject.
- "About %SERVICE_NAME%", a page about the service provider and involved third parties.
- "My Data", a page to visualize all personal data of the data subject.
- "My activity log", a page to visualize the contents of the event log.
- "My permissions", a page for data subjects to review the privacy policies for this service.

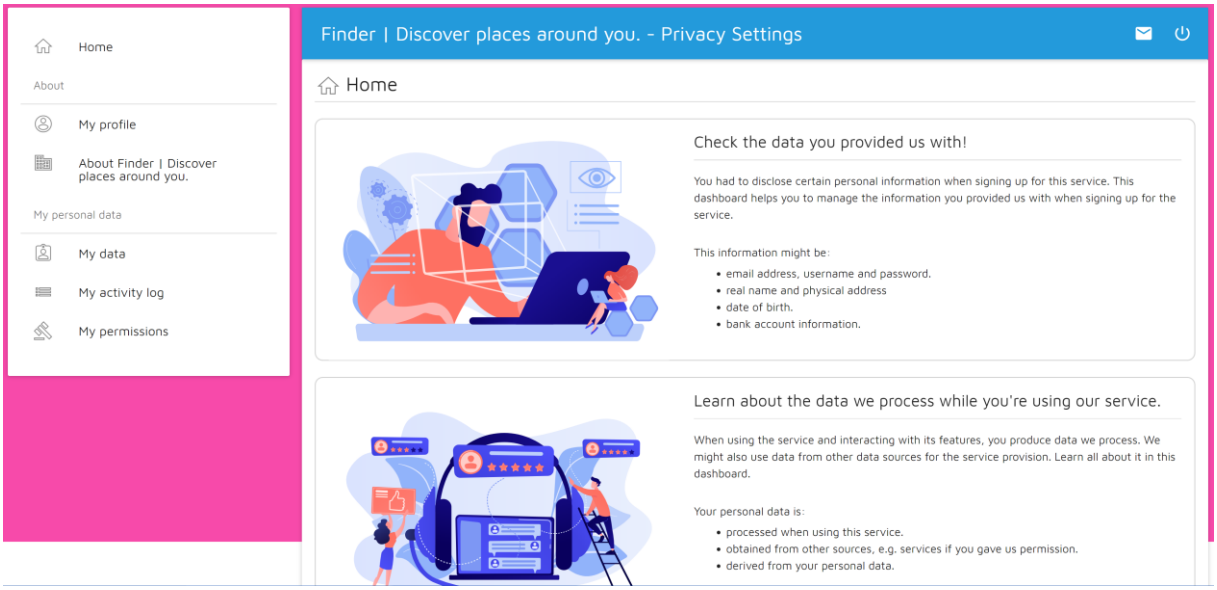

Figure 25: Overview of the third version of the redesigned privacy dashboard.

The page "My Profile" (see Figure 26) offers users details on which information the controller has about the user. It is meant to contain "hard facts" like email address, username, bank account information, physical address, occupation, marital status, and suchlike. It can also contain derived information like marketing or interest profiles.

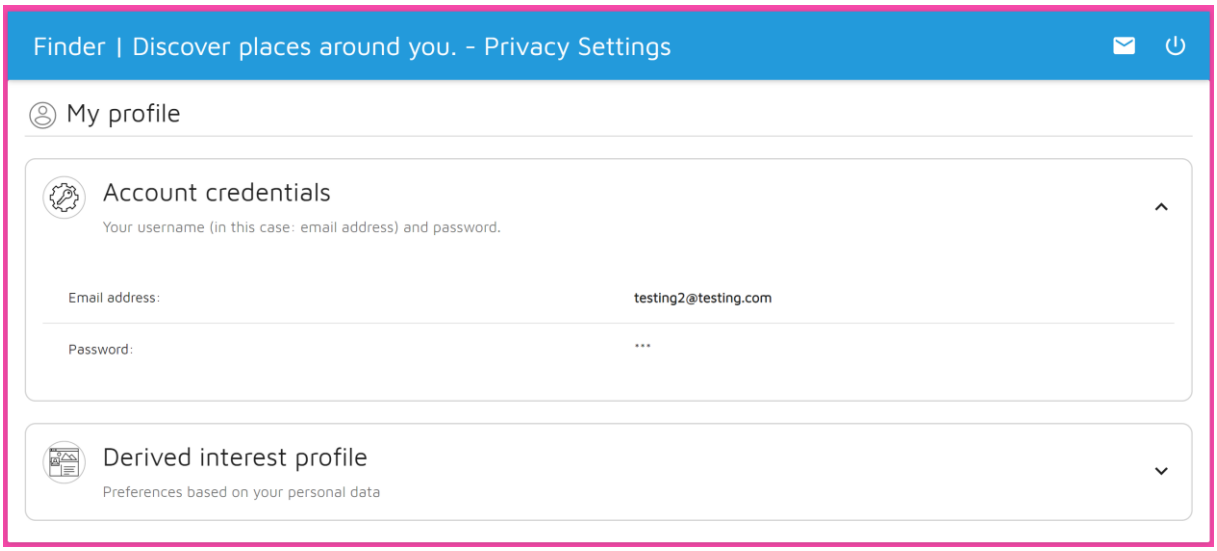

Figure 26: The "My Profile" page showing intentional and derived data.

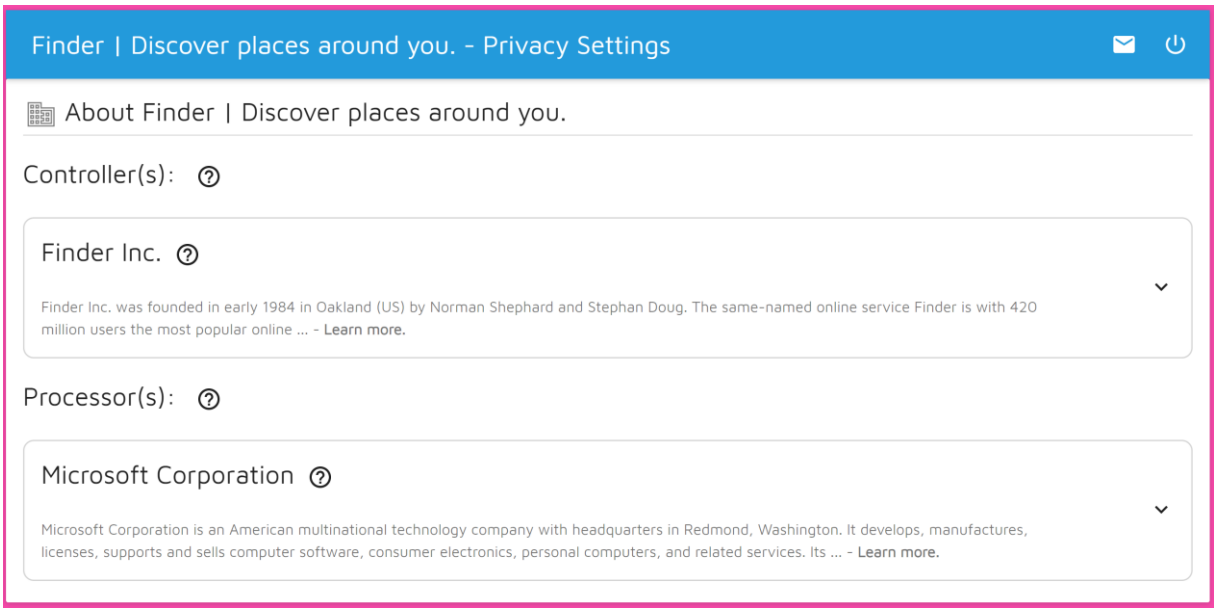

Figure 27: The page to give information the controller(s) and processor(s) and their roles with regard to the service.

Figure 27 shows the page, which gives data subjects information on the controller and processors involved in the service provision. Information on the individual legal entities can be given by the controller (who is meant to be in charge of the provision of the privacy dashboard) or obtained from public sources like Wikipedia. This information, however, must include links and addresses to the privacy policies of the service and controller and the data protection officers in charge. Thus, the automated provision of such information is difficult to realize but desirable. The page contains the legal terms controllers and processors, which confused many users in our user tests. Therefore, help texts are provided to explain those terms. Yet, we propose to replace these terms with “service provider” and “third parties”. Help texts are also provided for each legal entity, which are supposed to explain the role of the respective legal entity within the service provision.

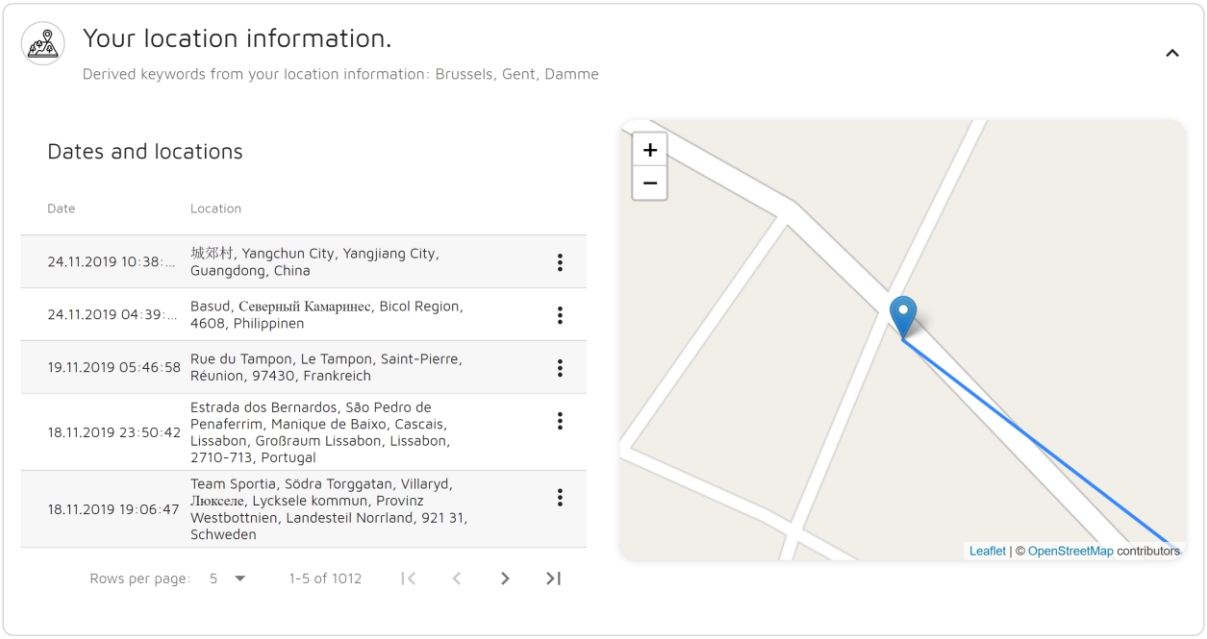

Figure 28: A user interface for location data visualization.

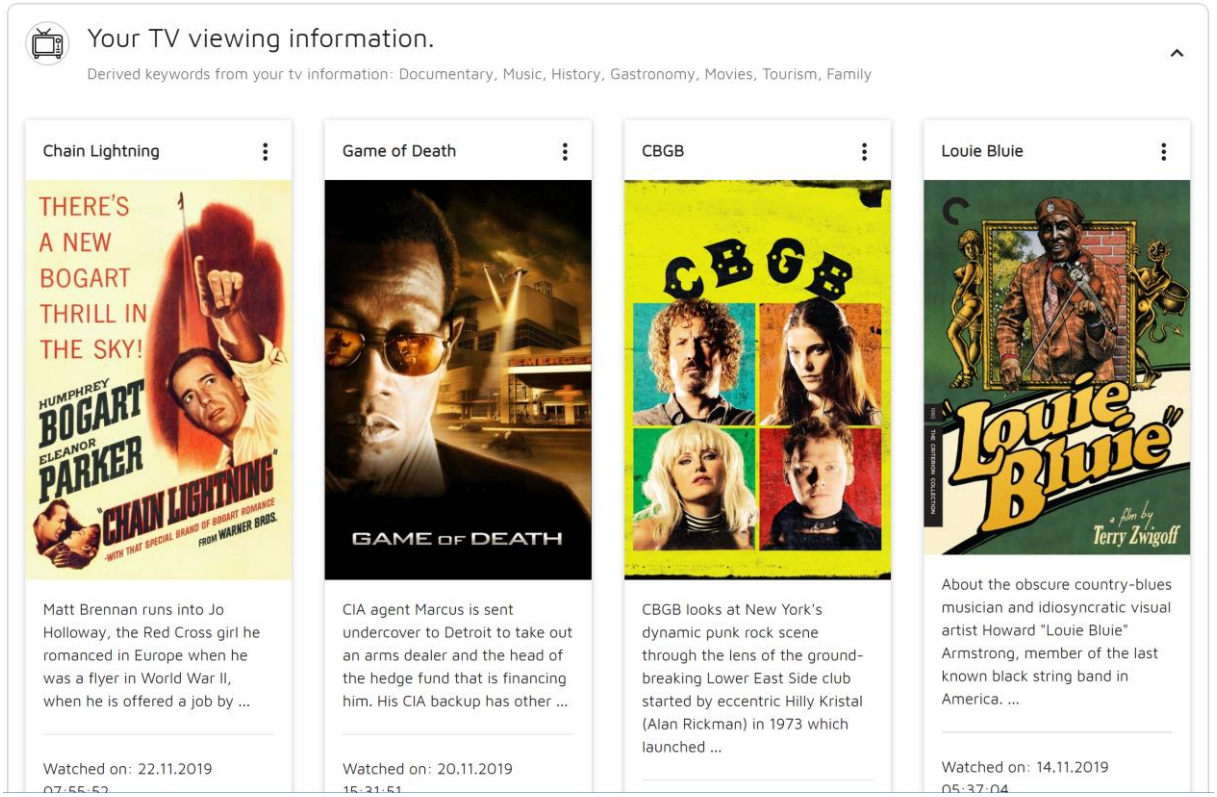

Figure 29: A user interface for TV viewing data visualization.

Figure 28, Figure 29, and Figure 30 show the contents of the “My Data” page. It proofed helpful for users to extend the actual (raw) data item with meta information in the visualization, i.e. a geolocation is extended with the physical address, a movie title is extended with a movie poser and description, or a website is extended with a thumbnail, a title, and a description. A data subject can request rectification or erasure for each data item. However, our user tests indicate that users would not use

means to rectify inaccurate data, but rather request erasure of the wrong data without replacing it with accurate data.

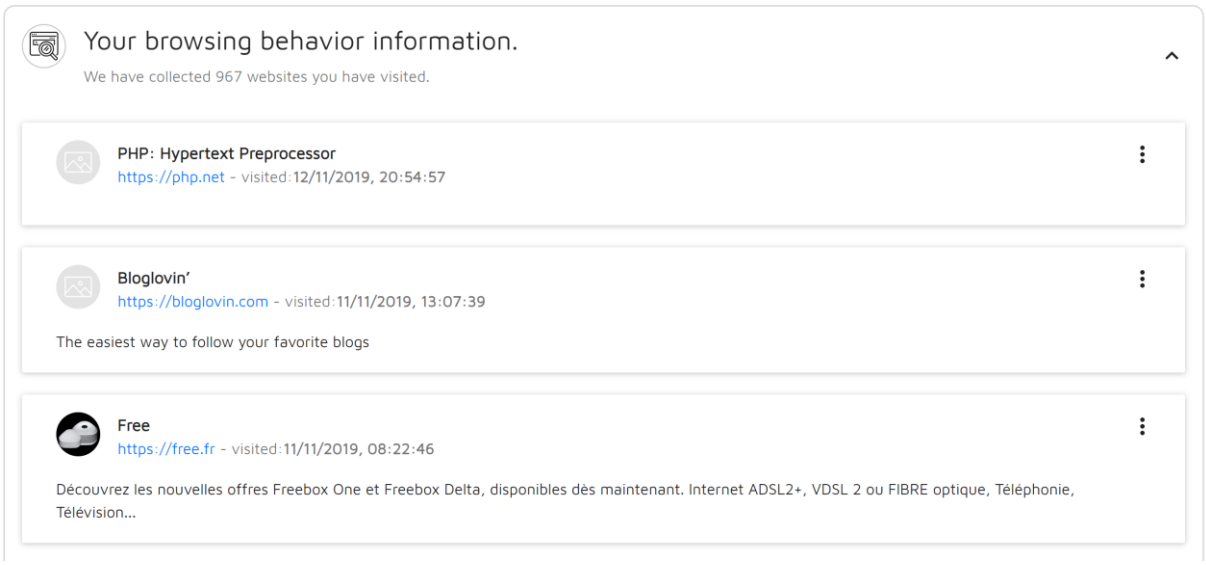

Figure 30: A user interface for browsing behavior visualization.

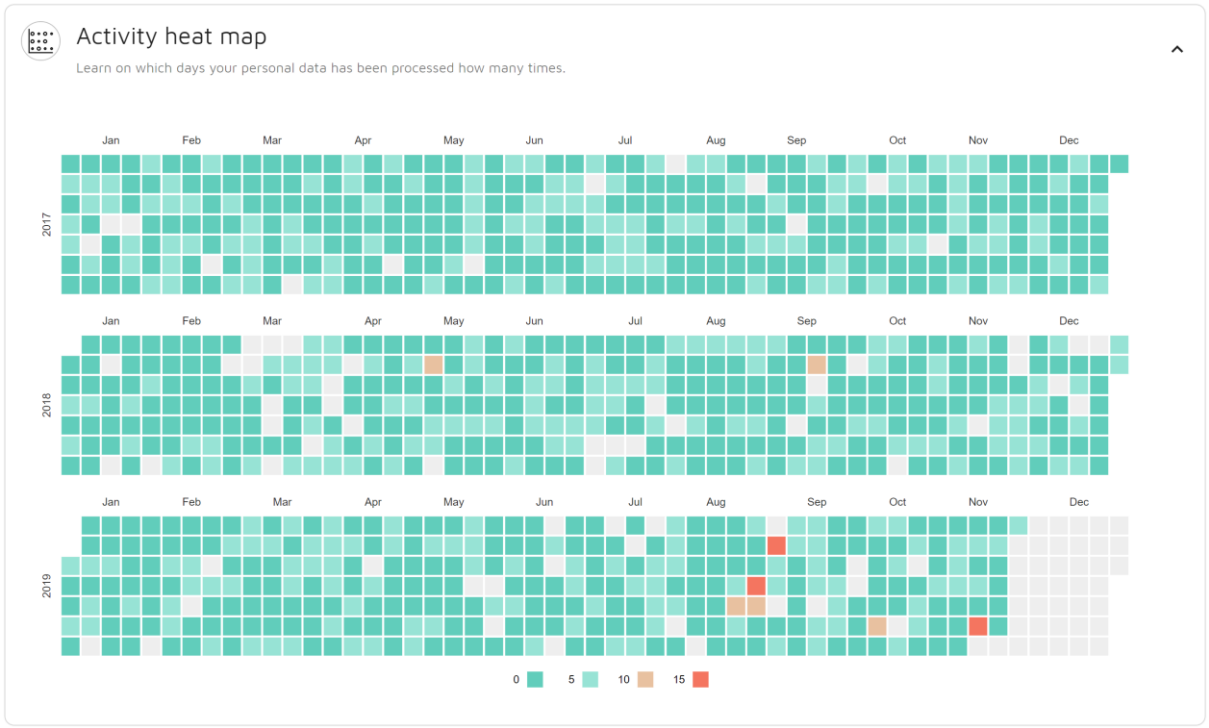

Figure 31: The activity heat map showing users when "how much" personal data was processed.

The “My activity log” page consists of two elements: (i) the activity heat map (see Figure 31) and (ii) the activity log (see Figure 32). The activity heat map is supposed to give users a broad overview of the contents of the event log with regard to the frequency of log entries. This way, users can match the heat map with their expectations and identify when and how much processing happened and whether this aligns with their service-usage or not. In the latter case, users could conclude that background processing is happening. The content of the event log is fully visualized in a table that is sortable by the individual attributes of event log format.

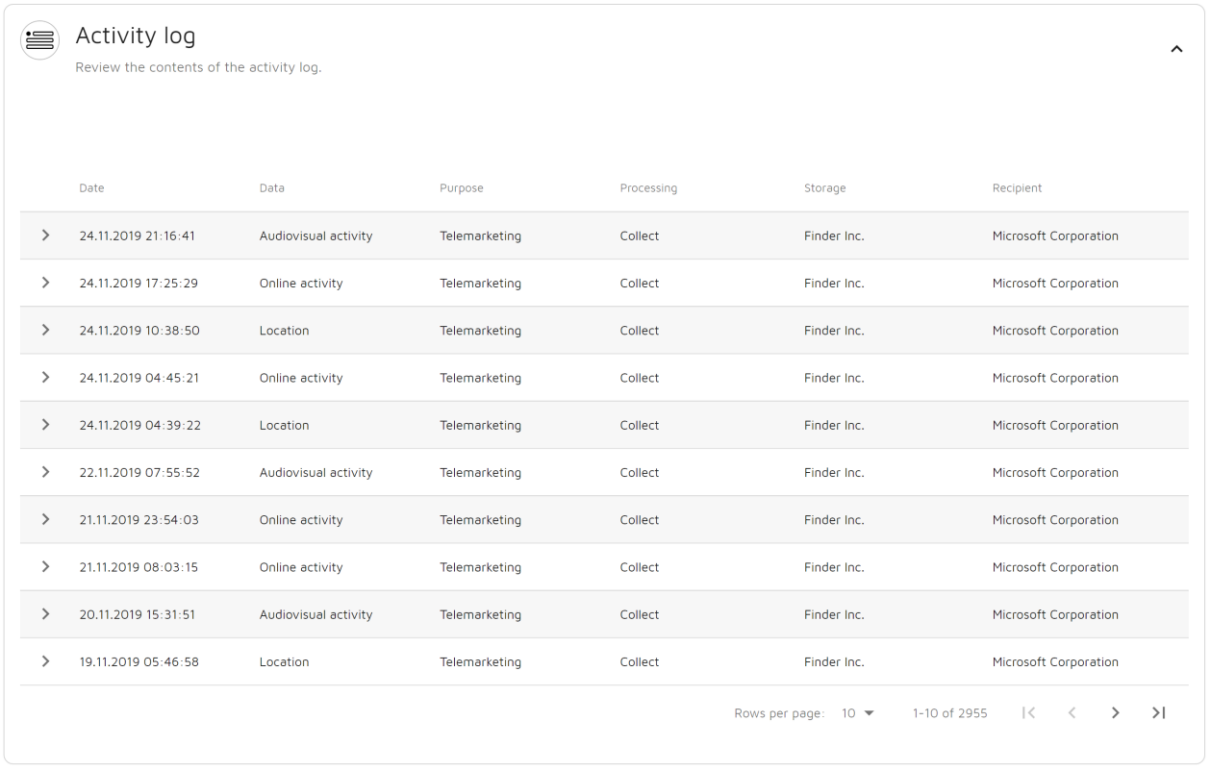

Figure 32: The contents of the event log represented in a table.

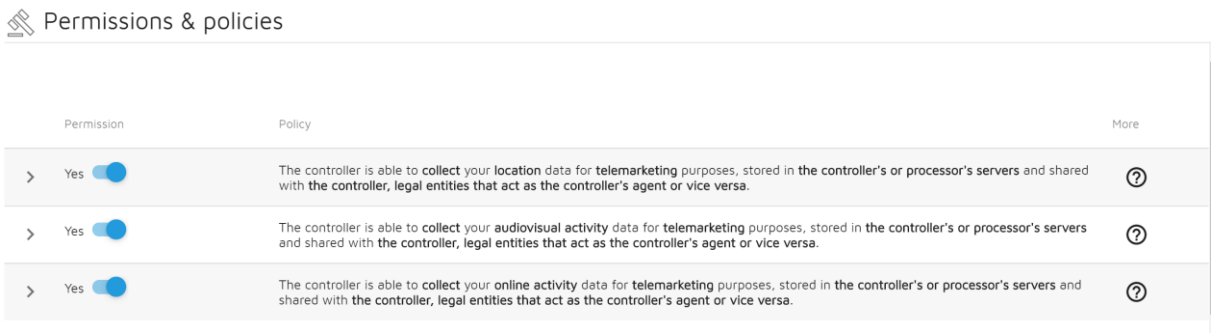

Figure 33: The policies view where data subjects can give or withdraw consent to controller-specified policies.

Figure 33 shows the “My permissions” page, which displays the user all controller-specified policies the user might consented to or not. It also offers means to give or withdraw consent. A help text is provided to further explain the policy to the user (see Figure 34). This help text contains a description of the policy, information on consequences in case the user does not agree, and risks involved in consenting to the policy. All policies are encoded in the SPECIAL policy format. The description is generated automatically. However, for the statements in the help text, the controller has to make dedicated statements, since this information cannot be expressed with the SPECIAL privacy policy language.

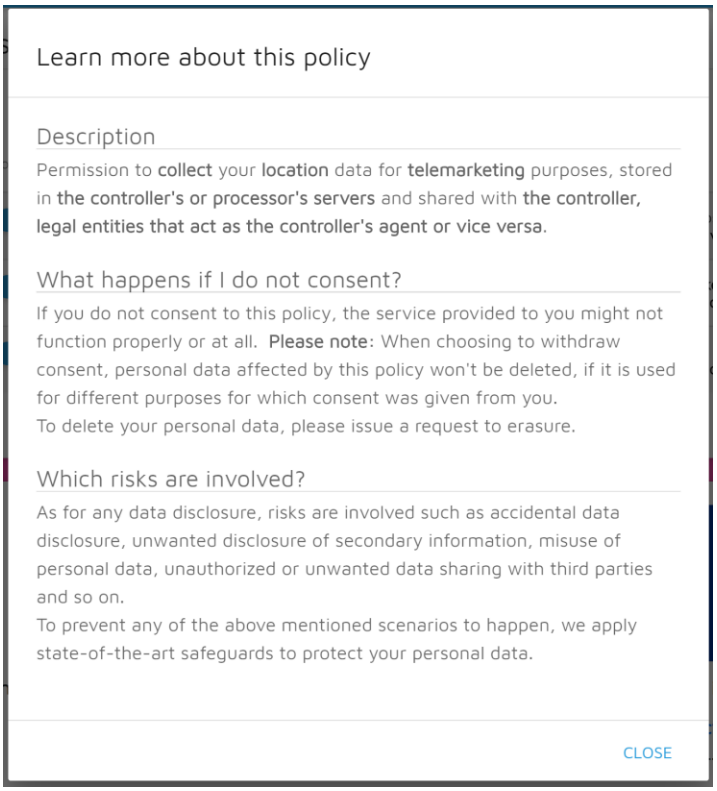

Figure 34: For each policy statements should be published by the controller giving information on alternatives to consenting and the risks involved giving consent.

This is the final version of the privacy dashboard. While visually improved, there is potential for further improvements left. At this point, we want to refer back to the functional and general requirements of the privacy dashboard and assess the end result:

ACCESS DATA

We provided means for data subjects to access their personal data processed within the context of a specific service by a set of controllers and processors for specific purposes. This vast and heterogenous data is visualized by the privacy dashboard and enriched with information from public sources.

EVENT LOG/ PROVENANCE

The privacy dashboard uses the SPECIAL event log format, visualizes its contents, and provides an overview of the event log with respect to a particular data subject.

ACCESS AND USAGE POLICIES

The SPECIAL policy language is used to encode policies. These policies are controller-specified and data subjects can consent to them or withdraw consent from consented policies. User-specified policies were not incorporated in the privacy dashboard, since our user studies indicate that users rather want to specify concrete policies like: “Do not track me when I’m at this particular location”. This statement cannot be made with the SPECIAL policy language.

POLICY TEMPLATES

Policy templates were neglected for the same reason as user-specified policies.

CONSENT ENGINE

The consent engine has been incorporated by the privacy dashboard.

BREACH NOTIFICATION

Breach notifications were not addressed by the privacy dashboard. Due to strict legal regulations, we found the privacy dashboard not the best option to inform users about data breaches as this would require users take the initiative (by logging into the privacy dashboard first). Furthermore, controllers might want to choose the information they want to disclose in case of a data breach carefully. Giving information on the event log level in the dashboard could be rather confusing to users. In addition to all this, when data breaches happen controllers might not be able to exactly say which data was leaked or whether data leaked at all.

PERFORMANT AND SCALABLE

The privacy dashboard is performant and scalable to the extent that it can handle and visualize a vast amount of personal data of a single data subject.

SECURE

It is secure to the extent that state-of-art technologies and best practices for Web applications have been considered. However, for the prototype of the privacy dashboard some minor insecure “shortcuts” have been taken for the sake of a faster development.

PRIVACY-ENHANCING

It is privacy-enhancing to some extent. Generally, it can offer help and guidance to users, who have privacy concerns.

USABLE

It is usable, however, needs further iterations and refinements in order to be a production ready solution.

4.5 Data Protection Officer Dashboard

Since we reintroduced the message section of the first version of the privacy dashboard in the last version of it, it became necessary to model, design, and partially implement the whole workflow related to a data subject request. Therefore, we implemented the Data Protection Officer (DPO) Dashboard to show how data subject requests can be retrieved, visualized, and further processed. The DPO Dashboard can be accessed via https://specialprivacy.github.io/DPO-Dashboard-DEMO/ and the source code is available at https://github.com/specialprivacy/DPO-Dashboard.

Figure 35 shows an overview of the DPO dashboard, which has a similar layout and design to the privacy dashboard. This does not necessarily have to be the case in a real-life scenario. In fact, the DPO dashboard is intended to be a separate application than can build upon a completely different software stack than the privacy dashboard. The DPO dashboard currently consists of two pages: the “Overview” page, which is intended to give DPOs statistics on retrieved data subject requests, and the “Requests” page, which offers the DPO to access and assess individual requests and if necessary forward them to the responsible unit in (or outside) the company.

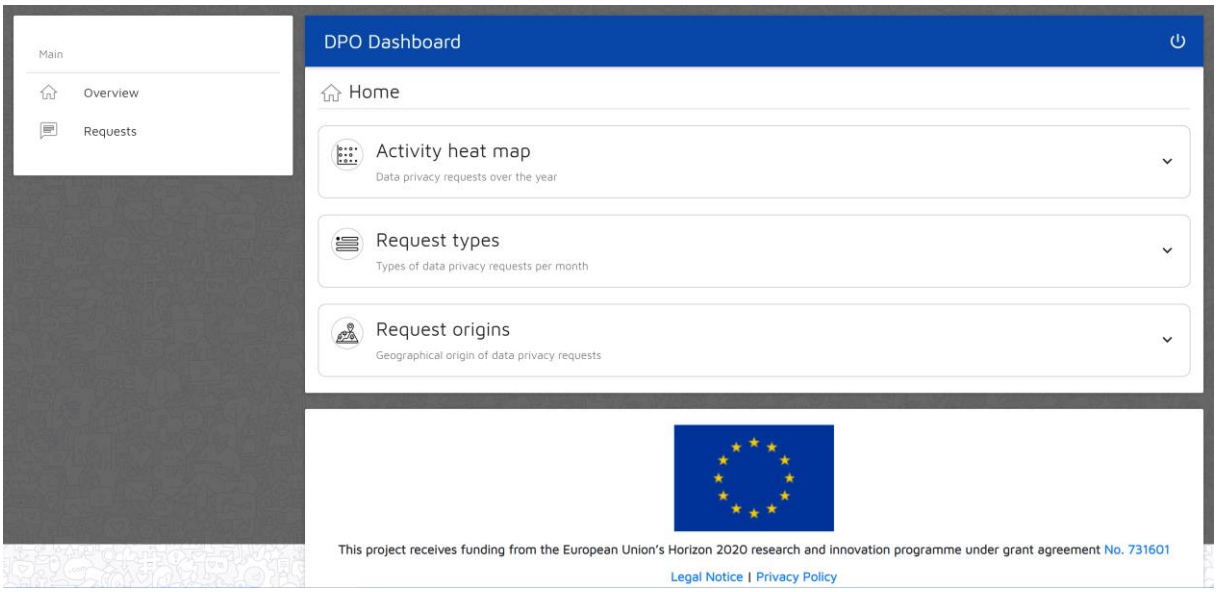

Figure 35: Overview of the DPO Dashboard with similar layout as the privacy dashboard.

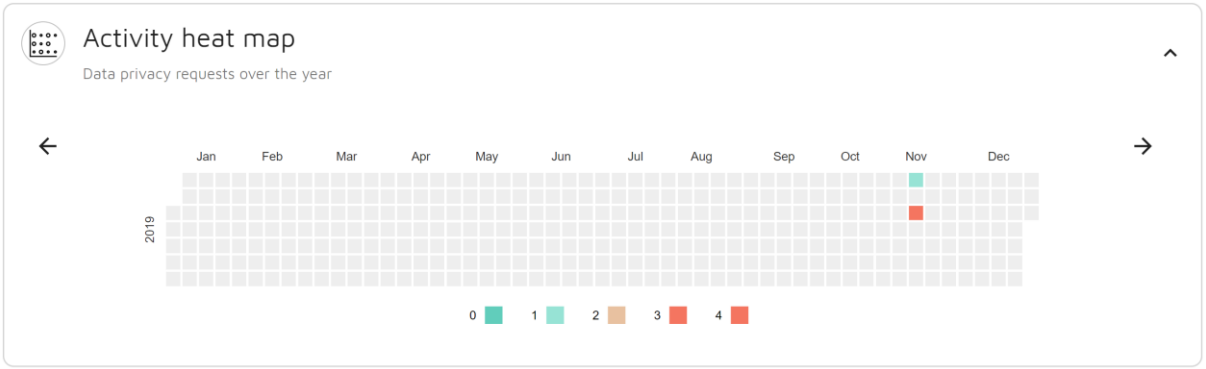

Figure 36: Activity heat map to indicate at which time data subject requests were issued on a more frequent basis.

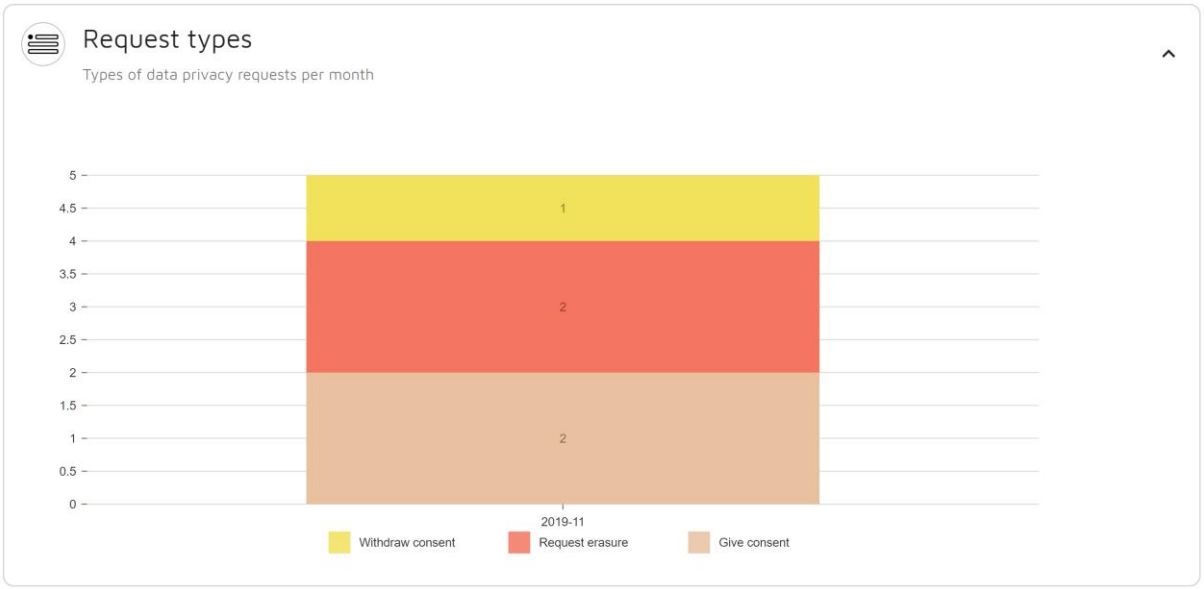

Figure 37: Statistics over the different request types to identify which type of requests were issued more than others.

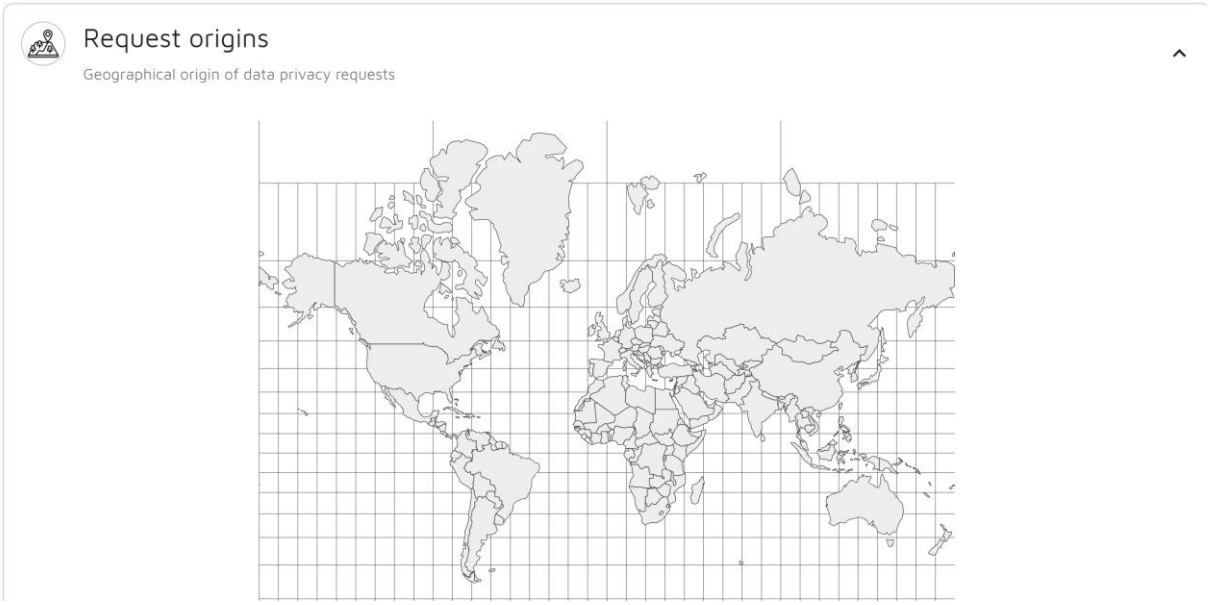

Figure 38: A world map to indicate from which countries requests were issued more than others.

Figure 36 depicts how an activity heat map can show DPOs when how many data subjects requests were retrieved. The arrows left and right offer DPOs to switch between years. This way, trends can be detected and even matched against events related to the company's personal data processing practices. It could answer questions like "Did changing our privacy policy caused more privacy concerns?".

Figure 37 gives statistics over the various request types of data subjects (request to rectification/ erasure/ portability/ etc.), which could offer DPOs and companies in general new insights on privacy-related developments of their customers. Not just the types of requests could be of interest, but also the geographical origin of data subject requests (see Figure 38) as services (Web services in particular) often target an international user group.

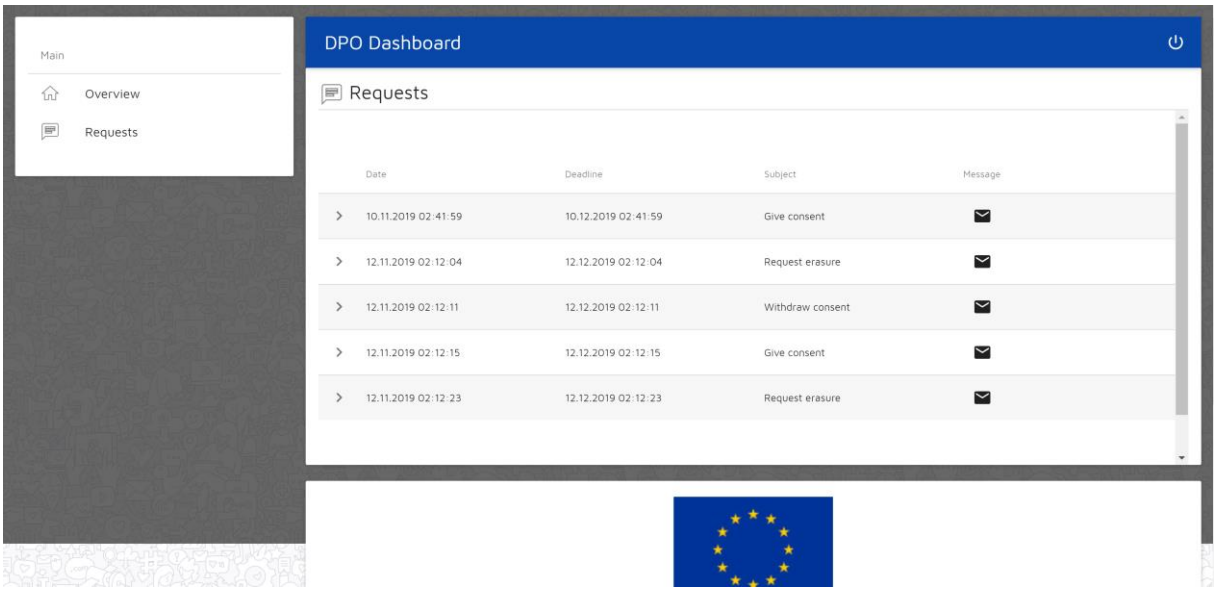

Figure 39: The "Requests" page to visualize the individual requests in a table.

Besides the statistics over retrieved requests, DPOs might be interested in inspecting individual requests. There the “Requests” page lists all retrieved requests in a table. In addition to the basic information (request type, date retrieved, date to respond), DPOs can manually forward the requests to the persons In charge, who are able to process and realize the data subject’s request. However, it is rather foreseen to use an application identifier that maps a request to a certain application (of the controller), so that requests can be directly forwarded to the units in charge. This is in line with the application-centric design approach of the privacy dashboard.

5 Consent engine and feedback mechanism

The developed consent interface prototype designs are presented in this chapter. As stated above, we developed multiple consent interfaces that offer different degrees of control to the data subject. The approaches are presented and discussed individually starting with the privacy plans approach, followed by the customizable consent approach, the broad consent with reduced complexity, and last the dynamic consent approach.

5.1 Broad consent with reduced complexity

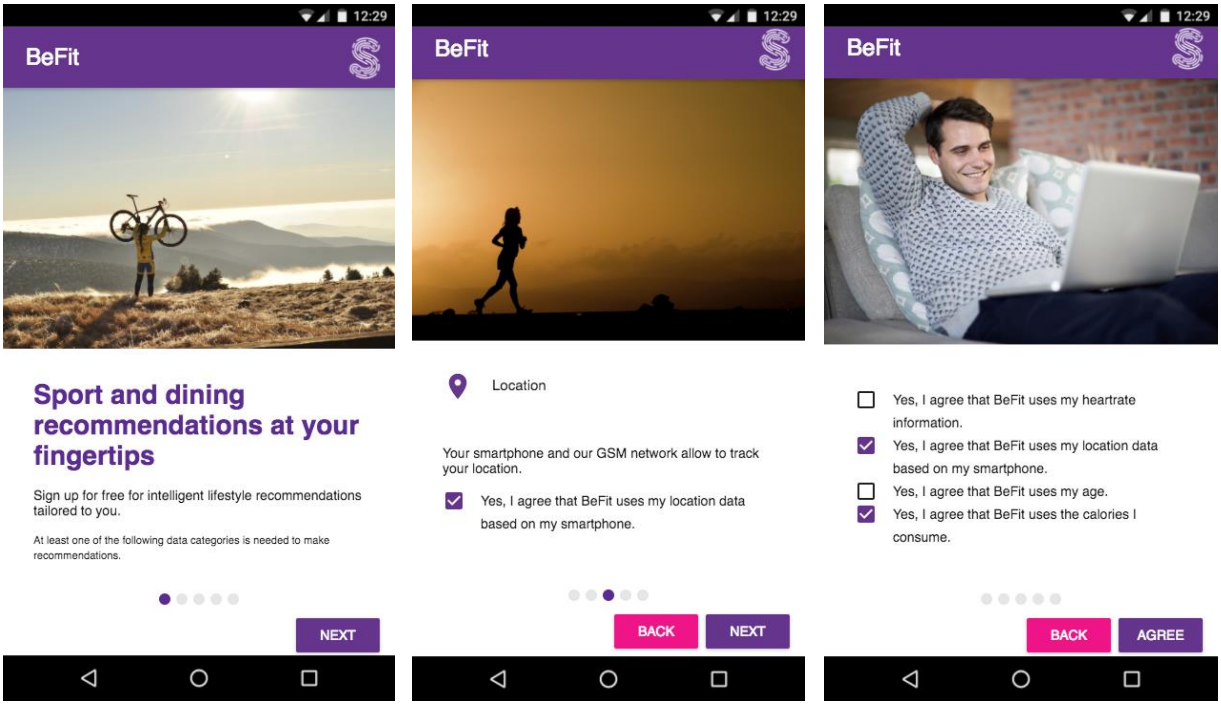

Figure 40: A mobile consent interface guiding data subjects through multiple views, which explain in detail what kind of data is used for which purposes.

This section presents and reports on the activities regarding the concept of broad consent with reduced complexity. Therefore, we first present the results as of D4.1 followed by the results as of D4.3.

5.1.1 Consent interfaces BeFit scenario

Due to today's popularity of mobile devices like smartphones and the changed user interaction mechanisms, the above presented design approaches might not be best suited for these kinds of devices. Furthermore, these approaches are very experimental and break the mental paradigm of users who currently need to agree with a privacy policy by clicking a checkbox. For this reason, this design approach tries to communicate the contents of a privacy policy more efficiently with regard to the length of texts and space that can fit on a screen. Addressing mobile devices in particular contributes to the overall goal to reduce text and complexity of privacy policies to make these more comprehensible and thus more accessible to data subjects. Figure 40 and Figure 41 show two variants of the mobile interfaces both with similar mechanisms to provide the least amount of information possible, while informing data subjects as much as possible.

These interfaces need to undergo an evaluation from a legal perspective and further user studies to evaluate their usability. However, it could be that these interfaces perform rather well since they are closer to familiar consent interfaces. The main challenge therefore in next iterations is to identify the limits of such interfaces. Studies shall reveal how much information can be communicated with these interfaces and at which points are users overwhelmed by the amount of information.

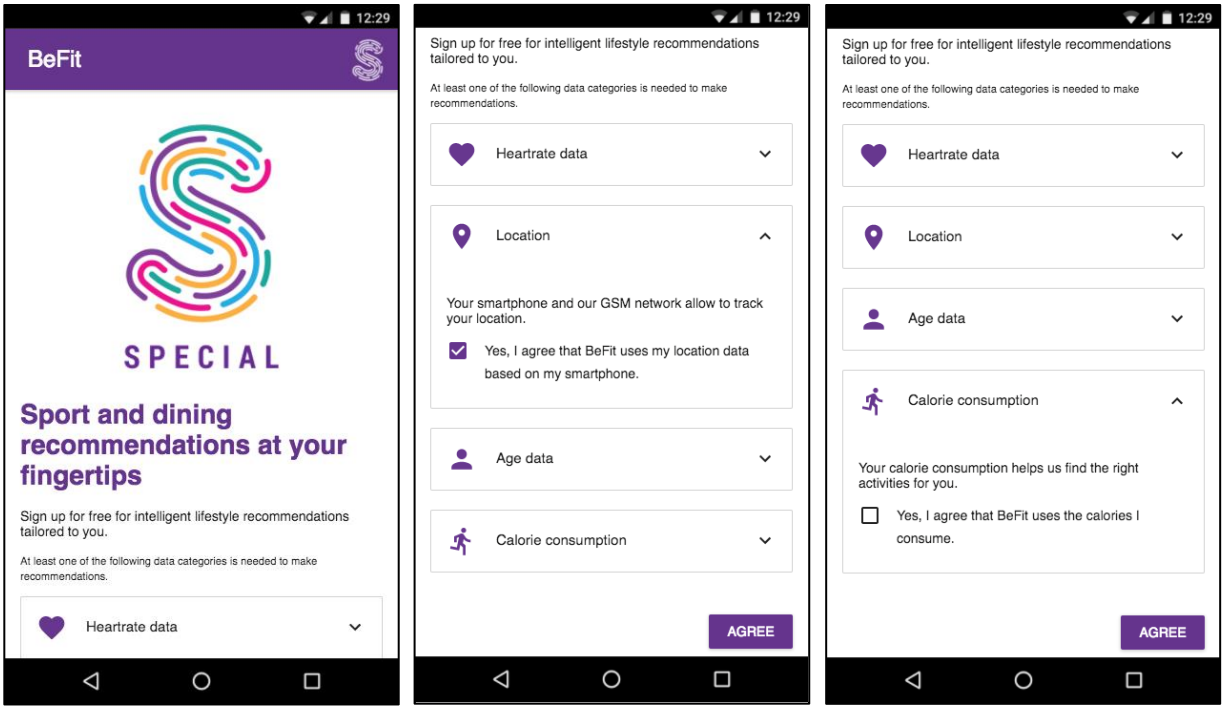

Figure 41: A mobile consent interface consisting of a single view and components that can be clicked or tapped to retrieve more information and to consent to the individual personal data processing practices.

5.1.2 Consent interfaces Proximus use case

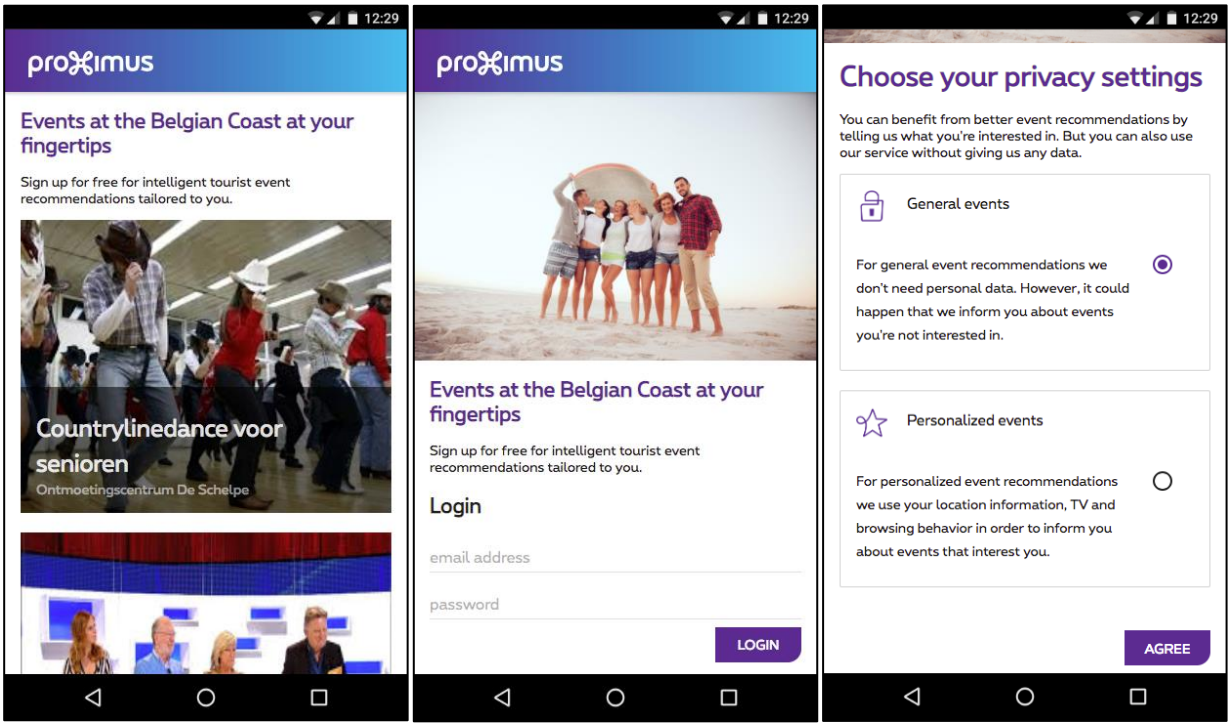

Figure 42: Mobile consent interfaces as of D4.3 developed for the Proximus use case

Since giving consent is a secondary task for the user, the actual service offered to the him or her (the reason the user is asked to give consent) needs to be addressed in the interface design and considered in the evaluation of these user interfaces. For this reason, a start screen was developed, which displays actual events around a certain location (e.g. the user's location). By clicking on one of those (indicating interest) the user asked to sign up for the service including giving consent.

Here, the options offered to the user were reduced. Besides the approach to give consent for each data category (see Figure 41), the user shall be primarily able to configure whether he or she wants to retrieve personalized event recommendations or not. This way, an almost anonymous usage of the service is possible. Users who desire personalized events currently cannot make further adjustments, however we will combine the two versions giving users a third option (e.g. **custom personalization**), which enables them to give consent for each data category as in Figure 41.

5.2 Dynamic consent

In this section, we describe our first prototype for the dynamic consent interfaces. This current state of the prototype covers the notice phase at the moment. However, we plan to address the other phases with our next release. Figure 43 shows the first two screens the user is presented with. They are supposed to explain the benefits of the service to the user and how and why the service wants to personalize the user experience. Figure 44 shows an example consent request to make the user familiar with the approach and the user interface that is used to give consent. We designed the consent request in a heads-up notification, since it is rather visible, when the smartphone is used, yet disappears rather quickly in case of no user interaction.

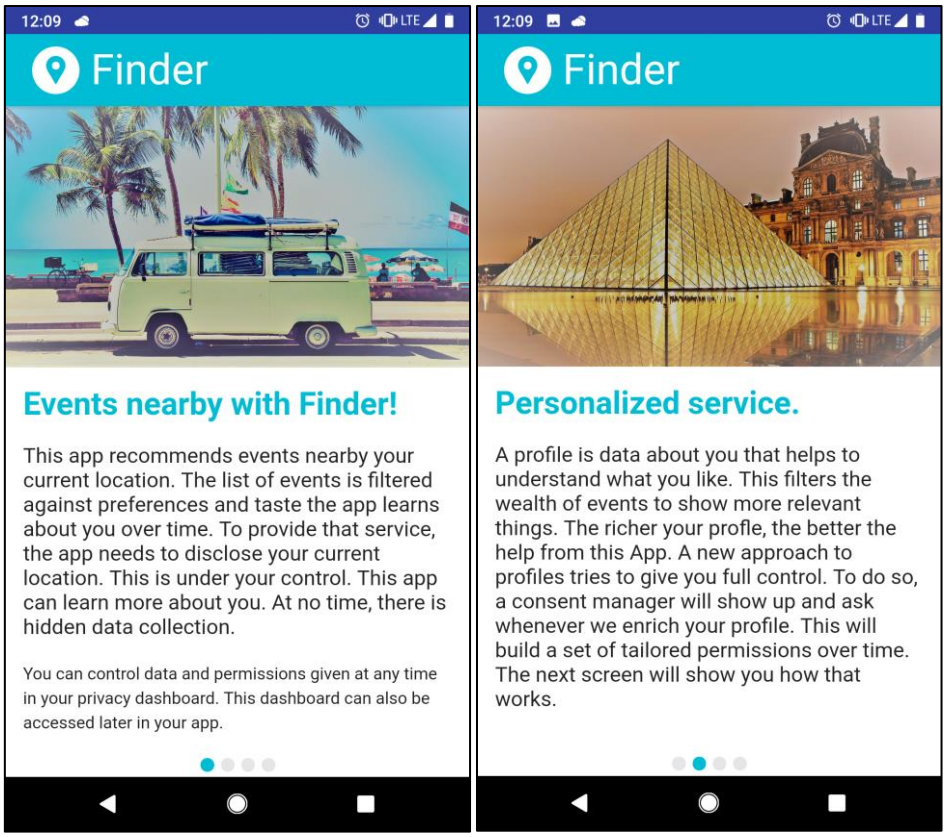

Figure 43: The first two screens of the Finder subscription explain the service and the personalization method.

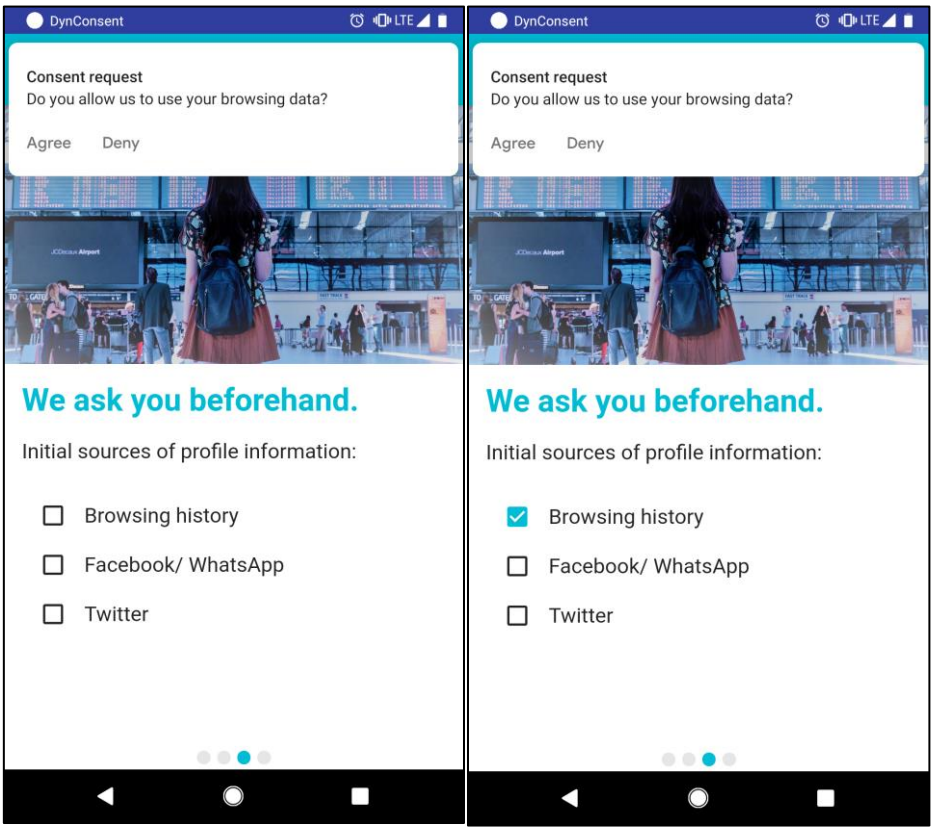

Figure 44: An example consent request is given during the subscription to explain the interface to the user.

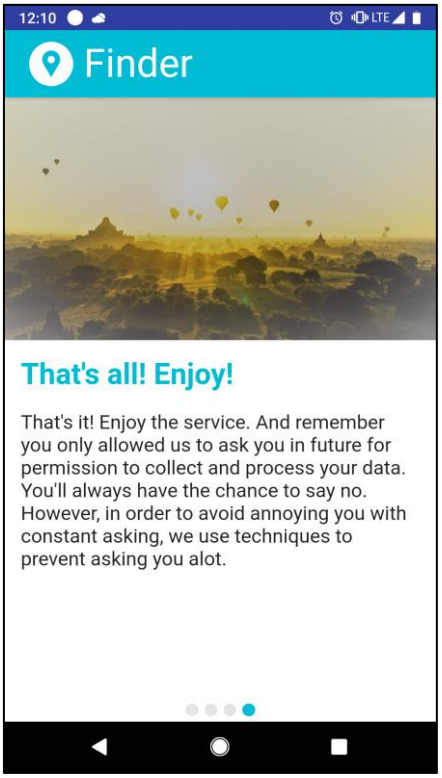

Figure 45: At last an explanation of the next steps is given to the user.

In Figure 45, the last screen of the service subscription is depicted. After the user has been made familiar with the dynamic consent approach, the set-up is completed. Afterwards the user is regularly asked by the consent engine for consent. In the final release, we will include a fully working prototype of the dynamic consent approach, which covers all three phases.

6 Advanced consent request

In this chapter, we first recap the GDPR requirements regarding informed consent, then we provide details about our exemplifying use case scenario from **D1.3 Policy, transparency and compliance guidelines V1.** Following on from this we describe the previous versions of the consent request UI and their usability evaluation results from **D4.2 Usability testing report V1**, **D4.3 Transparency dashboard and control panel release V2** and **D4.4 Usability testing report V2**. At the end of the section, we provide information about the fourth consent request prototype and how it was evaluated by the participants of the usability testing.

6.1 Introduction

Before discussing the fourth and the fifth versions of the consent request prototype and their usability evaluations, let us recall the requirements of the GDPR concerning informed consent and the use case scenario that our prototypes are based on (see **D1.3 Policy, transparency and compliance guidelines V1**), the functionalities of the previous prototypes and their usability evaluation results.

6.1.1 GDPR requirements

In the GDPR the processing of personal data is prohibited via Art. 6 except for some predefined scenarios (e.g.: public interest[18], legal obligations[19], etc.) and when the data subject has consented[20] to his or her personal data processing. According to Art. 4, the consent of the data subject should be: (i) freely given; (ii) specific; (iii) informed and with unambiguous indication of the data subject's wishes; (iv) given by a clear affirmative action by which he or she signifies agreement to the processing of personal data relating to him or her[21]. Although it is highly dependent on the concrete use case, the main information that must be presented in the consent request to the data subject is:

Data. What data (data categories) are processed?
Purpose. What is the purpose of data processing?
Processing. How are the data processed?
Storage. Where and for how long are collected data stored?
Sharing. With whom are the data shared?

6.1.2 Use case scenario

For the development of our consent request prototypes we used the exemplifying use case scenario introduced in **D1.3 Policy, transparency and compliance guidelines V1**:

> *Sue buys a wearable appliance for fitness tracking from BeFit Inc. She is presented with an informed consent request, comprised of a data usage policy that describes which data shall be collected, why they are collected, how they will be processed, stored and shared*

[18] GDPR art. 6(1)(e)
[19] GDPR art. 6(1)(c)
[20] GDPR art. 6(1)(a)
[21] GDPR art. 4(11)

in order to give her fitness-related information.

For the purpose of our research and analysis we made the use case more specific by adding the exemplifying concrete data flow (see Figure 46) where we describe what data are collected by BeFit for what purpose and sub-purpose, where the collected data are stored and for how long, how those data are processed, what data are shared with third parties and what third parties are involved.

We would like to stress that our current use case includes only the initial consent request (i.e., before the data subject starts using the device). This use case could be expanded to include situations where the consent requests are contextualized, incremental and distributed over time (see **D1.6 Legal requirements for a privacy-enhancing Big Data V2**).

6.2 Previous consent request prototypes

6.2.1 First version of the consent request prototype

In **D4.2 Usability testing report V1** we provided a detailed description of the first version of BeFit's consent request prototype (see Figure 47). To make our prototype more suitable for the usability evaluation, we developed a fully functional online version[22]. The online prototype enables participants to give their consent from any place comfortable for them, making our usability evaluation more realistic.

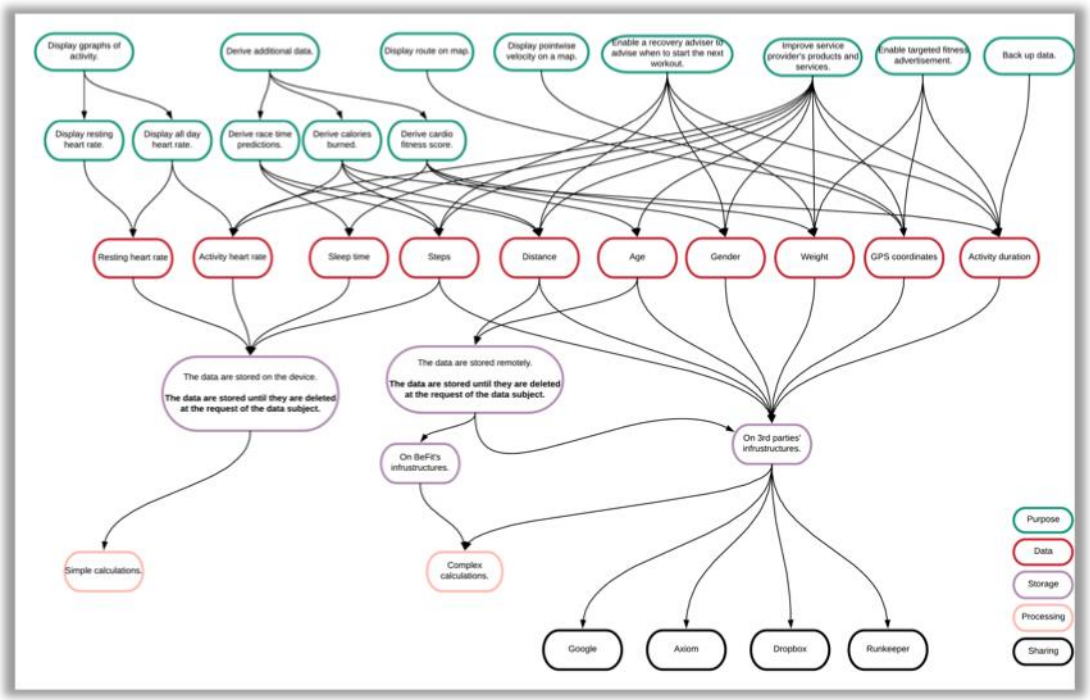

Figure 46: The information that must be presented to the data subject in BeFit's consent request.

While creating this online version we followed Jackob Nielsen's usability heuristics for user interface design[23]. The first prototype provides the following features.

[22] BeFit | Consent Request. https://cr-wizard-en.firebaseapp.com/wizard, last accessed: 13/11/2019.

[23] 10 Heuristics for User Interface Design: Article by Jakob Nielsen. https://www.nngroup.com/articles/ten-usability-heuristics/, last accessed: 06/12/2018.

Categorization. We grouped information according to five categories, namely purpose, data, storage, sharing and processing. This grouping is realized in the form of tabs (see Figure 47 (1)). To support the visualization, in addition to the name of the category on the tab, we added icons for each category.

Customization. The most important feature of our first version of the consent request UI is the full customization of data subject's consent. The user can fully adjust their consent specifically to their wishes. Our consent request gives the possibility to review information or give consent according to five categories mentioned in the categorization feature above. The user is given a possibility to drill down a concrete path and agree only to that path. This means that the data subject can also give permissions to process only specific data categories for chosen purposes, etc. The drill down feature is implemented by placing clickable icons of possible drill-down options near each item in the category/tab list (see Figure 47 (2)). The unique path, created by drill-down process, is displayed and can be navigated in the breadcrumb under the tabs (see Figure 47 (3)). The users give their consent just by selecting checkboxes (see Figure 47 (2)) that correspond to their preferences.

Revocation*.* The user can withdraw their consent by removing the selection in any checkbox at any time.

Understandability. To increase understandability and ease of use of the consent request we are using plain language and standard icons for the content. To help the data subject understand the implications of their consent, our consent request is supported by a graph (see Figure 47 (4)).

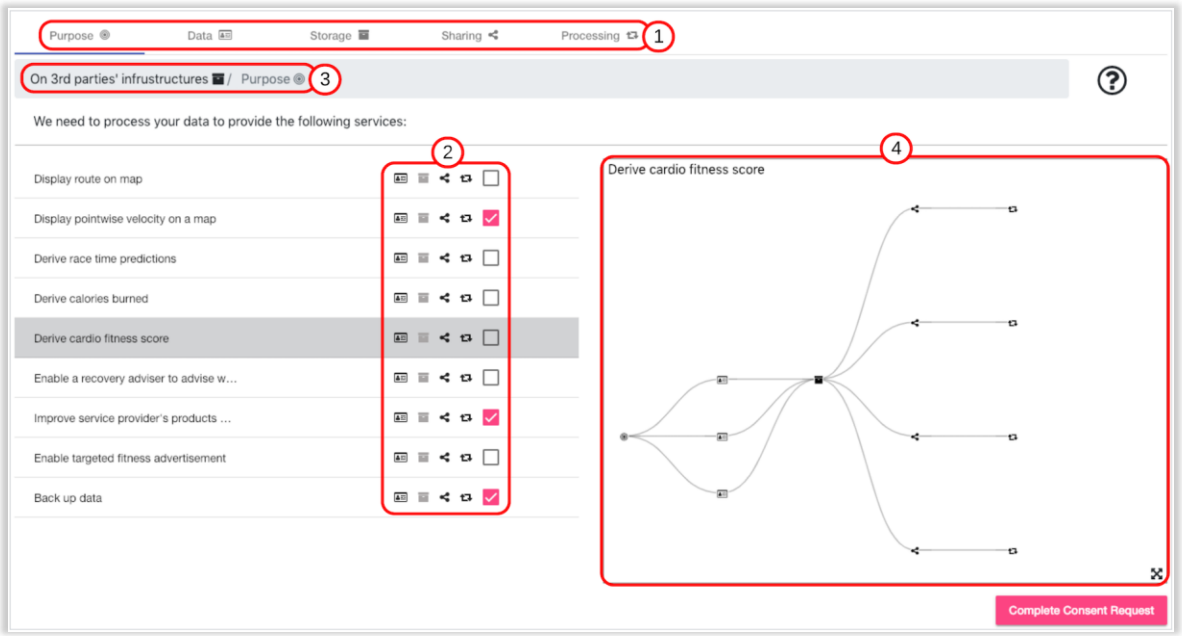

Figure 47: The first consent request UI prototype. (1) Tabs. (2) Drill down. (3) Breadcrumb. (4) Graph.

Summary**.** After users finish consenting (by clicking "Complete Consent Request" button), they are presented with an overview of all the information that they gave their consent to be processed by BeFit.

6.2.1.1 Usability evaluation

We checked the usability of our first UI for consent request by conducting a usability evaluation. For the evaluation we selected a think aloud method (van Someren 1994, Seidman 2006, Charters 2003) where we asked our participants to think aloud when testing the UI and record their screen as well as their spoken thoughts.

Twenty-seven participants, who were between 16 and 35 years old, took part in our usability evaluation. We targeted this segment of the population because the imaginary persona (Sue) in our use case was a student and the first UI was developed considering our persona.

Before the actual UI testing, the participants were asked to imagine themselves buying BeFit's wearable appliance for fitness tracking. As a second step they were presented with BeFit's instructions. After the participants read the instructions, they were asked to activate the device and give their consent for the processing of their data by BeFit. When the participants clicked the "Activate" button, they were redirected to a short user guide. Then the participants were forwarded to the application prototype for the actual testing. In the beginning the participants completed a set of predefined tasks of giving and withdrawing consent. After this exercise, the participants were asked to just give their own consent, as they would have done this, if they bought the BeFit smart watch. At the end of the assignment each participant filled in a questionnaire providing us with their demographic data as well as their impression of our consent request UI. The results of the evaluation are described in detail in **D4.2 Usability testing report V1**. The short overview of the results is presented below.

6.2.1.2 Evaluation Results

In general, the participants were overwhelmed with the consent information because they needed to read and understand all the details. When we asked users if they were overall satisfied with the consent request, 44% of the participants reported dissatisfaction (11% - very dissatisfied, 33% - somewhat dissatisfied) with the consent request. 15% of the users remained neutral towards the consent request, 30% were somewhat satisfied and 11% were very satisfied with our UI. However, the question "*how well the consent request meets your needs for privacy policy representation?"* received only 15% of negative answers. Most of the users selected somewhat well (41%), very well (29%) or extremely well (15%) as their answers.

When asked to assess the time it took to give or withdraw the consent, almost half of the participants (48%) answered that it took them *too long* to give or withdraw the consent. 22% selected *too long, but it was worthwhile* as their answer. For the rest of the users it took either *less time* (11%) or about the *right amount* of time (19%).

The users were prompted to select adjectives that they would use to describe the UI they were testing. As we expected a lot of the users (18 out of 27) found the UI *complex* and the whole process *time consuming*. Fifteen participants found the consent representation to be *confusing*. Apart from the negative adjectives, we also received some positive feedback. Nine participants described the UI as being *organized*, eight as *effective*, seven as *innovative*.

When answering open questions, the respondents mentioned that they found the graph functionality very useful and they liked the summary in the end of the process of giving their consent. A lot of the users highlighted that they liked flexibility and customization features. Some participants replied that they liked the readability of the consent. Some users mentioned they found the division of information into tabs very good, because it provided some structure and contributed to understandability.

The participants named four features that were the easiest for them to use, namely the *graph*, the *summary*, *tabs* navigation and structure, as well as giving and withdrawing consent by clicking on *checkboxes*. The hardest part was not to be lost in all the information that was provided to the users. A lot of them mentioned that it was the hardest to keep all the information in mind.

Since a lot of the participants said that they were overloaded with the information, they suggested *shortening* or *simplifying the information* that is presented to the user. Some users suggested simplifying the customization by offering *fewer options* to choose from. The respondents also suggested using *color-coding* for UI simplification.

6.2.2 Second version of the consent request prototype

We developed a second UI prototype taking into account the evaluation results of the first version. Since the graph functionality was well received by the users in our usability evaluation, we decided to use the graph as the basis for our next version of the consent request UI. The second version of the UI is depicted in Figure 48. For the purpose of the second usability evaluation we developed an online prototype with two localizations: English[24] and German[25]. As before, we used Angular Material[26] and D3.js[27] for the front-end development of the online version and Firebase[28], with its real-time database and hosting, for the server side.

The second version of the UI prototype incorporated the following features:

Categorization. The participants of the first UI evaluation liked the categorization of the consent information into purpose, data, storage, processing and sharing in the previous UI, so we kept this categorization in the second version of the UI.

Customization. The users also highly appreciated the customization and the flexibility of the consent request. However, they expressed their frustration with too many options. In our second UI prototype we retained the customization feature, but we reduced the options by presenting users with the list of available device functionalities and providing a possibility to browse just the functionalities by simply clicking on them (see Figure 48(1)). All the data processing that is required for the selected functionality is represented as a graph (see Figure 48(2)) showing the connections between data categories. If the data subject accepts the offered data processing for the functionality, the corresponding functionality is moved from the "Available Functionality" column to the "Accepted Functionality" column (see Figure 48(3)).

Understandability. From an understandability perspective, the participants of the usability testing positively evaluated the way the consent request was formulated. Since they liked the shortness, the plain language and the icons, we reused the consent text from the first version of the prototype. Every user action is backed up by feedback. In the second prototype we added color-coding to the graph (see Figure 48(4)), as it was suggested by many participants in the usability evaluation. A summary feature was also included in the second UI version. The pop-up with a graph-based overview of the data processing, the users consented to, is always available under the "Summary" button.

Revocation. In terms of revocation, our prototype provides the possibility to withdraw consent at any point in time by selecting functionalities in the "Accepted Functionality" column and clicking the "Revoke" button at the bottom of that column.

6.2.2.1 Usability evaluation results

We checked the usability of our second UI for consent request by conducting a usability evaluation. The participants followed the same protocol as in the first evaluation and recorded their screen during the testing. The results of the evaluation are described in detail in **D4.4 Usability testing report V2**. This time we targeted a broader segment of the population and the second UI prototype was evaluated by 73 participants.

Although the UI prototype was very easy to use, as evidenced in the video recordings, when we asked users if they were overall satisfied with the consent request, 39% of the participants reported dissatisfaction (18% - very dissatisfied, 21% - somewhat dissatisfied) with the consent request 36% of

[24] https://concent-request.firebaseapp.com/builder, last accessed: 13/11/2019.

[25] https://consent-request-de.firebaseapp.com/builder, last accessed: 13/11/2019.

[26] Angular Material. https://material.angular.io/, last accessed: 06/12/2018.

[27] D3.js - Data-Driven Documents. https://d3js.org/, last accessed: 06/12/2018.

[28] Firebase. https://firebase.google.com/, last accessed: 06/12/2018.

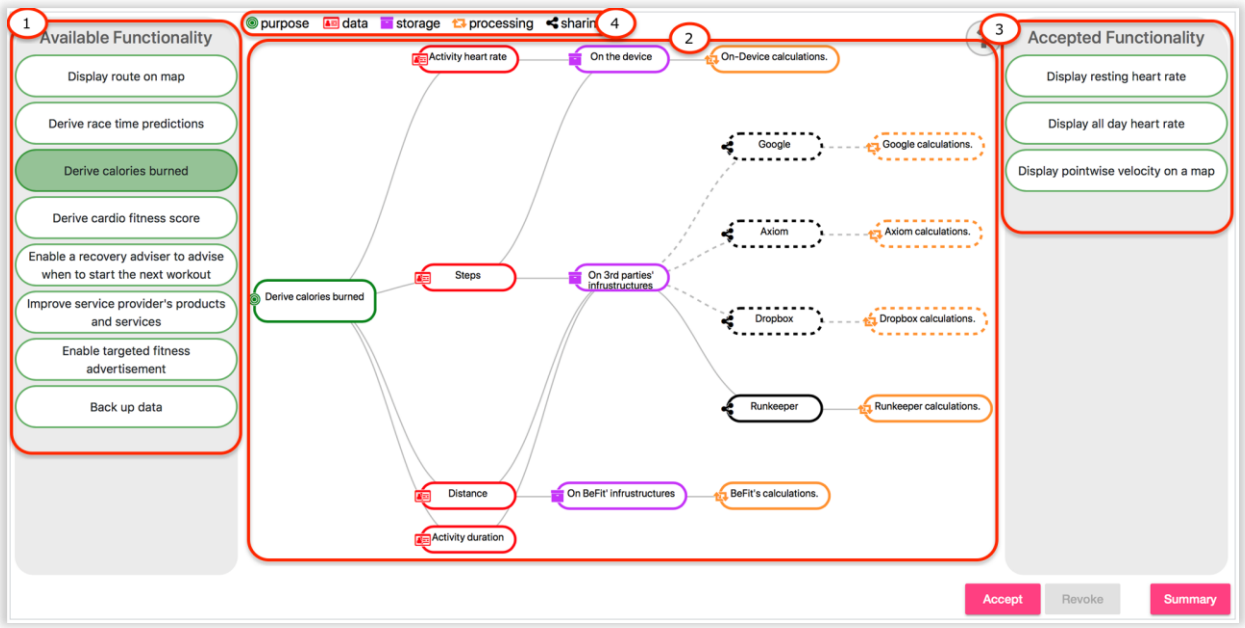

Figure 48: The second version of the consent request prototype. (1) Functionalities to select from. (2) Required data processing for the selected functionality. (3) Accepted functionalities. (4) Color-coding by data category.

the users (31% - somewhat satisfied, 5% - very satisfied) were satisfied with the prototype and 25% of the users remained neutral towards the consent request. Two thirds of the participants liked the UI prototype enough to want to recommend it to their friends. For the 30% of the users it is not likely that they would do so.

The question "*how well the consent request meets your needs for privacy policy representation?*" received 37% (26% - not so well, 11% - not at all well) negative answers. 36% of the participants reported that the way the consent request is presented meets their needs in some way. The others were extremely (7%) and very (20%) satisfied with the representation.

The way the users rated the time they spent on the tasks confirms what we observed in the videos. 38% of the participants were satisfied with the time it took them to complete the tasks and for 15% it took even less than they expected. 19% of the users think that it took them too long, but it was worthwhile. The rest still considered the process to be time consuming.

The users were prompted to select adjectives that they would use to describe the UI they were testing. The users' interaction in the video left a very good impression about the prototype usability. Surprisingly, users still described the prototype as being *confusing* (40%), *annoying* (33%), *complex* (26%), *frustrating* (18%). From the video analysis and questionnaire answers we can infer that this was caused by the absence of bulk consent withdrawal functionality. Users were first confused and then irritated that they had to repeat the same action. On the other hand, for 15% of the participants the UI was *easy to use*, 14% of the respondents considered the UI to be *flexible*, 12% - *innovative*, and 11% - *effective* and *friendly*.

Apart from the single- and multiple-choice questions, our questionnaire contained open questions. Answering those, the respondents named three main points why they liked the second UI prototype better than traditional consent requests. The improved UI is: (i) more understandable, (ii) provides customization, and (iii) provides transparency. The easiest part for the users was to browse the available functionalities. Some of the participants mentioned that the prototype was in general easy to use after one became familiar with the UI. The hardest part was the fact that the prototype did not allow for the withdrawal of consent for multiple functionalities at once, however, this issue can easily be fixed by adding a feature where the users can select the functionalities in bulk. Most of the participants did not suggest any improvements. Some of the participants pointed out that they understood the difficulty of the information visualization for the consent request, however they did

not know how the prototype could be improved. For others everything seemed to work well and the prototype did not need any adjustments.

The evaluation showed that there was still a need to simplify the customization feature even more. In order to address this issue, the consent request UI could be amended such that the functionalities or purposes for data processing are grouped into more general categories and the consent request allows consenting to a general category but still retains a more granular customization as well as detailed overview of the data processing available on demand. We implemented such a version of a consent request in the third iteration and describe this third interactive wireframe in the chapter below.

6.2.3 Third version of the consent request prototype

The third version of the UI, that is depicted in Figure 49, simplifies the customization even more, when compared to the second version, in terms of the information that has to be digested at once by data subjects. For the purpose of the third usability evaluation we developed an online prototype with two localizations: English[29] and German[30]. As before, we used Angular Material and D3.js for the front-end development of the online version. Java[31] and PostgreSQL[32] were used for the server side.

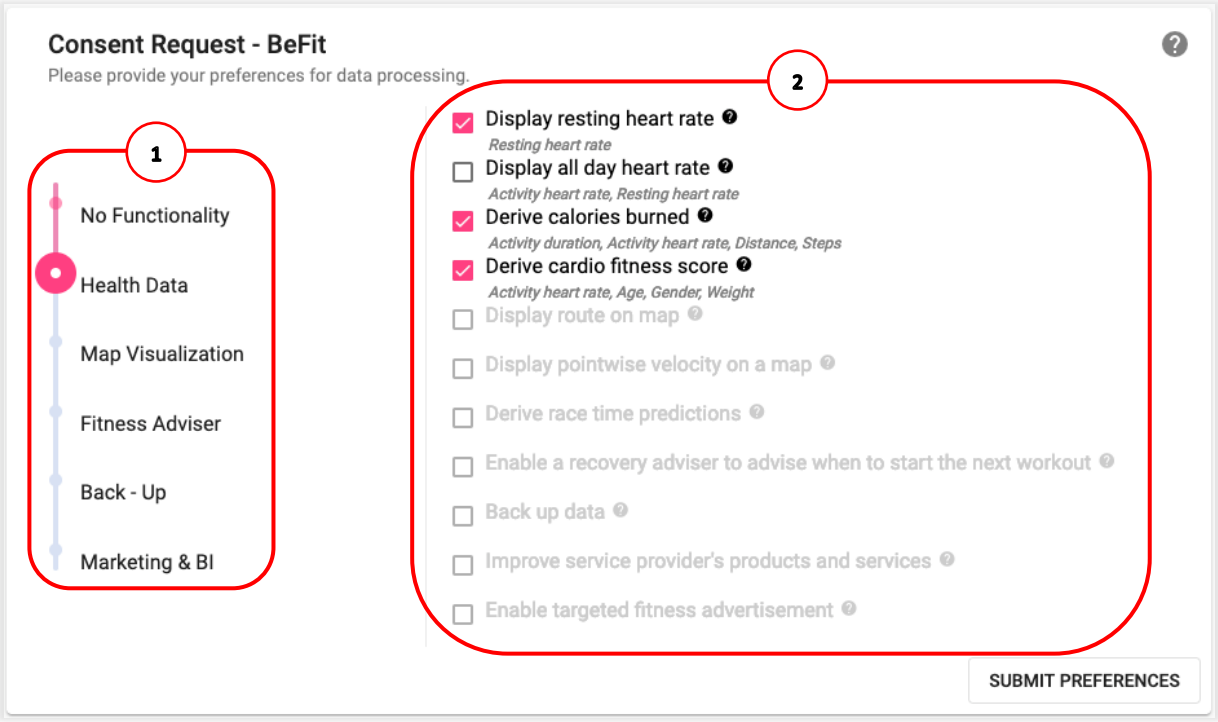

Figure 49: The second version of the consent request prototype. (1) Slider. (2) Consent per purpose.

The third version of the UI prototype incorporated the following features of consent request: categorization, customization, understandability, and revocation.

[29] http://cr-slider.soft.cafe/en/, last accessed: 13/11/2019.

[30] http://cr-slider.soft.cafe/de/, last accessed: 13/11/2019.

[31] https://go.java/index.html?intcmp=gojava-banner-java-com, last accessed: 12/03/2019

[32] https://www.postgresql.org/, last accessed: 06/12/2018.

Categorization. In the third UI version we grouped purposes for data processing into more general categories and allowed users to consent to those general categories by using a slider (see Figure 49(1)). The categories could be ordered from the most popular (according to the company's statistics) at the top to the least popular group of purposes at the bottom. The participants of the first and the second UI evaluations liked the categorization of the consent information into purpose, data, storage, processing and sharing, so we kept this categorization in the third version of the UI in the overview graph.

Customization. The users also highly appreciated the customization and the flexibility of the second version of the consent request. However, they again expressed their frustration with too many options. In the third version we reduced the options by presenting users with the list of more general functionality categories and providing a possibility to browse them by just sliding the pointer up and down. We still retained a more granular customization (see Figure 49(2)), where users could adjust their consent by selecting or deselecting checkboxes near each purpose.

Understandability. From an understandability perspective, the participants of the first and the second usability evaluations positively evaluated the way the consent request was formulated. Since they liked the shortness and the plain language, we reused the consent text from the second version of the prototype. Every user action is also backed up by feedback. For those users, who would prefer a more detailed overview of the data processing, we have the detailed overview available, on demand, upon clicking on "?" near each purpose.

Revocation. In terms of revocation, our prototype provides the possibility to withdraw consent at any point in time by deselecting a correspondent checkbox.

6.2.3.1 Usability evaluation results

We tested the usability of our third UI for consent request by, again, conducting a usability evaluation. The participants followed the same protocol as in the first and the second evaluations. They were thinking aloud and recorded their screen during the testing. Thirty-five participants, who were between 16 and 55+ years old, took part in our usability evaluation.

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. There were no very dissatisfied users and only 9% were somewhat dissatisfied with our UI.

The high overall satisfaction also reflects on the answers to the question about the recommendation of the website with our consent request to a friend. 40% said that it was very likely that they would recommend the website to a friend and 29% replied that it was moderately likely. 11% of the respondents would slightly likely and 3% would extremely likely advise a friend to use a website with our consent request. 17% of the participants would not recommend it to a friend.

When asked to provide their impression of the time it took to give or withdraw the consent, almost 40% of the participants answered that it took them *about the right amount of time* to give or withdraw the consent. 29% selected *it took less time than I thought it would* as their answer. 14% reported that it took *too long, but it was worthwhile.* For the rest of the users (17%), it still took too long to give or withdraw the consent.

The users were asked to select adjectives that they would use to describe the UI they were testing. 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, useful, clear, helpful, usable, effective, organized, satisfying, appealing, efficient* and *flexible*. Eight out of 35 participants still found the UI to be *complex* and time *consuming*.

We asked the participants, if they felt being in control of the processing of their data, when they used our consent request. 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 felt in control. 20% of the participants did not feel that they controlled the processing of their data. There were no users who strongly disagreed.

The graph that provided an overview of the data processing related to a specific purpose was found to be useful to a different extent by 92% of the users. 20% found it extremely useful, 23% - very useful, 40% - moderately useful, 9% - slightly useful. Only 8% of the users did not see usefulness in the graph.

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. Another 26% reported the color-coding to be very useful. This feature was rated as moderately useful by another 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. For the 11% of the participants the icons were not useful.

From the participants' answers to open questions we could derive four main points why they liked the third UI prototype better than traditional consent requests: (i) customization, (ii) detailed overview of the data processing for each purpose, (iii) control over the data processing, and (iv) usability. A lot of users commented that slider on the left side of the UI was the easiest part about using the UI. The respondents also highly evaluated the way the UI is organized. Since users did not have any major problems while using the UI, most of them did not offer any improvements. However, in the participants' videos we noticed that some of the users were in the beginning confused by the disabled checkboxes that belonged to the general categories that were not selected. We tried to solve this issue in the new version of the consent request prototype which we introduce in the following chapter.

6.3 Fourth version of the consent request prototype

The third consent request UI prototype received good feedback from the participants of the usability evaluation. So, we decided not to change the UI completely but to slightly improve that version to eliminate points of users' confusion. The starting page of the fourth version of the consent request UI is depicted in Figure 50. As before, we used Angular Material and D3.js for the front-end development

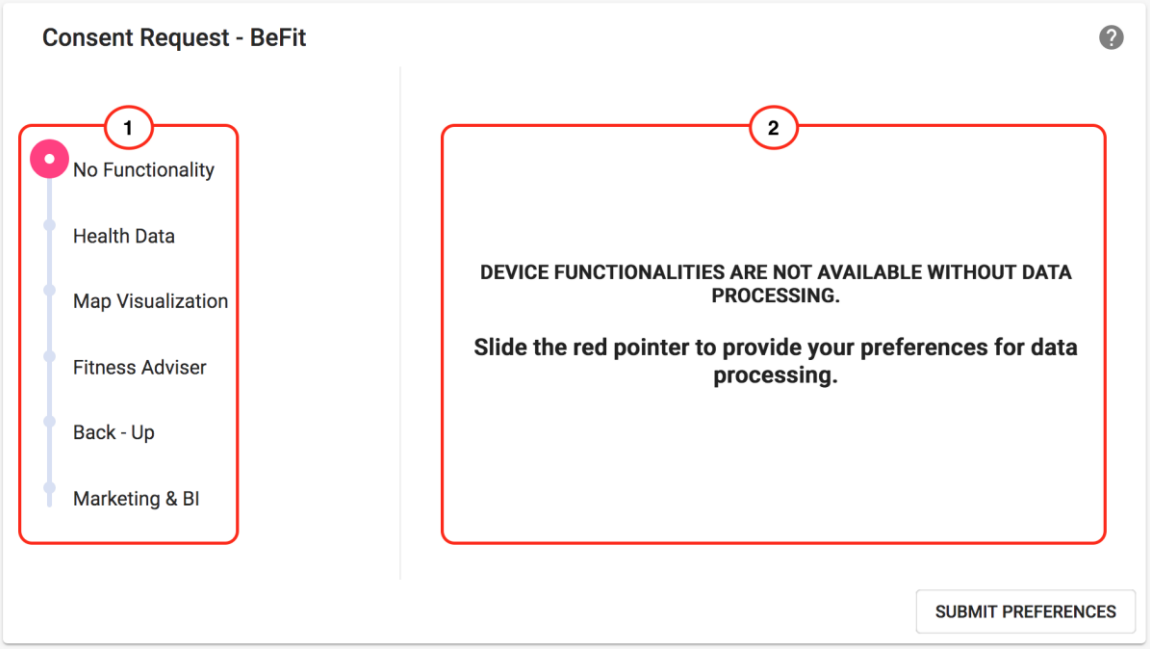

Figure 50: The starting page of the first subversion of the fourth version of the consent request UI. (1) Slider. (2) Message when no consent has been given.

of the online version. Java and PostgreSQL were used for the server side. The fourth version of the UI prototype incorporated the same features of the consent request as the third one: categorization, customization, understandability, and revocation.

Categorization. The purposes for the data processing remained grouped into more general categories and allowed users to consent to those general categories by using a slider (see Figure 50(1)). We preserved the order of the categories from the previous version. The participants of the UI evaluations consistently liked the categorization of the consent information into purpose, data, storage, processing and sharing, so we again kept this categorization in the fourth version of the UI in the overview graph (see **Figure 51**).

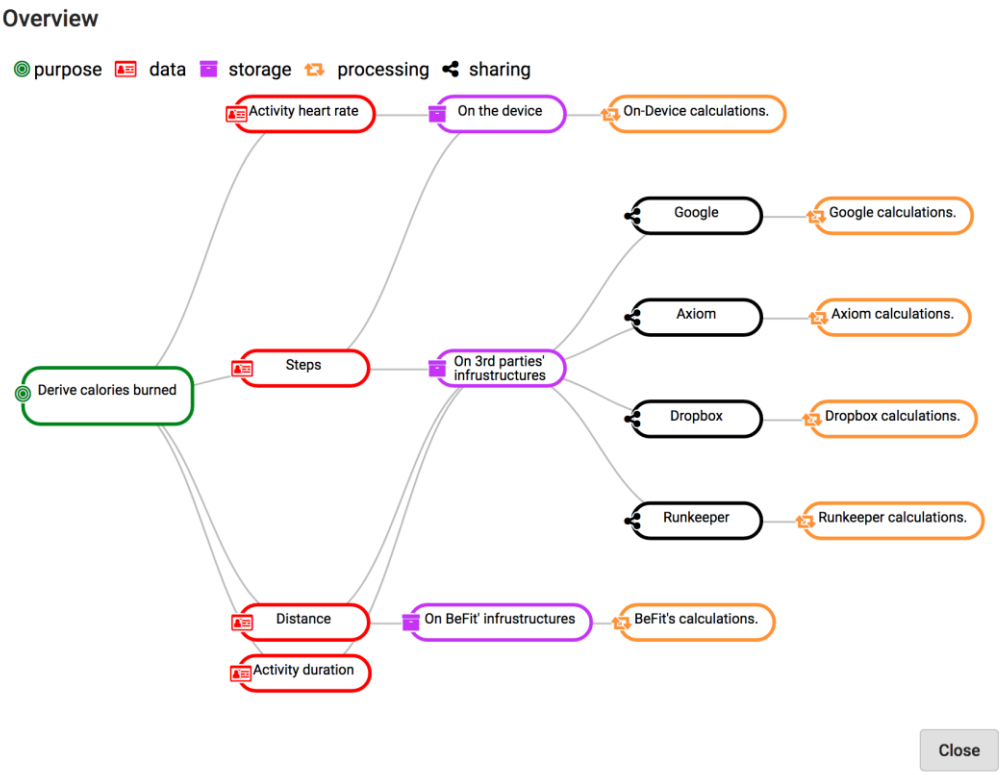

Figure 51: Example of an overview graph for "derive calories burned" purpose.

Customization. We retained the list of more general functionality categories and the possibility to browse them by just sliding the pointer up and down as it was presented in the third version. A more granular customization (see **Figure 53**(1)) also remained the same as in the third version and the users could adjust their consent by selecting or deselecting checkboxes near each purpose. However, we removed the disabled greyed-out checkboxes that were visible for the users in the third version of the consent request and showed only active checkboxes relevant to the selected more general functionality categories. We also updated the starting page of the consent request when no consent has been given yet. In the fourth version we show a message informing users that they should slide the pointer to provide their preferences for data processing (see **Figure 50**(2)) instead of showing the disabled greyed-out checkboxes as was done in the third version. For the purpose of the usability evaluation we created two subversions of the fourth version of the consent request with the same functionality and UI but with different information messages on the starting page. The first one is depicted in **Figure 50**(2) and has already been mentioned above. The second one can be seen in **Figure 52**.

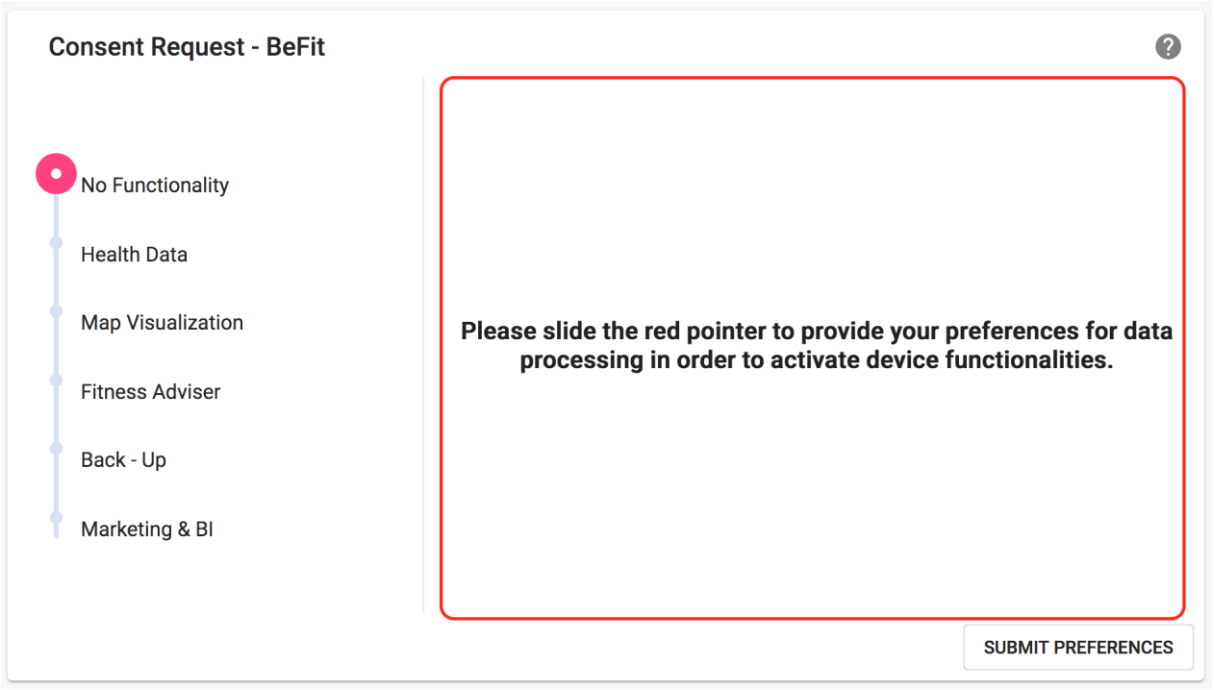

Figure 52: The starting page of the second subversion of the fourth version of the consent request UI - Message when no consent has been given.

Understandability. From an understandability perspective, the participants of all previous usability evaluations positively evaluated the way the consent request was formulated. Since they liked the shortness and the plain language, we reused the consent text from the third version of the prototype. Every user action is again backed up by feedback. For those users, who would prefer a more detailed overview of the data processing, we retained the detailed overview on demand, upon clicking on "i" icon near each purpose.

Revocation. In terms of revocation, our prototype provides the possibility to withdraw consent at any point in time by sliding the pointer up or by deselecting separate checkboxes.

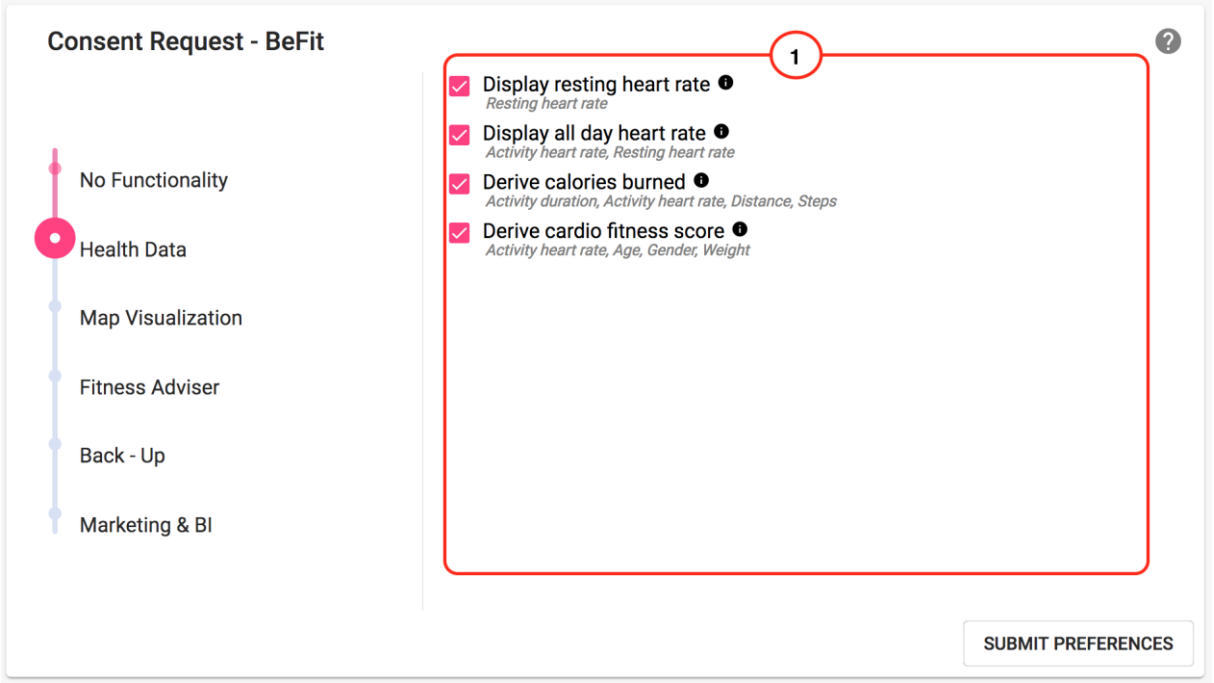

Figure 53: Consent per purpose for the "health data" category.

6.3.1 Usability evaluation

We tested the usability of the subversions of the fourth consent request UI by, again, conducting a usability evaluation. For the purpose of the fourth usability evaluation we developed prototypes with two localizations for both subversions: English[33] and German[34]. The participants followed the same protocol as in the previous evaluations. They were thinking aloud and recorded their screen during the testing. Each participant evaluated one of the two subversions.

6.3.1.1 Task introduction

Before the actual UI testing, the participants were presented with a use case and asked to imagine themselves buying BeFit's wearable appliance for fitness tracking (see Figure 54).

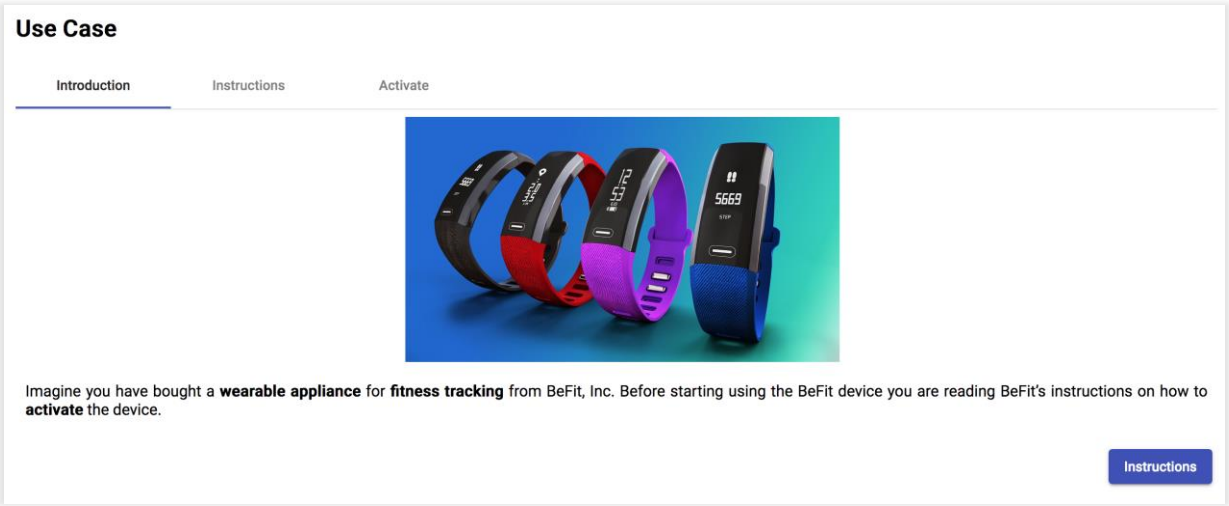

Figure 54: Assignment introduction.

Then, BeFit's instructions (see Figure 55) were shown to the participants.

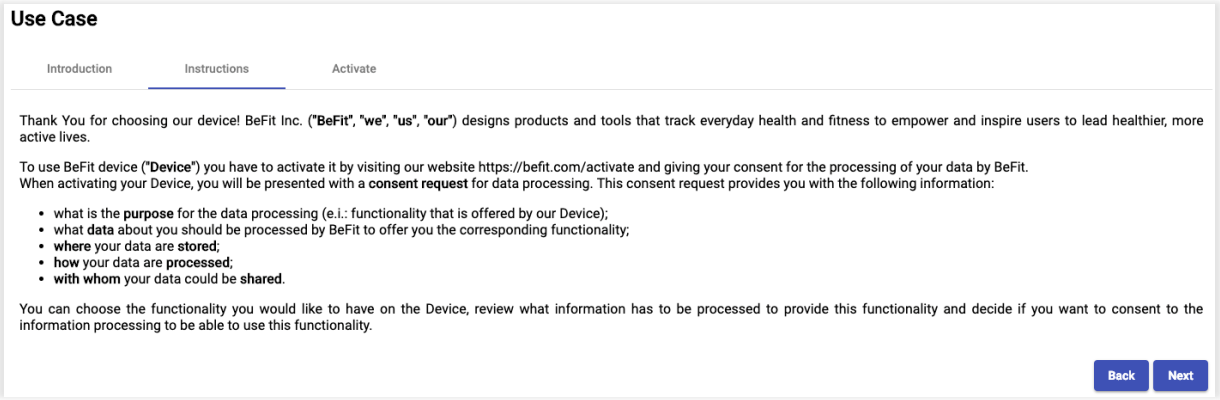

Figure 55: BeFit's instructions.

[33] The English version of the first subversion: http://cr-slider2.soft.cafe/en/qwerty. The English version of the second subversion: http://cr-slider2.soft.cafe/en/ytrewq.

[34] The German version of the first subversion: http://cr-slider2.soft.cafe/de/qwerty. The German version of the second subversion: http://cr-slider2.soft.cafe/de/ytrewq.

After the participants read the instructions, they were asked to activate the device and give their consent for the processing of their data by BeFit (see Figure 56).

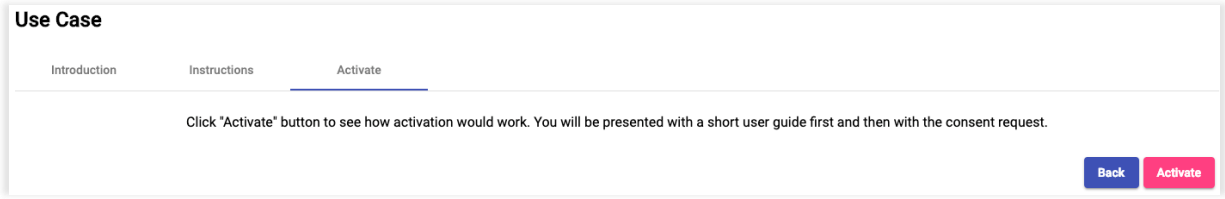

Figure 56: Device activation.

When the participants clicked the "Activate" button, they were redirected to a short user guide (see Figure 57). The user guide explains the functionality and the structure of the application. After reviewing the user guide and clicking "Done" button, the participants were forwarded to the application prototype for the actual testing.

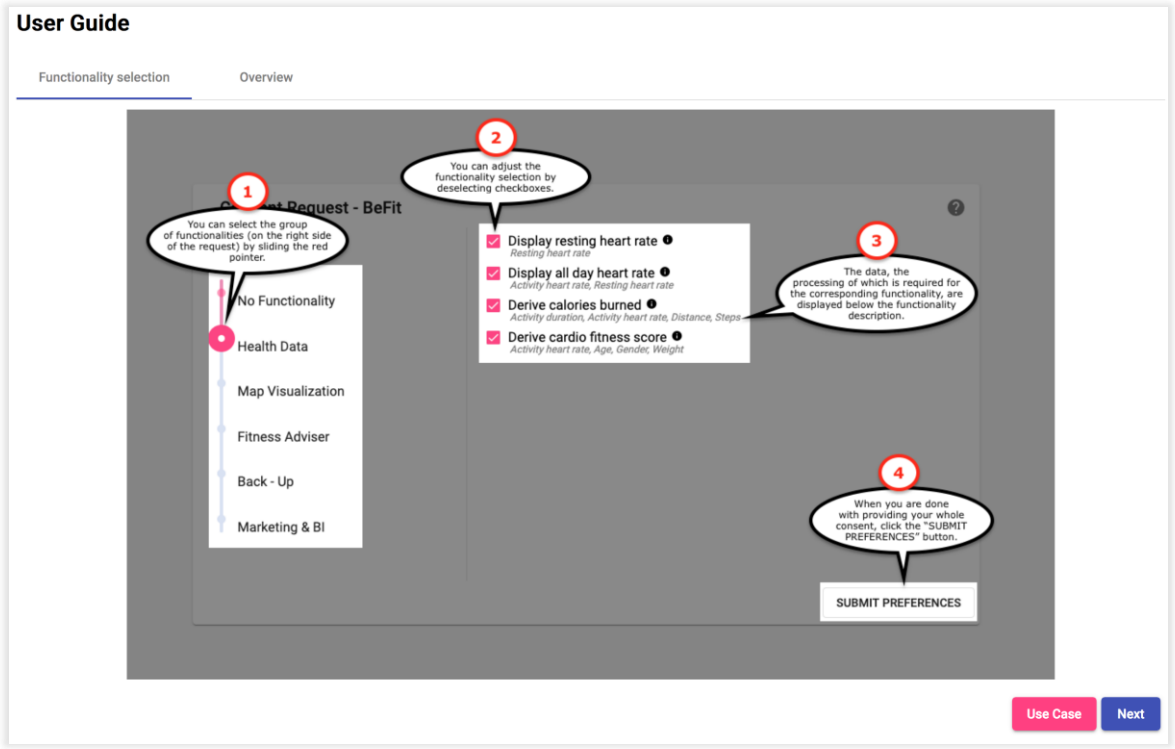

Figure 57: User guide (page "Functionality selection").

6.3.1.2 Testing tasks

In the fourth usability evaluation the users were given the same tasks as in the third usability testing.

1. *Please **give** your **consent**:*
    a. *To process your information to have **health data** on your device.*
    b. *To process your information for your activities to be **visualized** on a **map**.*
    c. *To enable the **fitness adviser**.*
    d. *To turn on the **back-up** of your data.*
2. *Please **withdraw** your **consent**:*

a. *To **derive your cardio fitness score**.*
b. *To **derive your race time predictions**.*
c. *To **back up** your data.*

3. *Please **withdraw** your **consent** to **all** the functionalities.*

Then they were asked to assess the overview (tree) graph functionality.

*Please have a look at the **detailed overview** of the required data processing for the functionality "**display route on map**".*

After this exercise, the participants were asked to just give their own consent, as they would have done this, if they bought the BeFit smart watch.

*Now, that you've got acquainted with how the consent request works, please imagine that you've decided to use the BeFit device and give **your** consent according to **your own** preferences.*

At the end of the assignment each participant filled in a questionnaire where they provided their demographic data as well as their impression of our consent request UI. The questions of both questionnaires can be found in the annexes (see Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**). We discuss the results of the usability evaluation in the following section.

6.3.2 Evaluation Results

6.3.2.1 Evaluation results of the first prototype subversion

Fifteen participants (53% - female, 47% - male) took part in our usability evaluation. The users belong to different age groups (53% - 16 to 25 years old, 27% - 26 to 35 years old, 13% - 46 to 55 years old, 7% - 36 to 45 years old). Almost one third of the participants (33%) graduated from high school. 27% have Bachelor's degree. The other 27% have Master's degree. The rest of the participants (13%) have no degree with some college. 60% of the participants come from Austria. Others come from Bosnia and Herzegovina, Czech Republic, Italy, Hungary, and Montenegro. More details on the demographic data can be seen in Figure 58.

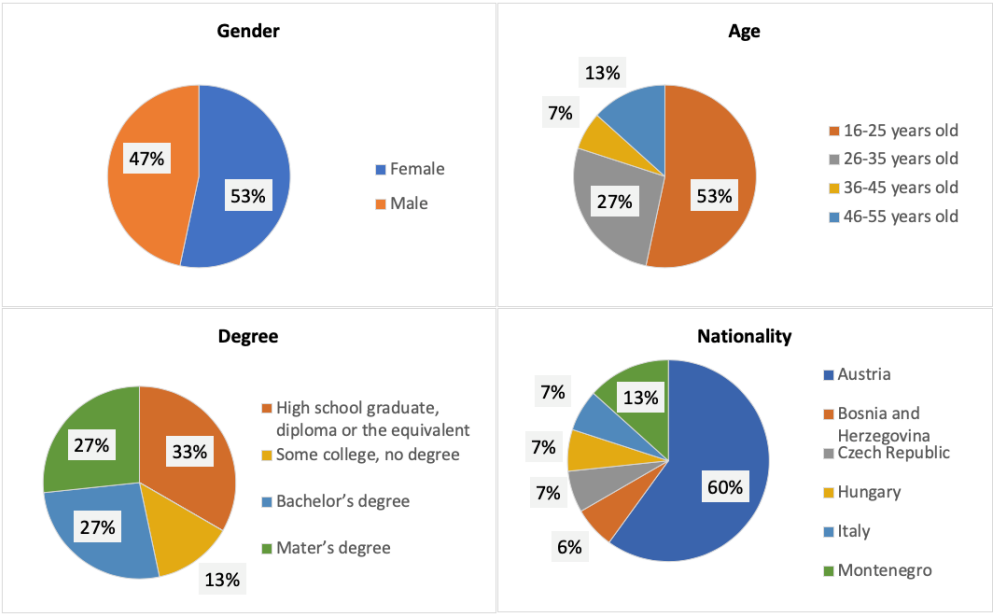

Figure 58: Demographics.

Figure 59 shows that more than a half of the participants rated their Internet surfing skills as competent (53%). 27% consider themselves experts in Internet surfing and 7% are advanced beginners. The

participants reported that they spent 1 - 3 hours (34%), 3 - 6 hours (20%), less than 1 hour (20%), 6 - 8 hours (13%) and more than 8 hours (13%) on the Internet per day and preferably use a laptop (46%), a desktop computer (27%) or a smartphone (27%) for the surfing. As can, also, be seen in Figure 59, almost all participants have no difficulty using computers.

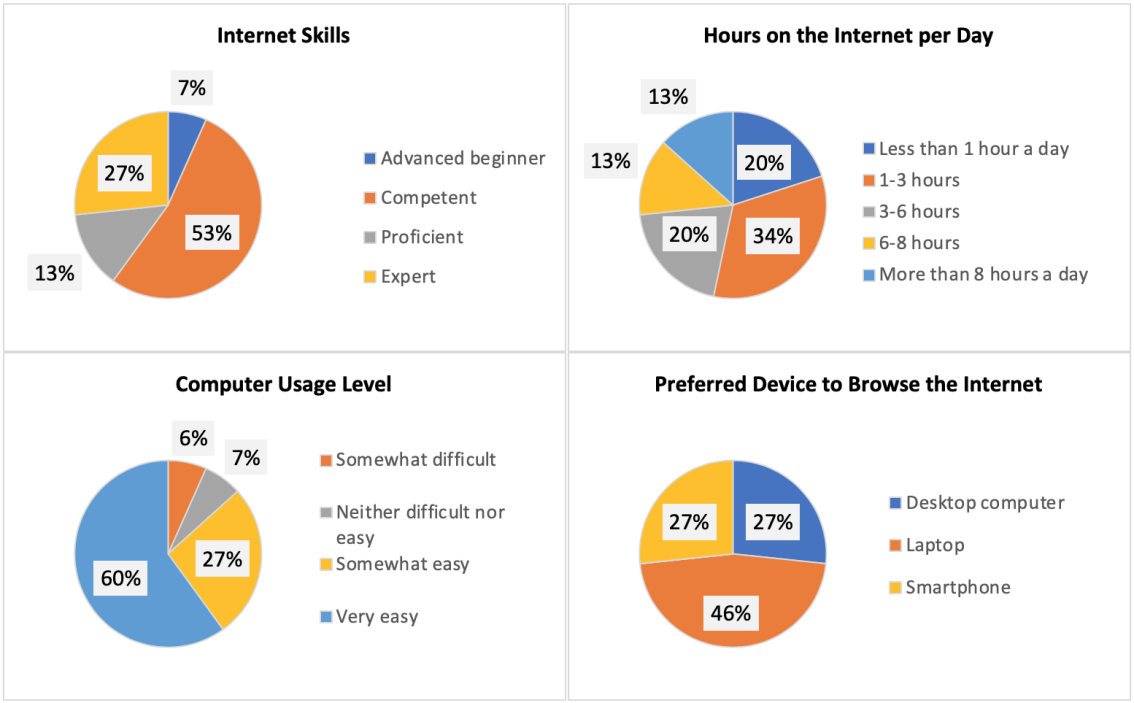

Figure 59: Internet and computer/device usage.

When we asked users if they were satisfied overall with the consent request, 40% of the users remained neutral towards the consent request (see Figure 60). 33% of the participants reported that they were somewhat satisfied with the consent request. 20% of the users were somewhat dissatisfied and only 7% were very dissatisfied with our UI.

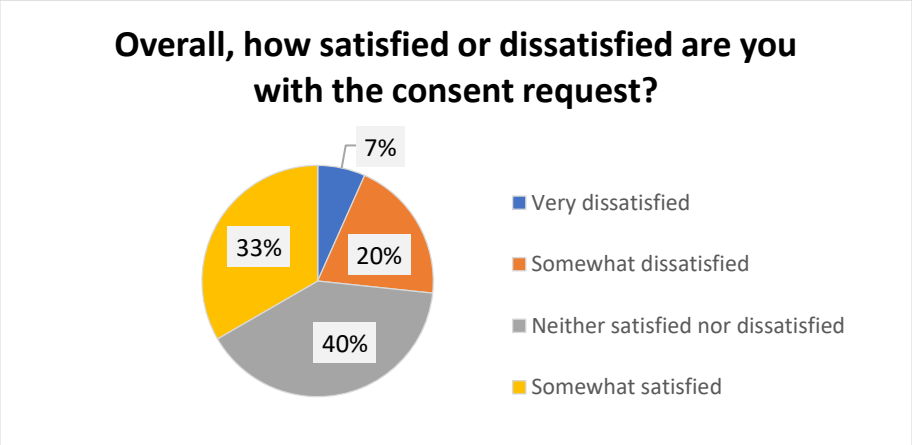

Figure 60: Satisfaction with consent request.

When answering the question about the recommendation of the website with our consent request to a friend 46% said that it was slightly likely that they would recommend the website to a friend and 27% replied that it was very likely (see Figure 61). 20% of the respondents would moderately likely advise a friend to use a website with our consent request. 7% of the participants would not recommend it to a friend.

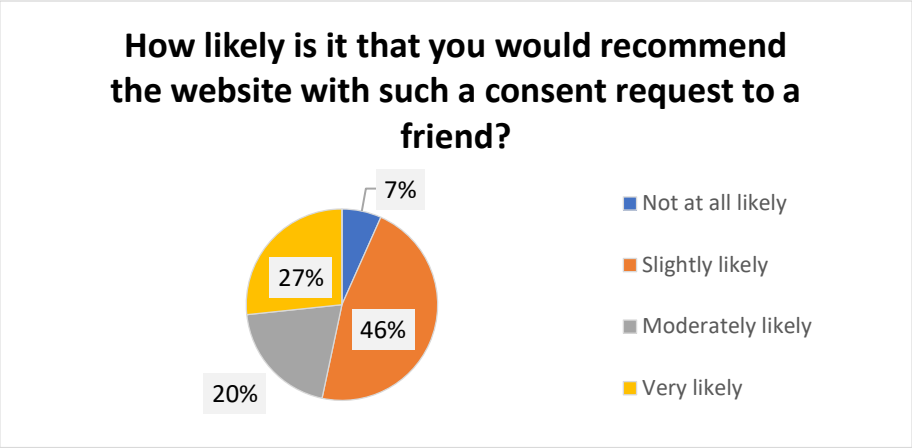

Figure 61: Recommendation of the consent request.

When asked to provide their impression of the time it took to give or withdraw the consent, 47% of the participants answered that it took them *about the right amount of time* to give or withdraw the consent (see Figure 62). 33% selected it took *too long* as their answer. 13% reported that it took *less time than they thought it would.* For the rest of the users (7%), it still took *too long, but it was worthwhile* to give or withdraw the consent.

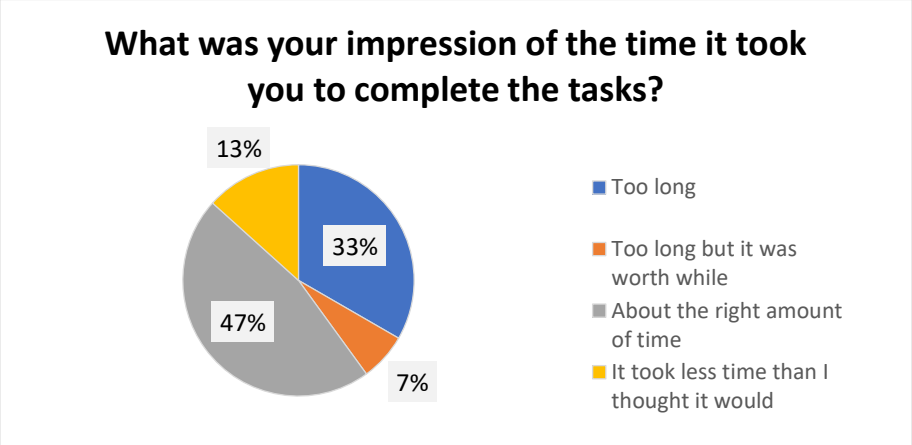

Figure 62: Assessment of the time needed for tasks completion.

The users were asked to select adjectives that they would use to describe the UI they were testing. Here we again used the shortened list of adjectives from Microsoft Desirability Toolkit, developed by Joey Benedeck and Trish Miner (Benedeck 2002). The adjectives users selected to describe the UI are listed in Figure 63. This time we received a mixture of positive and negative adjectives. The positive adjectives *organized* and *clear* received most of the participants' votes. 27% of the users described our UI as *useful* and *helpful*. Another 27% found the UI to be *time consuming*, *confusing* and *complex*.

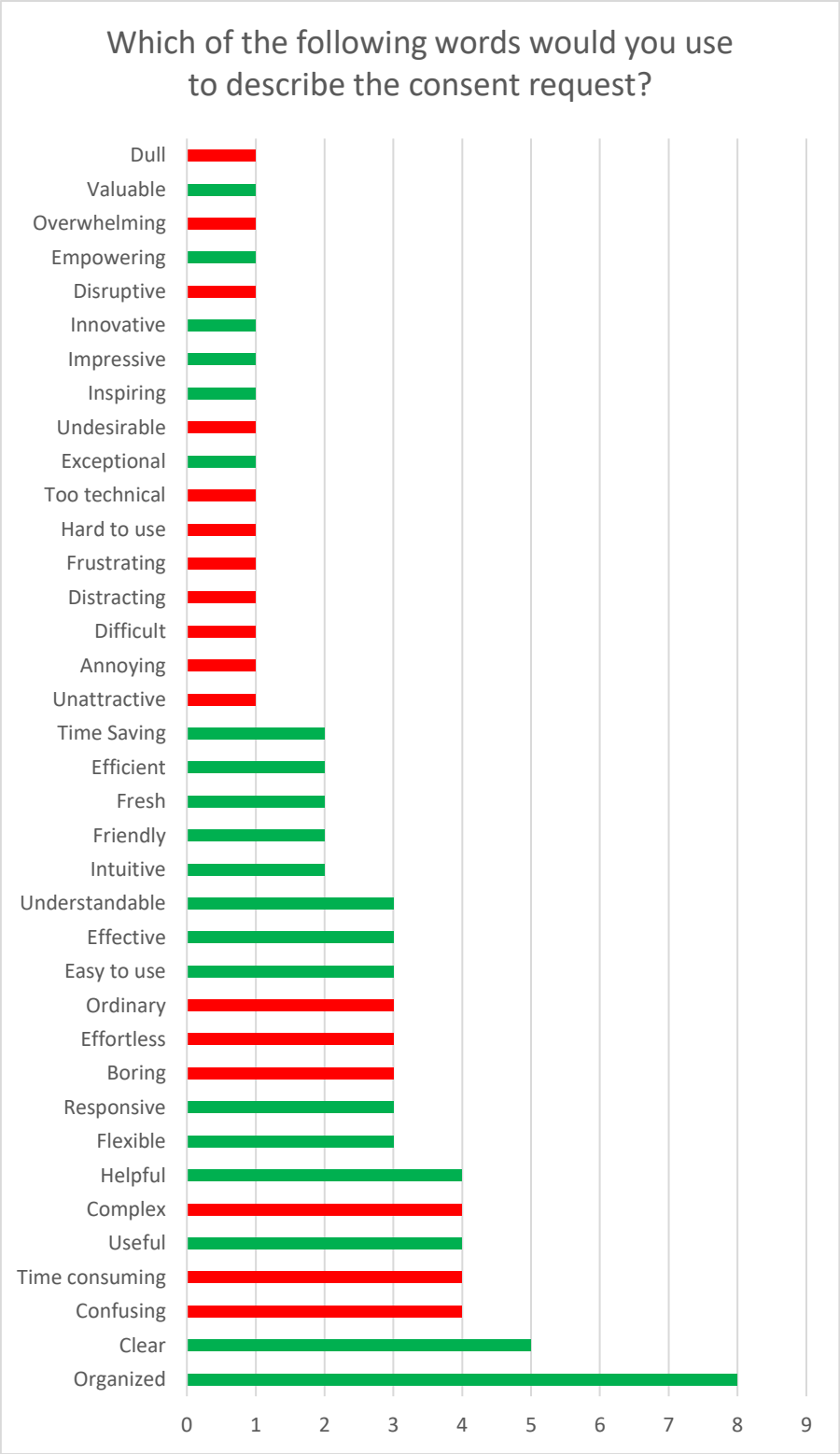

Figure 63: Adjectives that describe the consent request UI.

We asked the participants, if they felt being in control of the processing of their data, when they used our consent request. One third of the participants agreed that such a consent request gave them control over the data processing (see Figure 64). Another one third neither agreed nor disagreed that they felt in control. 27% of the participants did not feel that they controlled the processing of their data. 7% of the users strongly disagreed.

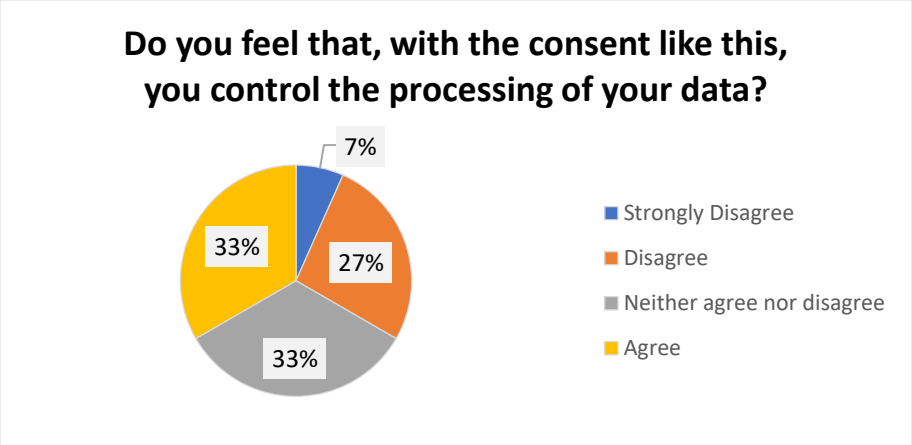

Figure 64: Perception of being in control of the data processing.

The graph that provided an overview of the data processing related to a specific purpose was found to be useful to a different extent by 74% of the users (see Figure 65). 27% found it very useful, 27% - slightly useful, 20% - moderately useful. 26% of the users did not see usefulness in the graph.

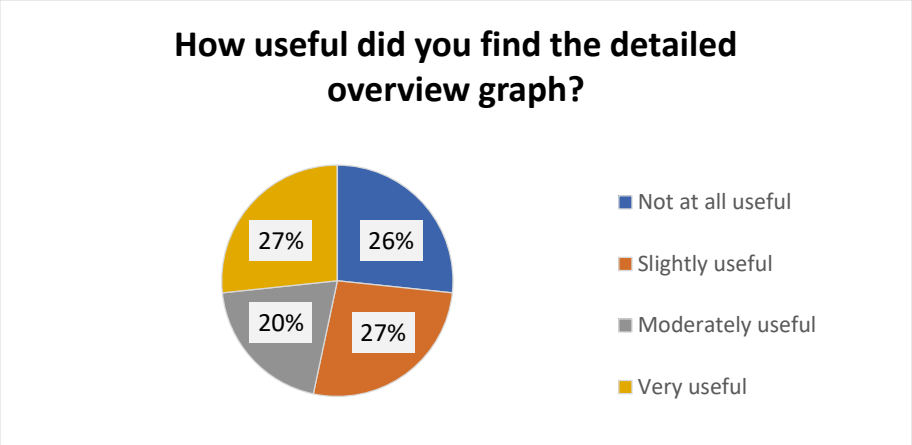

Figure 65: Usefulness of the overview graph.

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. 34% reported the color-coding to be very useful. This feature was rated as moderately useful by 20% of the participants. 13% of the participants found the color-coding to work extremely well in the graph. Another 13% found it to be slightly useful. The rest (20%) did not find color-coding useful. The icons helped 73% of users (40% - moderately, 27% - very, 6% slightly) to understand the graph better (see Figure 66). For the 27% of the participants the icons were not useful.

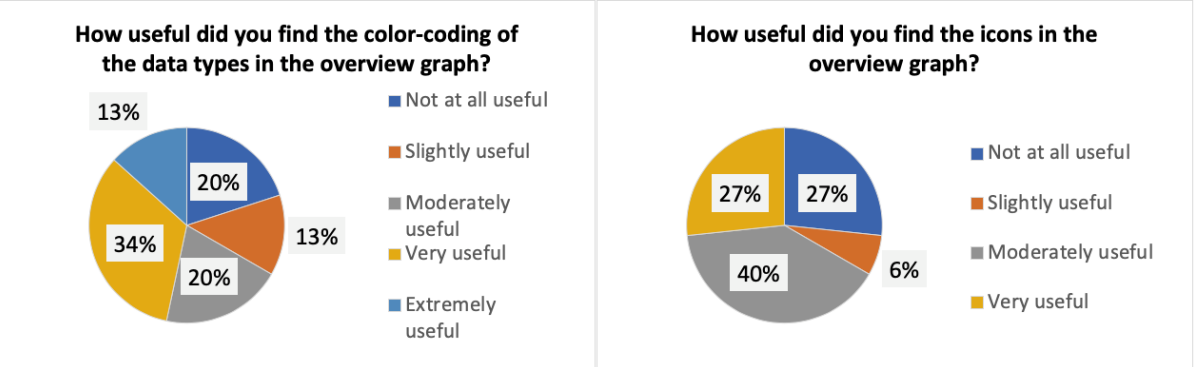

Figure 66: Usefulness of the overview graph features.

The analysis of the answers to the open questions is presented below.

What did you like most about the consent request in comparison to a traditional consent request?

The respondents named four main points why they liked the first subversion and the prototype in general better than traditional consent requests. The improved UI provides: (i) categories (e.g., *"I liked structure of the consent", "…detailed categories provide useful information…", "…clear structure helps a lot…"*), (ii) control over the data processing (e.g., *"…you can manage the consent form"*), and (iii) usability (e.g.: *"it was easy to use and all valuable information was easily accessible", "self-explanatory design", "understandable for the average user"*), (iv) customization (e.g.: *"user has the option to choose their preferences", "…adjusting data processing"*).

What was the easiest and the hardest part about using the consent request?

A lot of the participants highlighted that it was easy to see the information about the data processing (e.g., "*…no difficulty getting information on how your data is processed*") and to understand the graph (e.g., *"…it was the easiest to understand the graph"*). A lot of the participants mentioned that slider and checkboxes were also easy to use, however, one person had difficulty with checkbox depiction in the browser. For another participant it was hard to withdraw his or her consent ("*it was hard to find the right option to withdraw consent*"). For some users it was confusing in the beginning that the data processing near checkboxes belonged to more general categories on the left. However, after they made the connection between general categories and more detailed customization they had no problem using the prototype (e.g., "*after seeing that the checkboxes that were appearing on the right side were sub-categories of the categories on the left, everything was really clear.")*

What could be done to improve the consent request?

The participants suggested to enhance the prototype by adding (i) icons to categories (e.g., *"add some symbols near categories"*, (ii) color-coding (e.g., *"group subcategories using different colors", "make clear that new items appear by using color"*), (iii) enlarge buttons (e.g., *"older adults could benefit from bigger buttons"*). Multiple users suggested adding accelerator in the form of a checkbox to select/deselect all options at once per category (e.g., "*could also use a box that you can check or uncheck to check or uncheck all boxes"*).

6.3.2.2 Evaluation results of the second prototype subversion

Twenty-one participant (62% - female, 38% - female) took part in our usability evaluation. The users belong to different age groups (29% - 16 to 25 years old, 24% - 36 to 45 years old, 24% - 46 to 55 years old, 14% - 26 to 35 years old, and 9% - 55 years old and over). 38% of the participants have Bachelor's degree and 29% have Master's degree. 14% of the participants graduated from high school. The other 14% have no degree with some college. 5% of the participants have a doctorate degree. 52% of the participants come from Austria. Others come from the USA, Germany, Slovakia, Bosnia and Herzegovina, Czech Republic, Hungary, and Romania. More details on the demographic data can be seen in Figure 67.

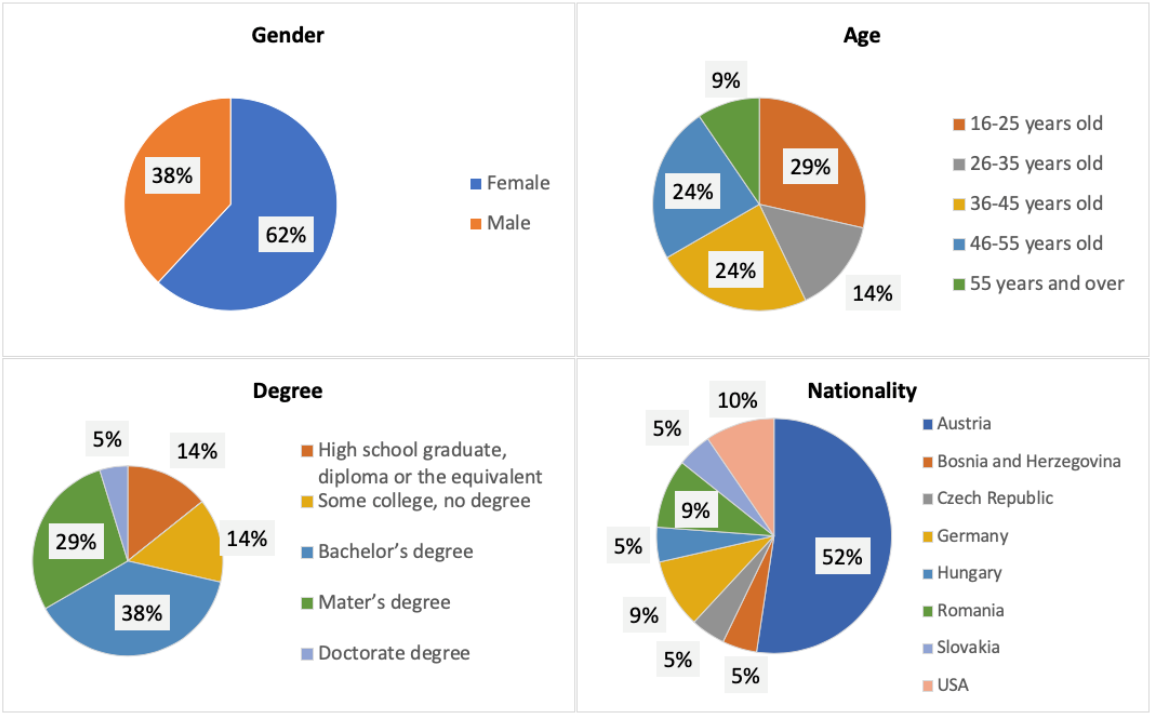

Figure 67: Demographics.

Figure 59 shows that 76% of the participants rated their Internet surfing skills as proficient (38%), competent (24%) and expert (14%). 24% of the participants were advanced beginners. The respondents usually spend 3 - 6 hours (57%) or 1 - 3 hours (38%) on the Internet per day and preferably use a laptop (33%), smartphone (33%) or a desktop computer (23%) for the surfing. As can, also, be seen in Figure 68, almost all participants have no difficulty using computers.

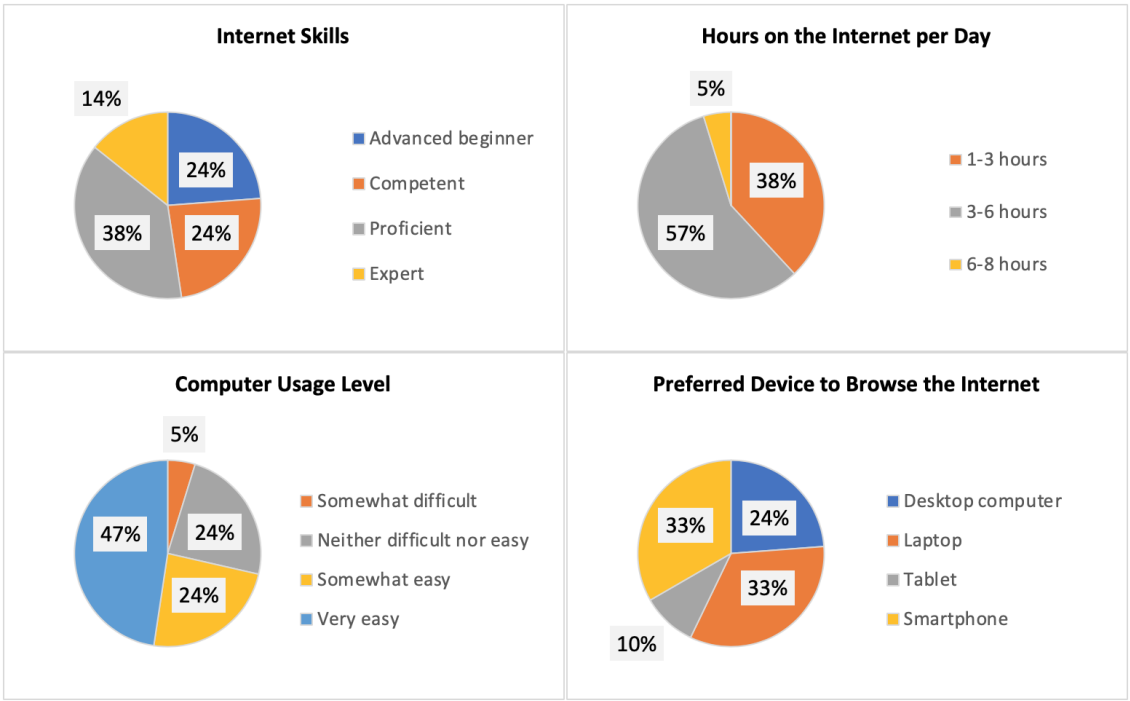

Figure 68: Internet and computer/device usage.

When we asked users if they were satisfied overall with the consent request, 48% of the participants reported satisfaction (29% - somewhat satisfied, 19% - very satisfied) with the consent request (see

Figure 69). 19% of the users remained neutral towards the consent request. Another 19% were very dissatisfied and 14% of the users were somewhat dissatisfied with our UI.

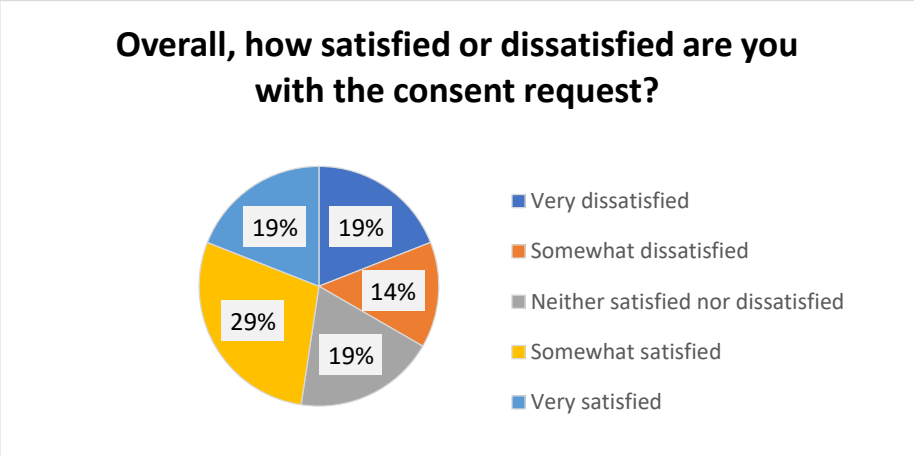

Figure 69: Satisfaction with consent request.

We asked participants if they would recommend the website with such a consent request to a friend. 29% said that it was very likely that they would recommend the website to a friend and 9% replied that it was extremely likely (see Figure 70). 19% of the respondents would slightly likely and 17% would moderately likely advise a friend to use a website with our consent request. 29% of the participants would not recommend it to a friend.

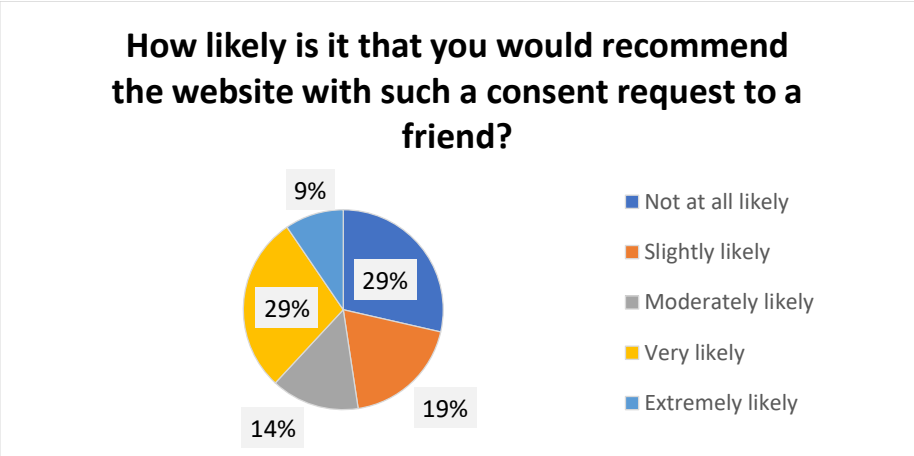

Figure 70: Recommendation of the consent request.

When asked to provide their impression of the time it took to give or withdraw the consent, almost 48% of the participants answered that it took them *about the right amount of time* to give or withdraw the consent (see Figure 71). 33% selected *too long* as their answer. 19% reported that it took *too long, but it was worthwhile.*

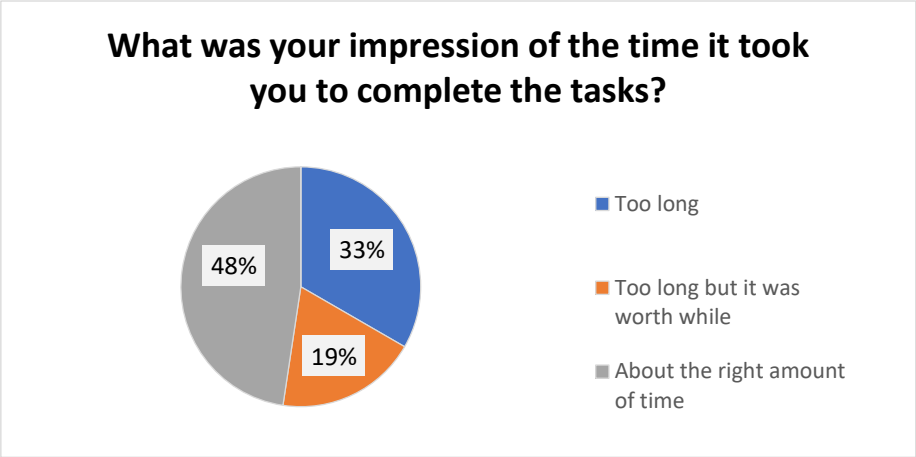

Figure 71: Assessment of the time needed for tasks completion.

The users were asked to select adjectives that they would use to describe the UI they were testing. Here we again used the shortened list of adjectives from Microsoft Desirability Toolkit, developed by Joey Benedeck and Trish Miner (Benedeck 2002). The adjectives users selected to describe the UI are listed in Figure 72. *Easy to use* received most of the participants' votes. Some of the users found the UI *effective*, however, the same amount of users described the UI as *annoying* and time *consuming*. 24% of the users found this UI *intuitive, useful, helpful,* and *efficient*.

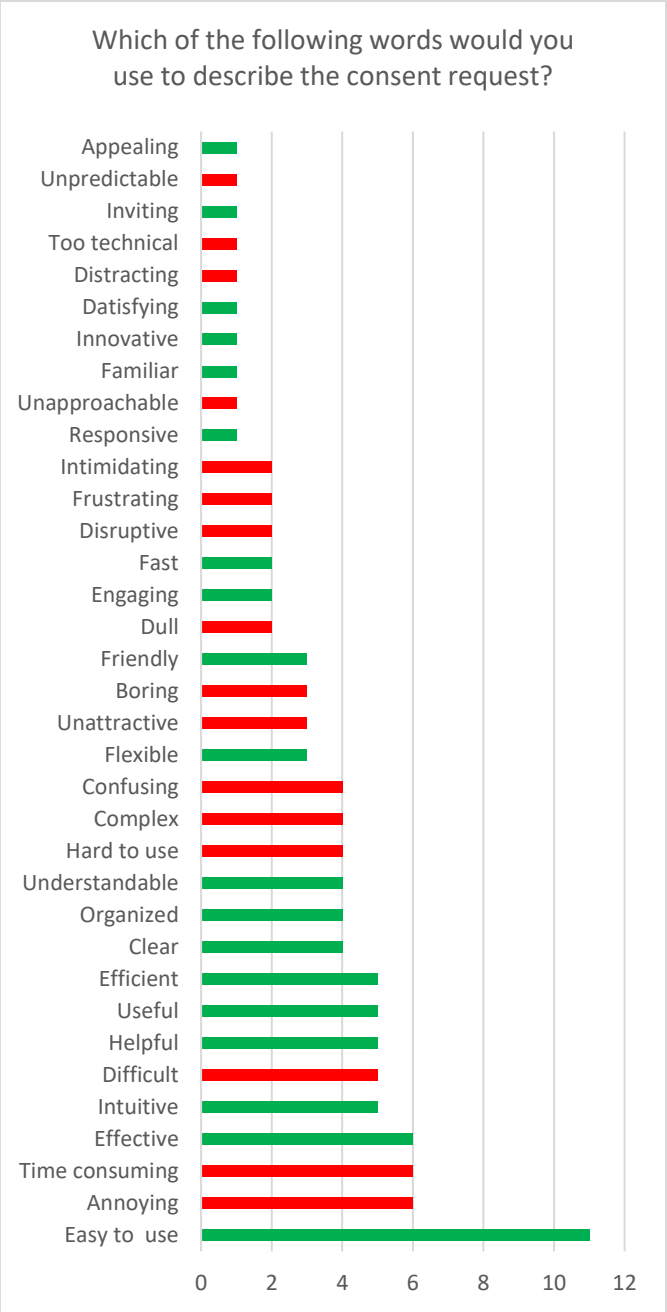

Figure 72: Adjectives that describe the consent request UI.

We asked the participants, if they felt being in control of the processing of their data, when they used our consent request. More than a half of the participants agreed (33% - agree, 19% - strongly agree) that such a consent request gave them control over the data processing (see Figure 73). 5% neither agreed nor disagreed that they felt in control. 29% of the participants did not feel that they controlled the processing of their data and 14% of the users even strongly disagreed that they were in control of their data processing.

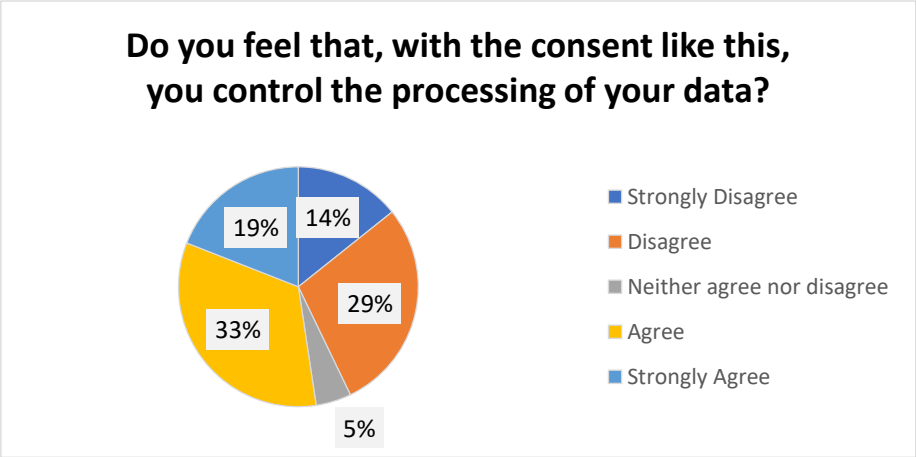

Figure 73: Perception of being in control of the data processing.

The graph that provided an overview of the data processing related to a specific purpose was found to be useful to a different extent by 81% of the users (see Figure 74). 29% found it very useful, 14% - moderately useful, 38% - slightly useful. 19% of the users did not see usefulness in the graph.

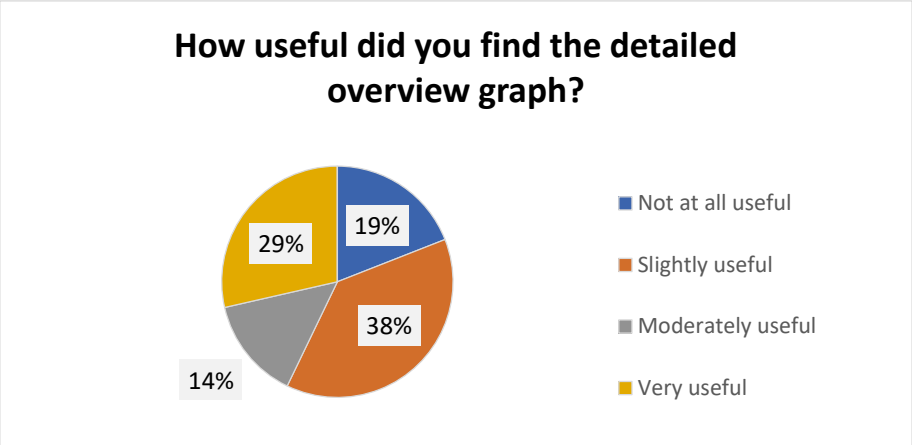

Figure 74: Usefulness of the overview graph.

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. 43% reported the color-coding to be moderately useful. This feature was rated as extremely useful by another 14% of the participants. 10% found it to be very useful and 9% slightly useful. The rest (24%) did not find color-coding useful. The icons helped 86% of users (33% slightly, 29% - very, 19% - moderately, 5% extremely) to understand the graph better (see Figure 75). For the 14% of the participants the icons were not useful.

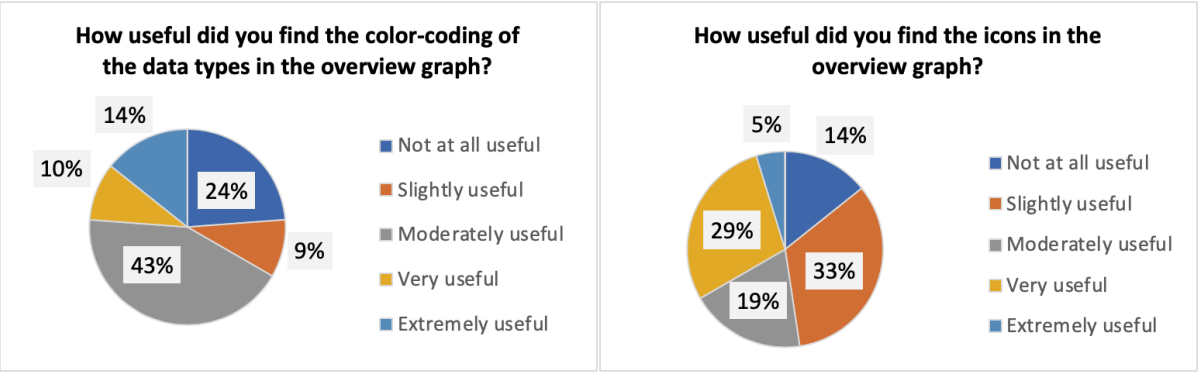

Figure 75: Usefulness of the overview graph features.

The participants that evaluated the second subversion of the prototype answered the open questions similarly to the group that evaluated the first subversion (see Subsection 6.3.2.1). Thus, the respondents did not provide any additional insights in the open-question section of the questionnaire.

7 Conclusions & Future work

This deliverable presents the activities and efforts made within the context of WP4 of SPECIAL during the last three years since the beginning of WP4 in month 9. We mainly addressed the two tasks **T4.1 Transparency dashboard and control panel** and **T4.2 Consent engine and feedback mechanism** which cover the transparency dashboard and control panel and the consent engine and feedback mechanism. We therefore reviewed the proposal to formulate goals the define the scope of WP4 and derived the goal and scope of this deliverable from that. As goals of WP4 we identified functional components such as data access, policy expression and templates, consent management, and breach notification. We identified general requirements for the dashboard like performance, scalability, security, privacy, and usability. This deliverable addressed the functional components data access, policy templates, and consent management focusing on the general requirement usability.

We presented the third and final version of our prototype for the privacy dashboard and elaborated on its design. We presented multiple designs and prototypes for consent interfaces and dynamic consent, which we developed and partially evaluated in user studies during the last 35 months. There, we already highlighted the next steps needed to improve the prototypes with regard to legal and usability requirements.

We plan to further pursue the design and development of the privacy dashboard. Therefore, we created another repository for the privacy dashboard that is meant to be used for continuous development even after the end of SPECIAL. This continuous version of the dashboard be accessed via https://specialprivacy.github.io/Privacy-Dashboard-DEMO/ and the source code is available at https://github.com/specialprivacy/Privacy-Dashboard. This way, we want to use the insights gained within SPECIAL and make them available to everyone.

8 References

1. Biere, C. et al.: PrivacyInsight: The Next Generation Privacy Dashboard. Lect. Notes Comput. Sci. 9857, October, 1–226 (2016).
2. Charters, E.: The use of think-aloud methods in qualitative research: An Introduction to think-aloud methods. Brock Educ. 12, 2, 68–82 (2003).
3. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. Inf. Syst. Res. 17, 1, 61–80 (2006).
4. Lai, Y.-L., Hui, K.-L.: Internet Opt-In and Opt-Out: Investigating the Roles of Frames, Defaults and Privacy Concerns. 2006 ACM SIGMIS CPR Conf. Comput. Pers. Res. 253–263 (2006).
5. Liu, R. et al.: When privacy meets usability: Unobtrusive privacy permission recommendation system for mobile apps based on crowdsourcing. IEEE Trans. Serv. Comput. PP, 99, (2016).
6. Schneier, B.: A Taxonomy of Social Networking Data. IEEE Secur. Priv. Mag. 8, 4, 88–88 (2010).
7. Seidman, I.: Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences. (2006).
8. Solomon, P. et al.: The think aloud method: A practical guide to modelling cognitive processes. (1995).
9. Steinfeld, N.: “i agree to the terms and conditions”: (How) do users read privacy policies online? An eye-tracking experiment. Comput. Human Behav. 55, 992–1000 (2016).

9 Annexes

9.1 Demographic Data Questionnaire

1. **What is your gender?**
   - Male
   - Female
2. **What is your age**
   - less than 16 years old
   - 16-25 years old
   - 26-35 years old
   - 36-45 years old
   - 46-55 years old
   - 55 years and over
3. **What is the highest level of education you have completed?**
   - Some high school, no diploma
   - High school graduate, diploma or the equivalent
   - Trade/technical/vocational training
   - Some college, no degree
   - Bachelor's degree
   - Master's degree
   - Doctorate degree
4. **What is (or was) your field of studies?**
   - Natural and Physical Sciences
   - Information Technology
   - Engineering and Related Technologies
   - Architecture and Building
   - Agriculture, Environment and Related Studies
   - Health
   - Education
   - Management and Commerce
   - Society and Culture
   - Creative Arts
   - Food, Hospitality and Personal Services
5. **On average, how many hours per day do you spend on the Internet?**
   - Less than 1 hour a day
   - 1-3 hours
   - 3-6 hours
   - 6-8 hours
   - More than 8 hours a day
6. **How would you assess your current skills for using the Internet?**

- Advanced beginner
- Competent
- Proficient
- Expert

7. How easy is it for you to use computers?

- Very difficult
- Somewhat difficult
- Neither difficult nor easy
- Somewhat easy
- Very easy

8. What is your preferred device to browse the Internet?

- Desktop computer
- Laptop
- Tablet
- Smartphone

9.2 Usability Testing Questionnaire

1. **What do you remember agreeing to?**
    - Data
    - Sharing
    - Storage
    - Purpose
    - Processing
2. **Overall, how satisfied or dissatisfied are you with the consent request?**
    - Very satisfied
    - Somewhat satisfied
    - Neither satisfied nor dissatisfied
    - Somewhat dissatisfied
    - Very dissatisfied
3. **How likely is it that you would recommend the consent request to a friend?**
    - Not at all likely
    - Slightly likely
    - Moderately likely
    - Very likely
    - Extremely likely
4. **What was your impression of the time it took you to complete the tasks?**
    - Too long
    - Too long but it was worth while
    - About the right amount of time
    - It took less time than I thought it would
5. **Which of the following words would you use to describe the consent request?**
    - Annoying
    - Appealing
    - Boring
    - Clear
    - Compelling
    - Complex
    - Confusing
    - Cutting edge
    - Dated
    - Difficult
    - Disruptive
    - Distracting
    - Dull

- Easy to use
- Effective
- Efficient
- Effortless
- Empowering
- Engaging
- Exceptional
- Familiar
- Fast
- Flexible
- Fresh
- Friendly
- Frustrating
- Gets in the way
- Hard to Use
- Helpful
- High quality
- Impressive
- Ineffective
- Innovative
- Inspiring
- Intimidating
- Intuitive
- Inviting
- Irrelevant
- Old
- Ordinary
- Organized
- Overwhelming
- Patronizing
- Poor quality
- Powerful
- Responsive
- Rigid
- Satisfying
- Slow
- Time-consuming
- Time-Saving
- Too Technical
- Unapproachable
- Unattractive
- Uncontrollable
- Understandable

- Undesirable
- Unpredictable
- Usable
- Useful
- Valuable

6. **How well the consent request does meet your needs for privacy policy representation?**
   - Extremely well
   - Very well
   - Somewhat well
   - Not so well
   - Not at all well
7. **Information on which tab or tabs did you find useful and informative?**
   - Purpose
   - Data
   - Storage
   - Sharing
   - Processing
   - None
8. **Which tab or tabs should be removed because they are useless and overcomplicate everything**
   - Purpose
   - Data
   - Storage
   - Sharing
   - Processing
   - None
9. **How understandable did you find the tree graph?**
   - Not at all understandable
   - Slightly understandable
   - Moderately understandable
   - Very understandable
   - Extremely understandable
10. **How useful did you find the tree graph?**
    - Not at all useful
    - Slightly useful
    - Moderately useful
    - Very useful
    - Extremely useful
11. **What would you suggest to improve the tree graph?**

    Leave a comment

12. What did you like most about the consent request in comparison to a traditional privacy policy?

Leave a comment

13. What's the easiest part about using the consent request?

Leave a comment

14. What's the hardest part about using the consent request?

Leave a comment

15. Was there anything surprising or unexpected about the consent request?

Leave a comment

16. What could be done to improve the consent request?

Leave a comment

17. How easy is the consent request to use?

Leave a comment

18. Which feature (or features) of the consent request are most important to you?

Leave a comment

19. Which feature (or features) of the consent request are least important to you?

Leave a comment

20. What might keep people from using the consent request?

Leave a comment