SPECIAL

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

Deliverable D4.1

Transparency dashboard and control panel release V1

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-M16
Deliverable number:	D4.1
Deliverable title	Transparency dashboard and control panel release V1
Contractual Date of Delivery:	30-04-2018
Actual Date of Delivery:	27-04-2018
Editor (s):	
Author (s):	Philip Raschke (TUB), Olha Drozd (WU), Bert Bos (W3C)
Reviewer (s):	Sabrina Kirrane (WU), Piero Bonatti (CeRICT)
Participant(s):	TUB, WU, W3C, CeRICT
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):	42

Disclaimer

This document contains 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 privacy dashboard that serves as control panel for them to access and assess their private 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 law.

New legal requirements imposed by the European Union's General Data Protection Regulation (GDPR)[1], which comes 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 month nine of the project, i.e. September 2017, and this deliverable is written and submitted in month 16 of the project, i.e. April 2018. It documents our efforts taken during these eight months to fulfil the tasks **T4.1 Transparency dashboard and control panel** and **T4.2 Consent engine**

[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)

and feedback mechanism. During that time, we developed a first prototype for the dashboard that was evaluated within a first user study and multiple consent interfaces that currently evaluated via multiple user tests.

The remainder of this document is structured as follows: in Chapter 2 the objectives and overall scope of WP4 are discussed, followed by a description of the scope of this deliverable. In Chapter 3 concepts are presented and discussed. Subsequently, Chapter 4 presents the developed prototype of the dashboard, and the chapters 5 and 6, which present multiple approaches for consent interfaces. Finally, a summary and conclusion are given including an outlook on the planned next steps.

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 this deliverable will be defined.

2.1 Overall scope of WP4

Figure 1 depicts a mind map of the *so-called* **transparency dashboard and control panel** (in the following only ***dashboard*** or ***privacy dashboard*** for simplicity reasons) 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.

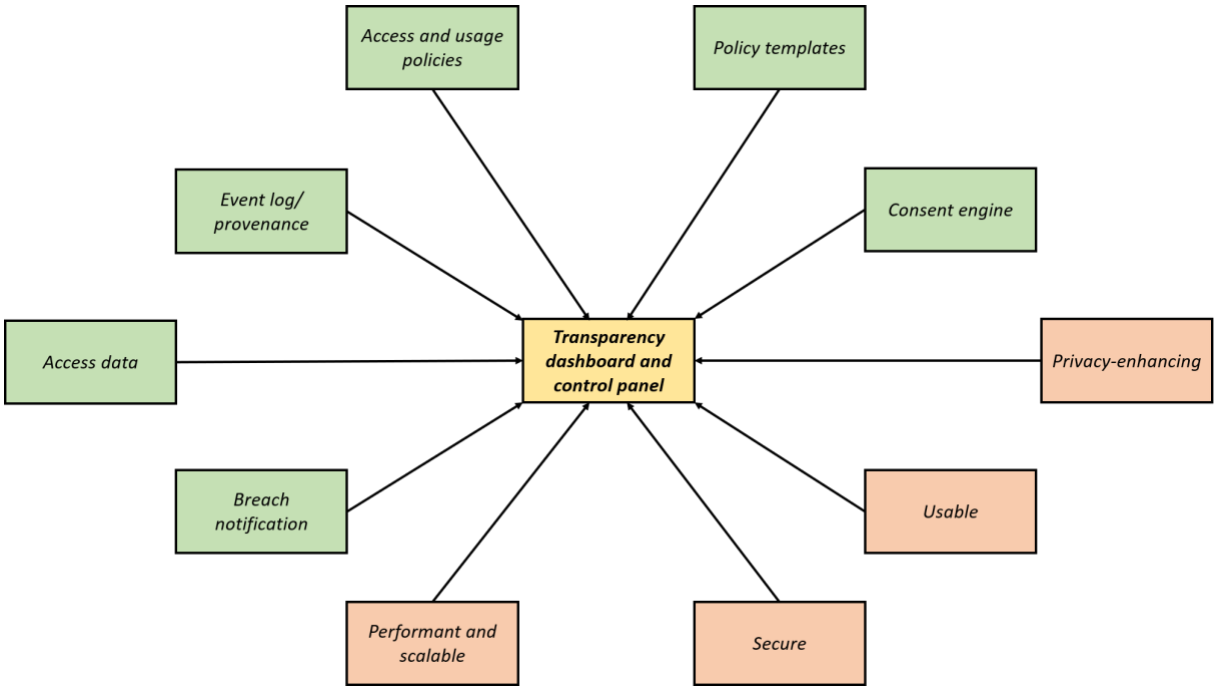

Figure 1: A mind map of the transparency dashboard and control panel derived from the SPECIAL proposal.

2.1.1 Functional components

ACCESS DATA

The dashboards 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 within a specific context for various 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 logs data format is part of work package two (WP2) and is described in deliverable **D2.3 Transparency Framework V1** 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 is a core functionality of the privacy dashboard. However, the underlying policy language SPECIAL introduces in WP2 (see deliverable **D2.1 Policy Language V1**) goes beyond conventional access control systems, since 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, thus, 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, erasure, or object. 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 even more 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 central challenge of WP4, which will be evaluated in user studies to find out if policy templates really ease the complexity of privacy policies and decisions.

CONSENT ENGINE

The consent engine is another core component of the dashboard. 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. Therefore, we plan to address and reflect the ***privacy calculus theory*** (Dinev and Hart 2006) in our consent interfaces.

BREACH NOTIFICATION

The breach notification is a new 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 dashboards 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 will 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?

[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.

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

2.2 Scope of this deliverable

To narrow the scope of this deliverable, the description of D4.1 in the proposal is used besides the above given explanation of WP4. The deliverable is 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**

Therefore, it is helpful to cite the descriptions of tasks **T4.1 Transparency dashboard and control panel** and **T4.2 Consent engine and feedback mechanism** at this point.

> *"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**

Based on the descriptions of the tasks, we include in this deliverable a first prototype of the SPECIAL privacy dashboard and multiple prototypes for consent interfaces. With regard to the overall scope of WP4, we postpone the functional components *access and usage policies* and *breach notification*. Consequently, our prototypes address the components *access data*, *event log/ provenance*, *policy templates*, and *consent engine*. The general requirements are the subject of deliverable **D4.2 Frontend Scalability and Robustness testing report V1**, which will be submitted in month 18 (June 2018).

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. For this reason, the chapter is separated into two subsections.

3.1 Concept 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.

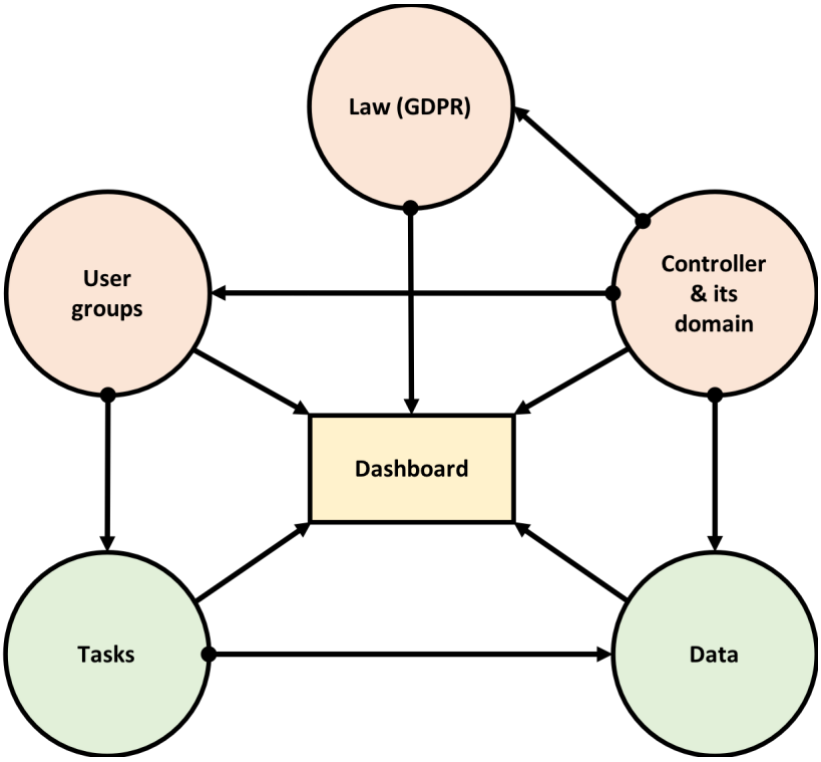

Figure 2: Identified factors that the privacy dashboard's appearance depends on including principle requirements like usability, legal, or business requirements.

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. 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 may differ. 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.

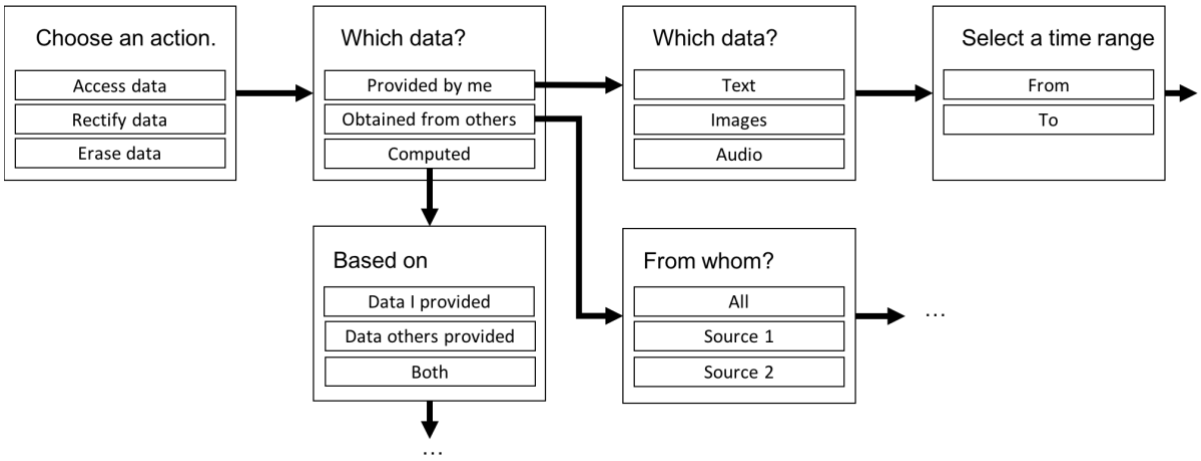

Figure 3: A wizard-like design that guides data subjects through a series of questions leading them to the desired information or action.

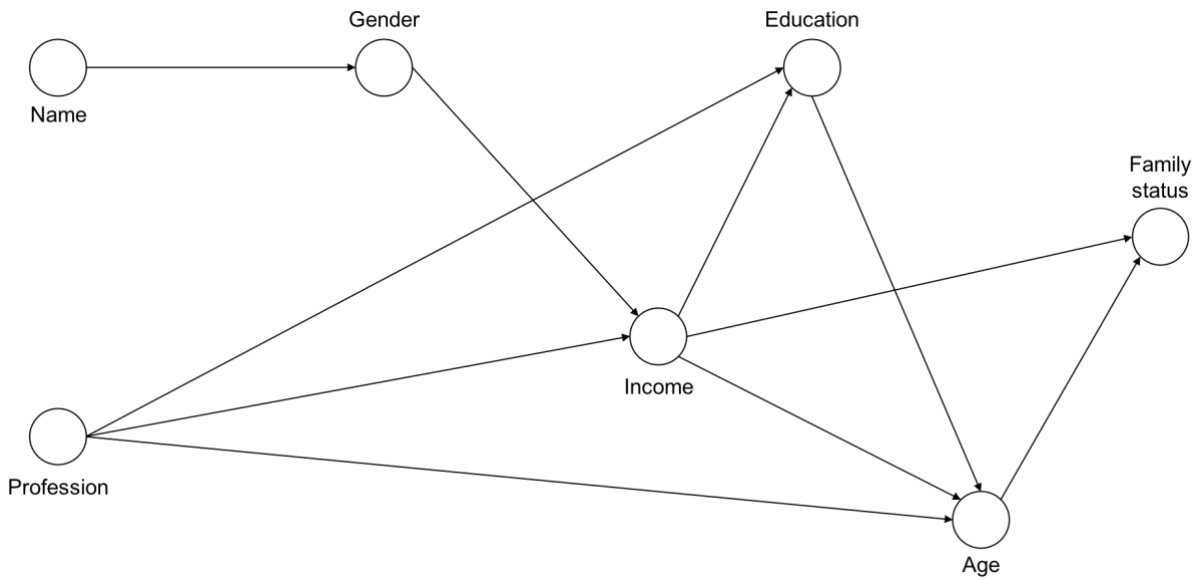

Figure 4: A graph visualizing what information were processed and combined and what information have been derived from that combination.

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.

Purposes of processing personal information are categorized into two categories: (i) user features and (ii) personal data processing. The first category consists of functional features the data subject desires to use like photo upload, photo sharing, video upload, video sharing, 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. For giving consent to one of the purposes in the second category, data subjects retrieve points they can spend to "get" the user features they desire. The purposes and their value are determined by the data controller beforehand.

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. To confirm this assumption, user studies are needed.

This principle is also used to define policy templates that can be offered to data subjects in a pricing table like manner, which represent different privacy plans the data subject can choose for this particular service. Conceivable profiles include for example: *most privacy preserving/ limited functionality*, *moderate data disclosure/ full functionality*, and *maximum data disclosure/ premium functionality*.

To compare this approach with more familiar consent interfaces that rather meet the expectations of data subjects with regard to giving informed consent, alternative interfaces are designed and implemented that aim to reduce the amount of text needed to communicate the contents of a controller's privacy policy to the data subject. Here, giving consent remains a statement represented by ticking a checkbox. These approaches can suffer from the "all-or-nothing" paradigm, however they might be well suited to inform data subject about data processing practices and involved privacy risks.

Since these concepts offer different levels of control to data subjects, a combination of all of them is conceivable and reasonable. Data subjects that feel their preferred privacy setting is not represented by any of the policy templates might want to "customize" consent by earning and spending points. Analogously, data subjects who want to give consent based on precise information and on a very fine-grained level might use a familiar consent interface that offers more text and less interactivity.

Further concepts with regard to *broad and dynamic consent*, which are discussed in deliverable **D1.3 Policy, transparency and compliance guidelines V1**, will be discussed in **D4.3 Transparency dashboard and control panel release V2**.

4 Transparency dashboard and control panel

This chapter presents the current state of the privacy dashboard developed during the last eight months. 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*[13]. To adapt state-of-the-art design principles for such kind of applications and to ease the process of styling, *Google's Material Design*[14] guidelines were followed. Therefore, the React library *material-ui*[15] has been used. In the following screenshots and corresponding descriptions will be given to describe the prototype textually. The current state has been also published on the Internet (http://raschke.cc/SPECIAL-privacy-dashboard/).

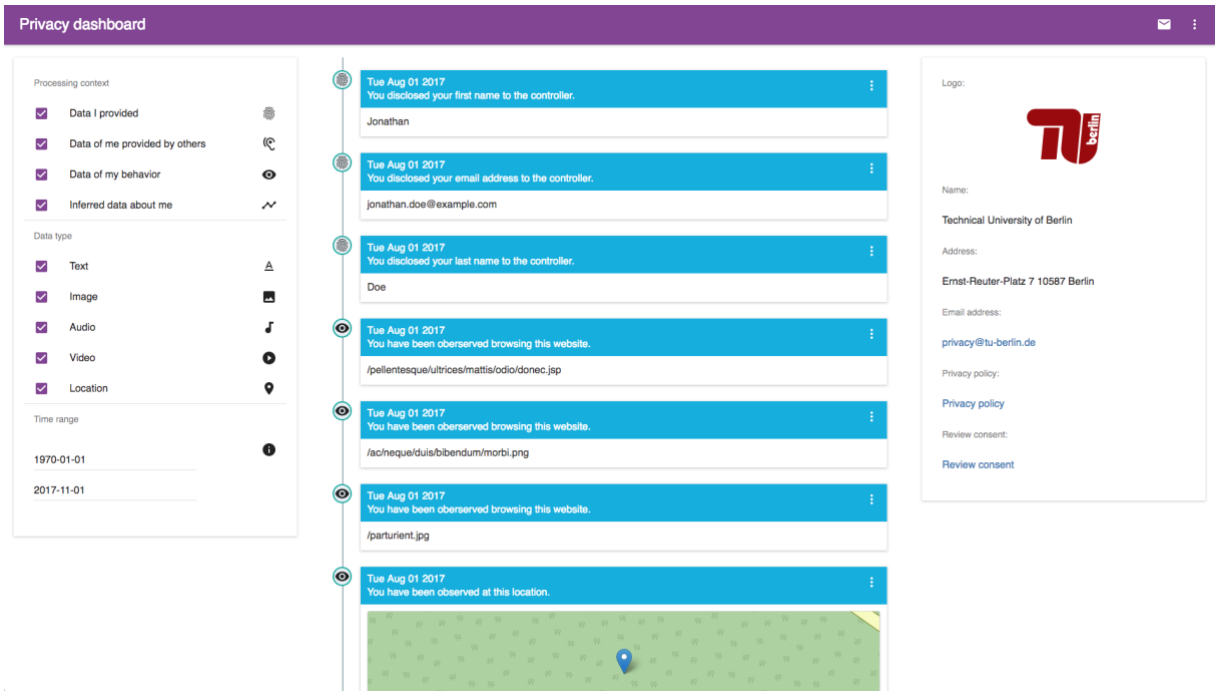

Figure 5: The current version of the privacy dashboard structured into three-columns.

As it can be seen in Figure 5, we have decided to follow a rather user-centric (also data-centric) design approach. In the left sidebar (see Figure 9 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 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.

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

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

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

- **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 can be seen in Figure 6, 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. A grouping of data items with regard to the time is reasonable and will be realized in the next iteration.

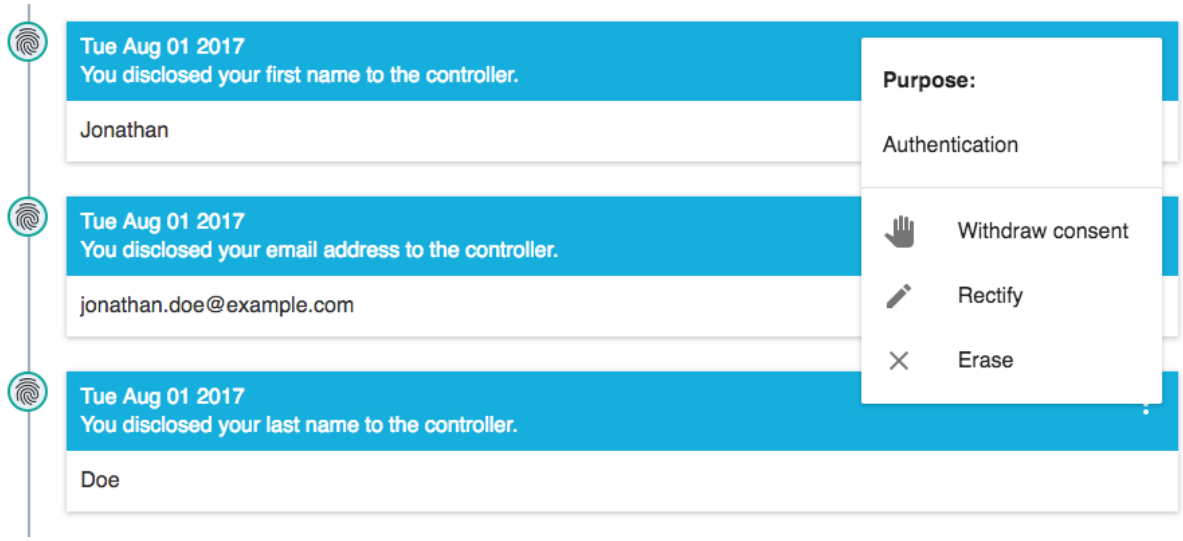

Figure 6: Representation of each data item by a visual component that gives context information on the processing.

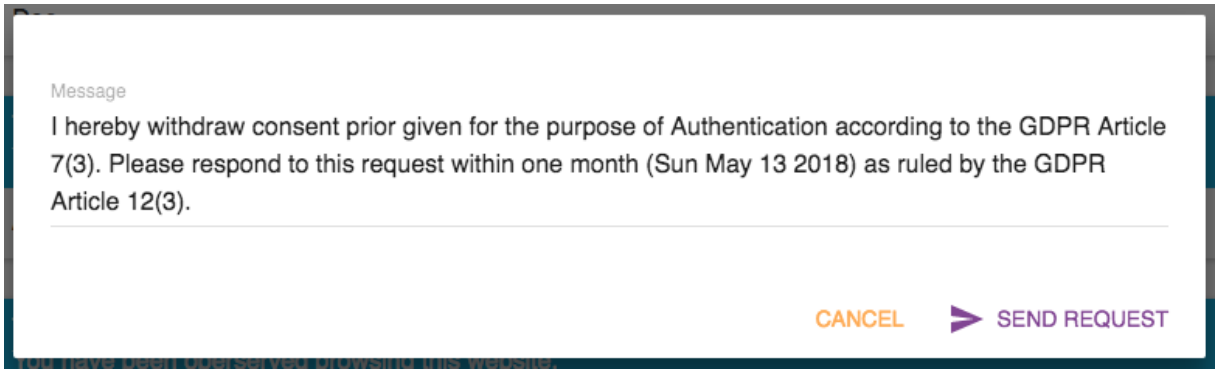

Figure 7: The withdrawal of consent is represented through a predefined written notice that is sent to the controller. The message can be edited by the data subject.

Withdrawing consent, requesting rectification, or erasure actually are legal requests that have to be responded by the controller within a certain time according to the GDPR[16]. Although it is a goal of SPECIAL to automatize 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 7 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 8. Messages are categorized into pending and answered requests. Here, the data subject can review sent messages and the answers of the controller to their request. Further requests and responses to answers from the controller can be sent as well.

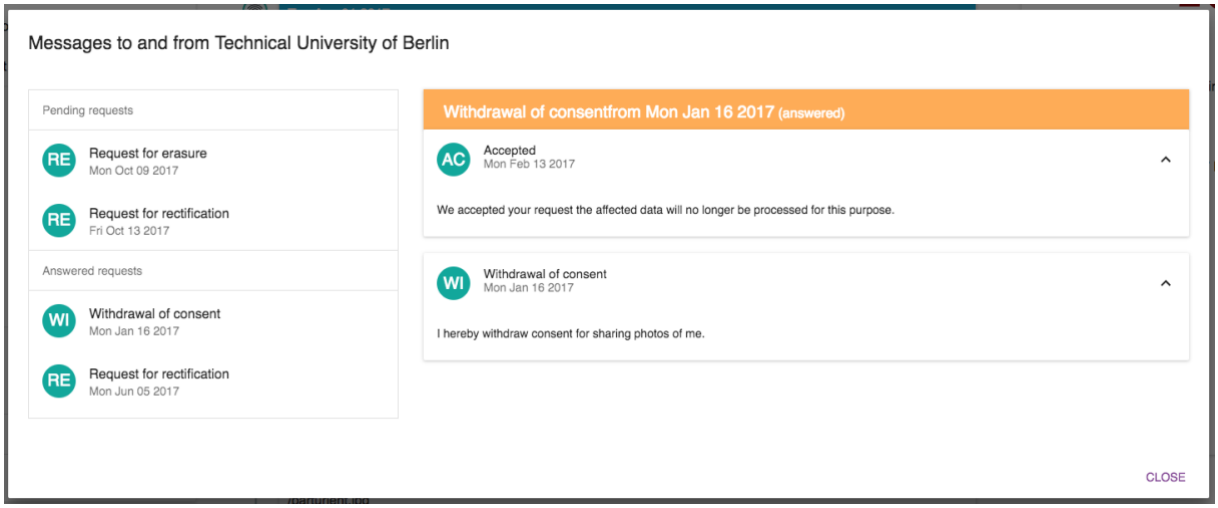

Figure 8: A message section gives an overview of pending and answered requests.

[16] GDPR art. 12(3)

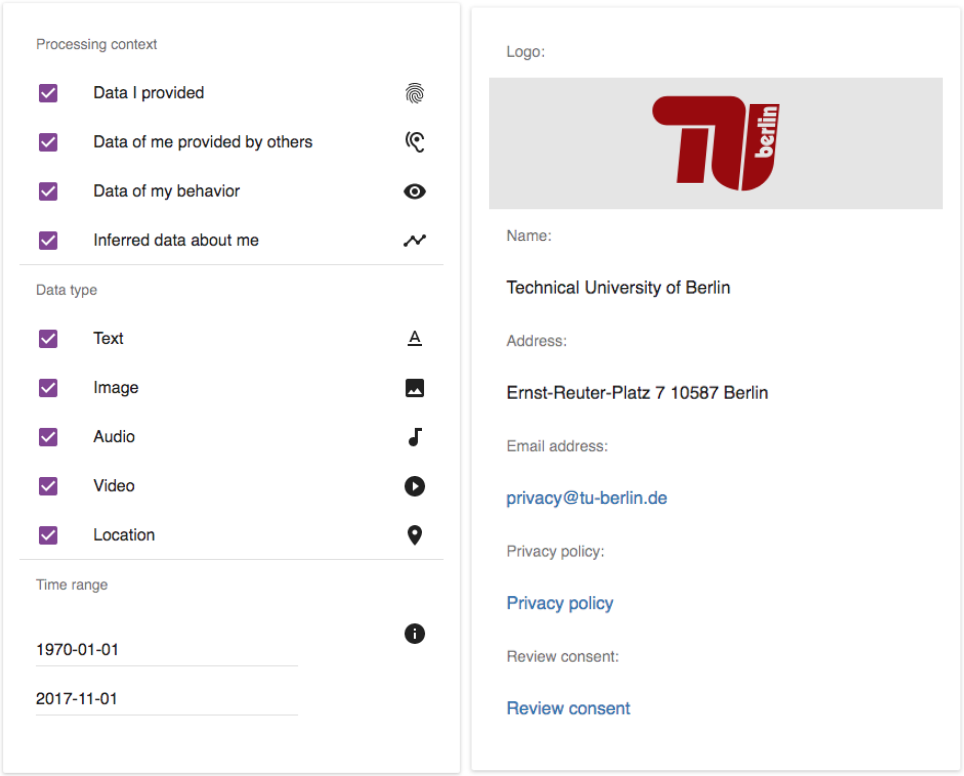

Figure 9: The left sidebar offers data subjects to filter the presented personal data. The right sidebar gives information on the controller in question.

Figure 9 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 option ***Review consent*** leads to the consent interfaces. The controller component of the dashboard needs further attention in the next iteration to identify, which information are relevant to data subjects with regard to the data controller.

The dashboard will be further evaluated in multiple user studies with different user groups and types. The results of these user studies will be included in the deliverables **D4.3 Transparency dashboard and control panel release V2** and **D4.4 Usability testing report V2**.

5 Consent engine and feedback mechanism

The developed of consent interface prototype designs are presented in this chapter. As stated above, we developed multiple consent interface that offer different degrees of control to the data subject. The approaches are presented and discussed in the following individually starting with the pricing tables approach, followed by customizable consent approach, and lastly the mobile consent interfaces.

5.1 Approach: Pricing tables

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 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 10, addresses the significance of the purpose, while (currently) neglecting all other information of the privacy policy. It is therefore an experimental approach, which possibly is not sufficient at the moment to meet legal requirements for informed consent. Following iterations will address this issue.

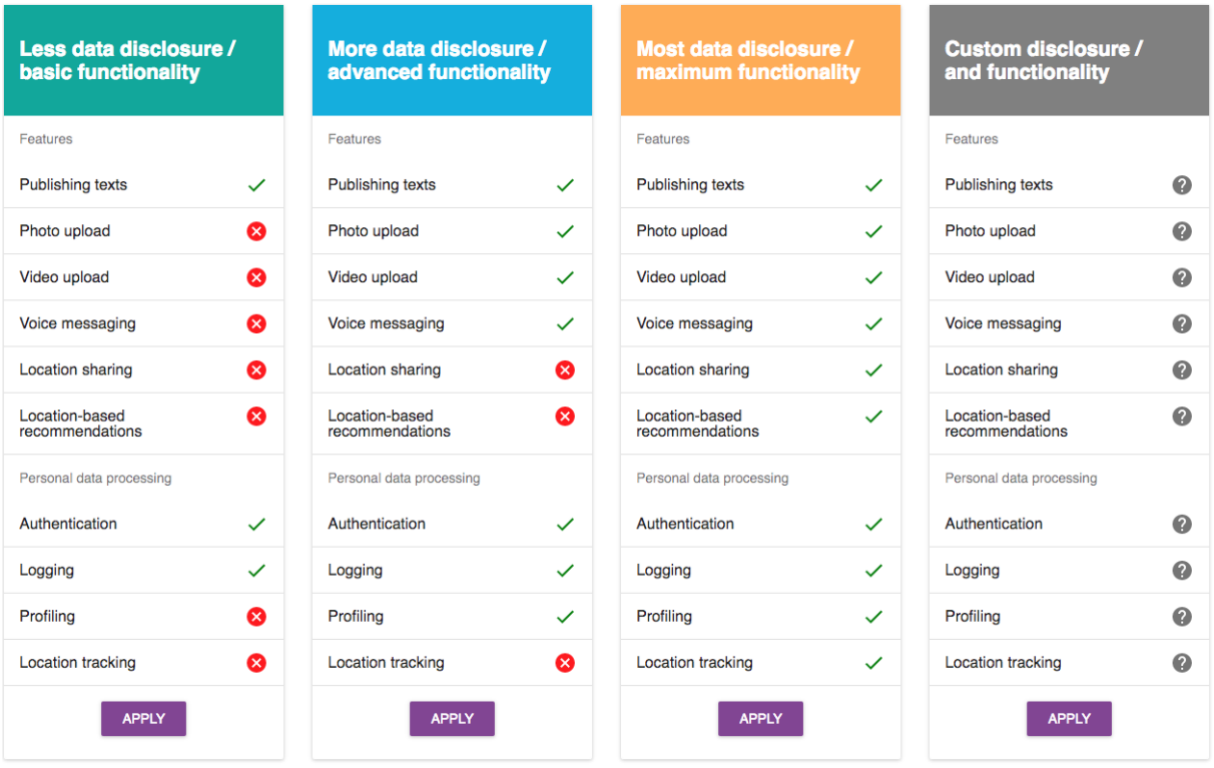

Figure 10: Data privacy plans to easily and quickly choose a privacy setting that reflects the privacy preferences of the data subject.

As already explained in Chapter 3, purposes for processing personal data are defined by the data controller and categorized into ***Features*** and ***Personal data processing***, while the first category represents functionalities the data subject intends to acquire and the second category compromises personal data processing practices that the controller mainly benefits from. Figure 10 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 features like photo and video upload and voice messaging only if being allowed to profile the data subject.

User studies are supposed to show whether data subjects are willing to accept such consent interface as a formal and legally valid mean to consent to the processing of their personal data. Moreover, this prototype misses relevant information that would be part of the privacy policy but are currently not included in this design. It would be interesting to investigate the best way to define these data privacy plans and which privacy plans are chosen more frequently than others and why. Thus, this approach will be pursued in the next iterations.

5.2 Approach: Customized consent

If the data subject has chosen to configure a customized data privacy plan, he or she is presented the consent interface depicted in Figure 11. As explained in Chapter 3, consenting to purposes of the category ***Personal data processing*** could "earn" the data subject points that can be "spent" to acquire features. The values are supposed to be predefined by the controller as well. 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.

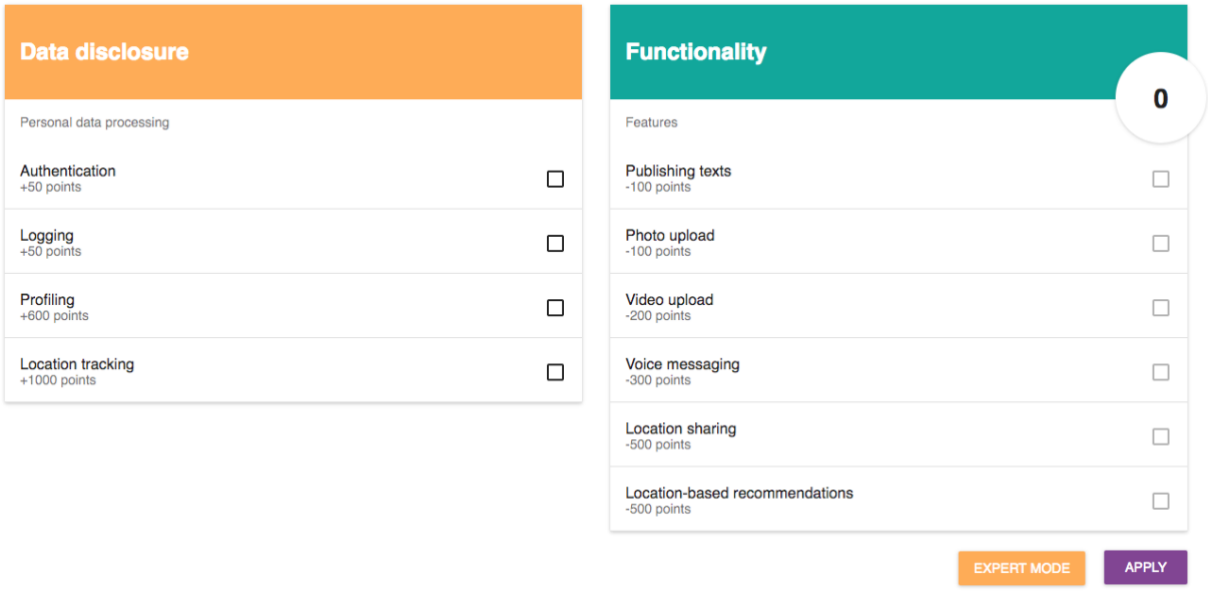

Figure 11: Consenting to purposes (that the controller benefits from) allows data subjects to "get" features they desire.

The current prototype does not meet the legal requirements as well and needs to be extended in upcoming iterations to meet legal requirements of the GDPR. However, it is conceivable that this design encourage more data disclosure (with reference to one of the goals of WP4). Figure 12 shows a configuration with "unspent" points that the data subject might consider to use (by consenting to ***Photo upload*** for example). This design approach gives personal data a concrete counter value. However, it has to be carefully evaluated whether data subjects perceive this interface and the interaction with it as given consent. Reviewing the situation in Figure 12 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***).

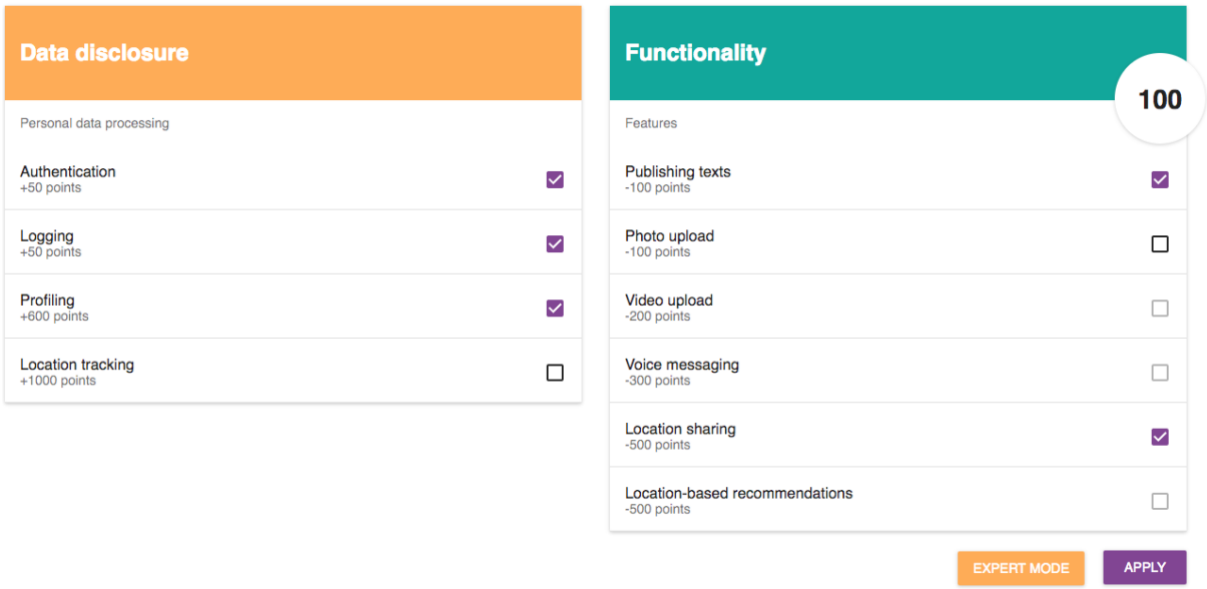

Figure 12: A custom configuration allowing data subjects to consent to the processing of their physical location without allowing the controller to track their location or give location-based recommendations.

5.3 Approach: Mobile consent interfaces

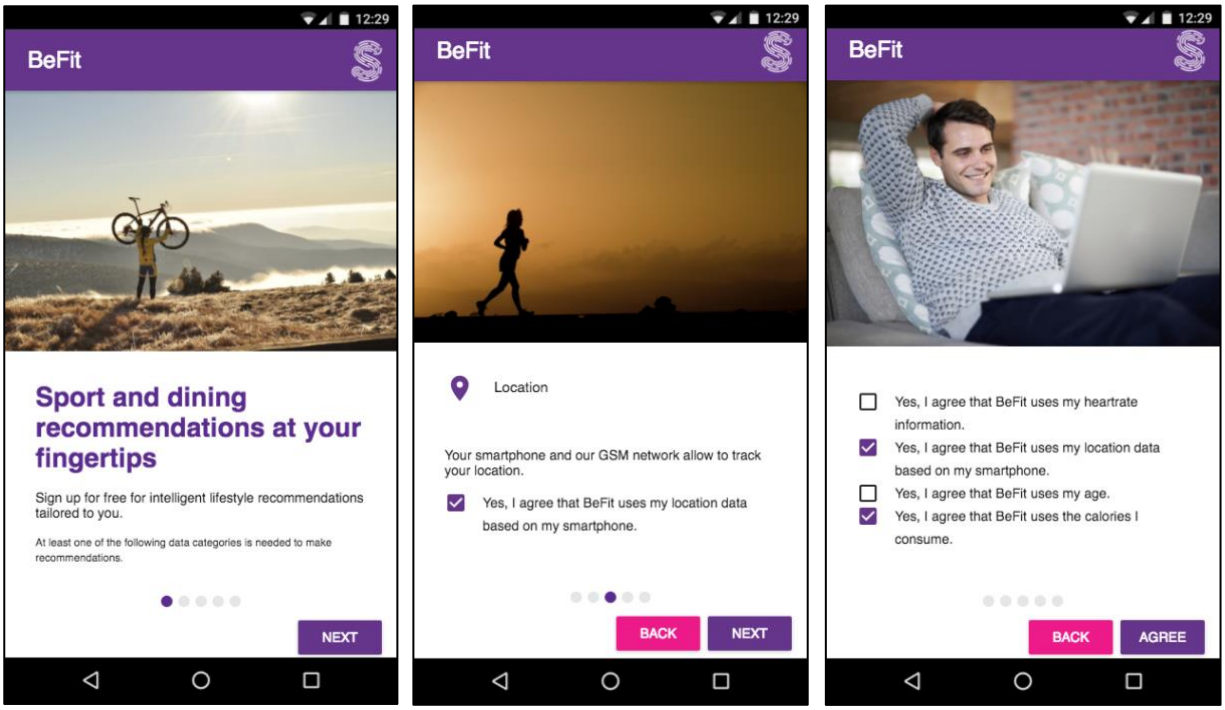

Figure 13: A mobile consent interface guiding data subjects through multiple views, which explain in detail what kind of data is used for which purposes.

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. Figures 13 and 14 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.

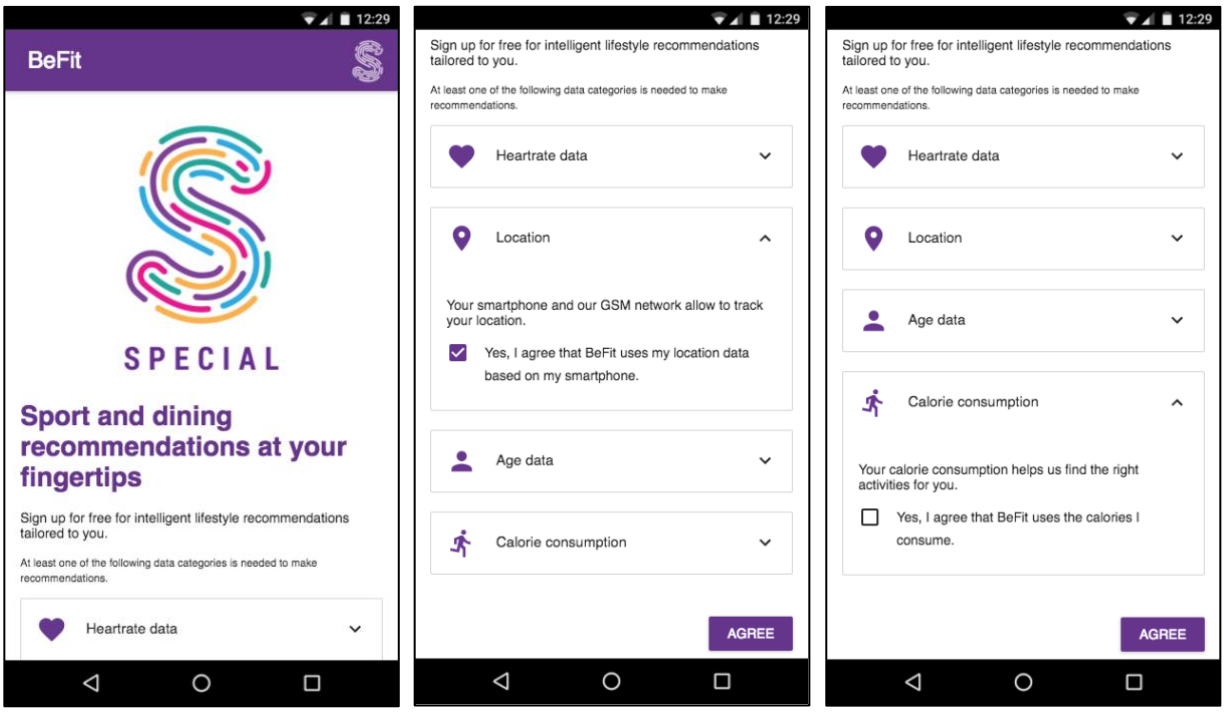

Figure 14: A mobile consent interface consisting of a single view and components that can be clicked or tapped to retrieve more information and to consent to the individual personal data processing practices.

6 Interface development for the dynamic consent request

In this chapter, we first review the requirements of the GDPR concerning informed consent and the background information about the dynamic consent requests. Then we describe our exemplifying use case scenario and the user interface wireframes for the dynamic consent request that we created based on this use case. In the end of the section we provide details on our user study and the interactive wireframe for the dynamic consent request that we developed for that user study.

6.1 Introduction

Before discussing our first version of the user interface (UI) for the informed consent request and its functionality, let us recall the background information about consent request that this UI is based on (cf. D1.3 Policy, transparency and compliance guidelines V1).

In the GDPR the processing of personal data is prohibited via Art. 6 except for some predefined scenarios (e.g.: public interest[17], legal obligations[18]) and when the data subject has consented[19] 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[20]. 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?

In **D1.3 Policy, transparency and compliance guidelines V1** we identified the need for **dynamic consent** instead of a ready-made, set in stone, static consent forms. Depending on the context, our dynamic consent could have all or some of the following features:

Categorization. The dynamic consent request groups similar requests into categories and asks for consent once per category.

Customization. More control is given to the user by providing a possibility to choose what data he or she allows to be processed, for what purpose, where those data can be stored and, if he or she allows data sharing - with whom.

Innovation. The user has an option of consenting to very general data processing for such purposes as service optimization and business intelligence.

Historical Data. The list of purposes could include processing of data subject's personal data that were gathered at some point in the past.

Revocation. The data subject should be able to withdraw his or her consent for future processing and sharing of all (or a part) of his or her data at any time.

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

[18] GDPR art. 6(1)(c)

[19] GDPR art. 6(1)(a)

[20] GDPR art. 4(11)

Understandability. The consent request should be presented in an understandable way, so that the data subject understands the implications of his or her consent.

6.2 Use case scenario for the consent request UI

For the development of the first version of our consent request UI 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. She is presented with a dynamic 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 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 15) 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. Although the dataflow we use for our use case (and, as a result, also for our UI of the consent request) is simplified, it is clear from Figure 15 that increasing data in the graph will increase its complexity. For the purpose of the initial development of the UI wireframes (creating a skeleton of our UI) and subsequent user studies there is no need for a highly complex use case. Scalability can be tested later in the course of the UI development.

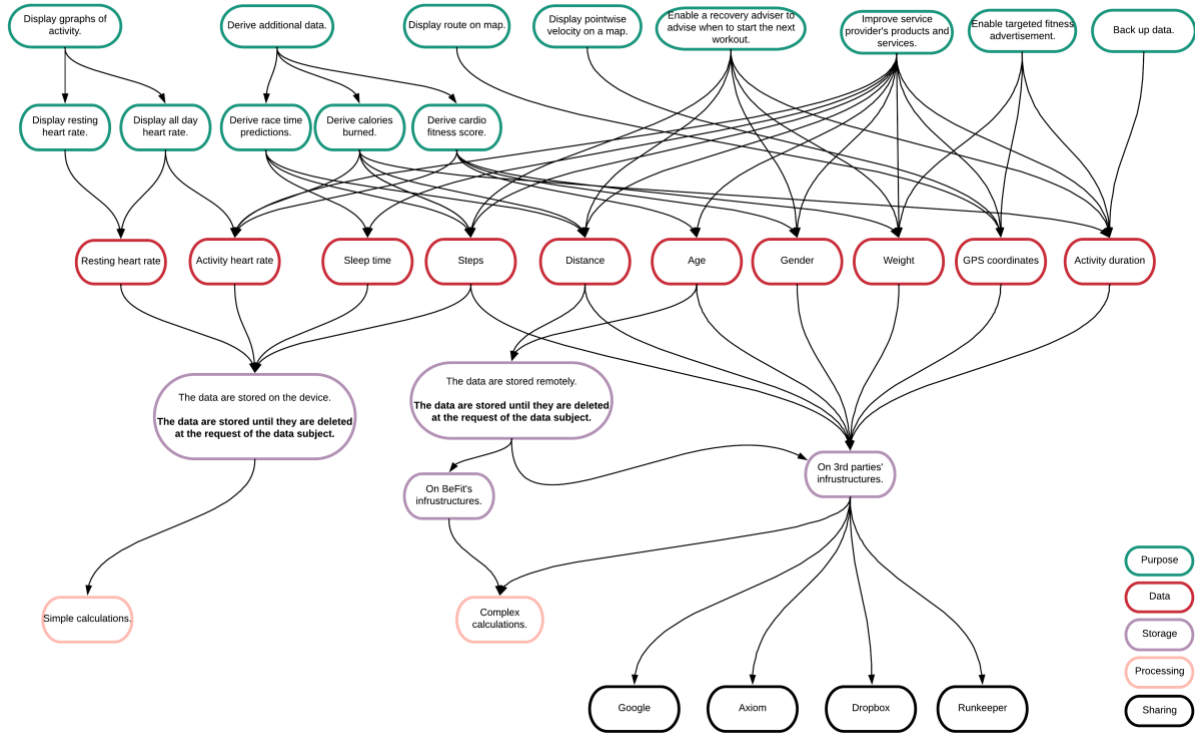

Figure 15: The information that must be presented to the data subject in BeFit's consent request.

6.3 Dynamic consent request UI wireframes

Based on our discussions with the consortium partners, we decided to create different versions of the UI wireframes for the dynamic consent request to be tested with users to find how they perceive those

UIs and what improvements could be made. We drafted three possible UI wireframes, namely graph, tabs, and user agent to be reviewed in one of our consortium meetings. All of them have features of the dynamic consent request as well as fulfill the requirements of the GDPR, in terms of the main information that should be presented to the user.

6.3.1 The Graph

The first UI wireframe is in the *graph* form as in Figure 15. The graph should be interactive allowing users to customize the consent and to withdraw their consent at any point in time. Figure 16 depicts one of the ways how the possibility to give consent could be implemented. The data subjects could choose any element of the graph. After the element is chosen, the button "Allow" would appear in the selected element.

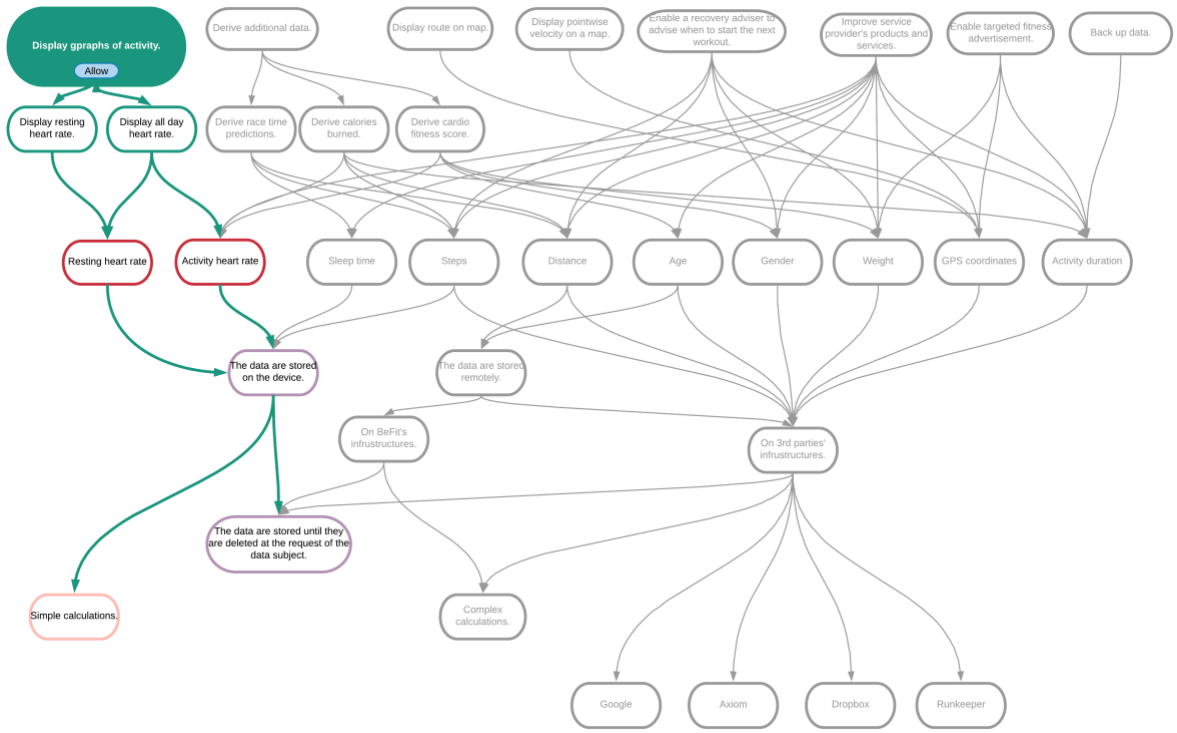

Figure 16: Possibility to give consent by clicking "Allow" button in the selected element of the graph.

The users should have an option to give their consent selectively. Figure 17 shows a possible option to present unique paths to the user, so he or she can decide what exactly to consent to.

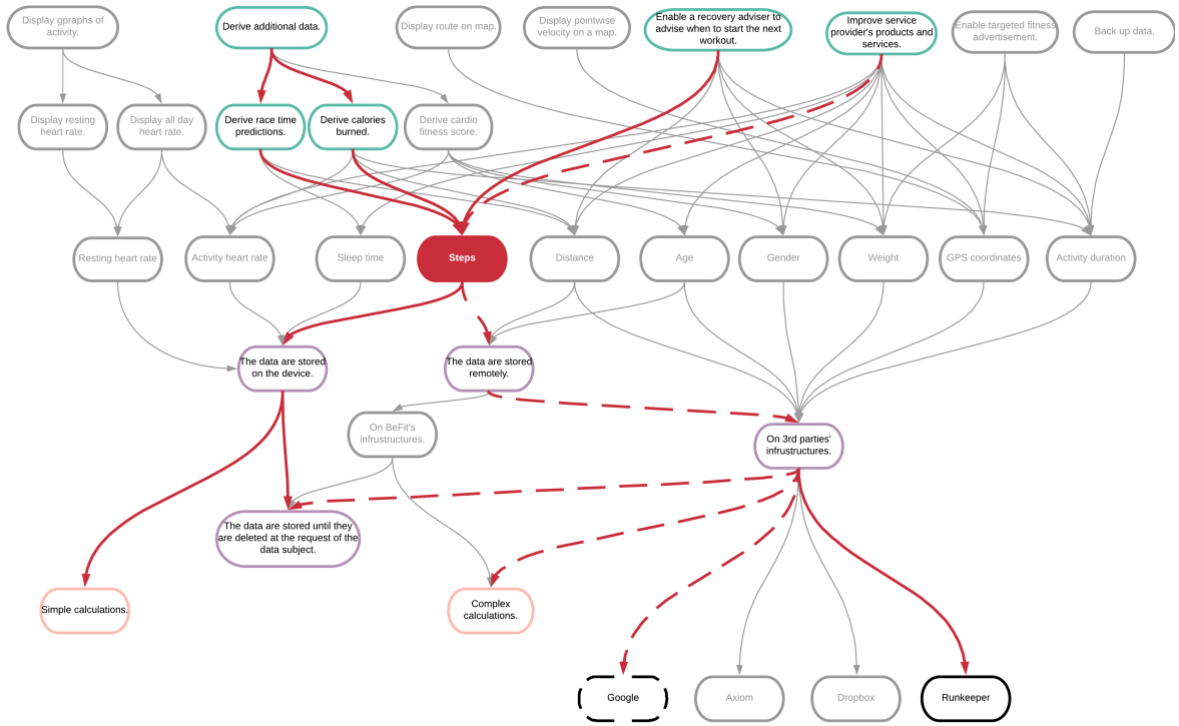

Figure 17: View of the unique path that could help the user to see what exactly he or she would be consenting to.

The graph also provides a possibility to withdraw the consent, or a part of it, at any point in time and as easily as it was given. Figure 18 depicts the consent withdrawal for the graph wireframe. The consent is withdrawn in the same way as it was given: the user selects an element and clicks, in the case of withdrawal, the button “Deny”.

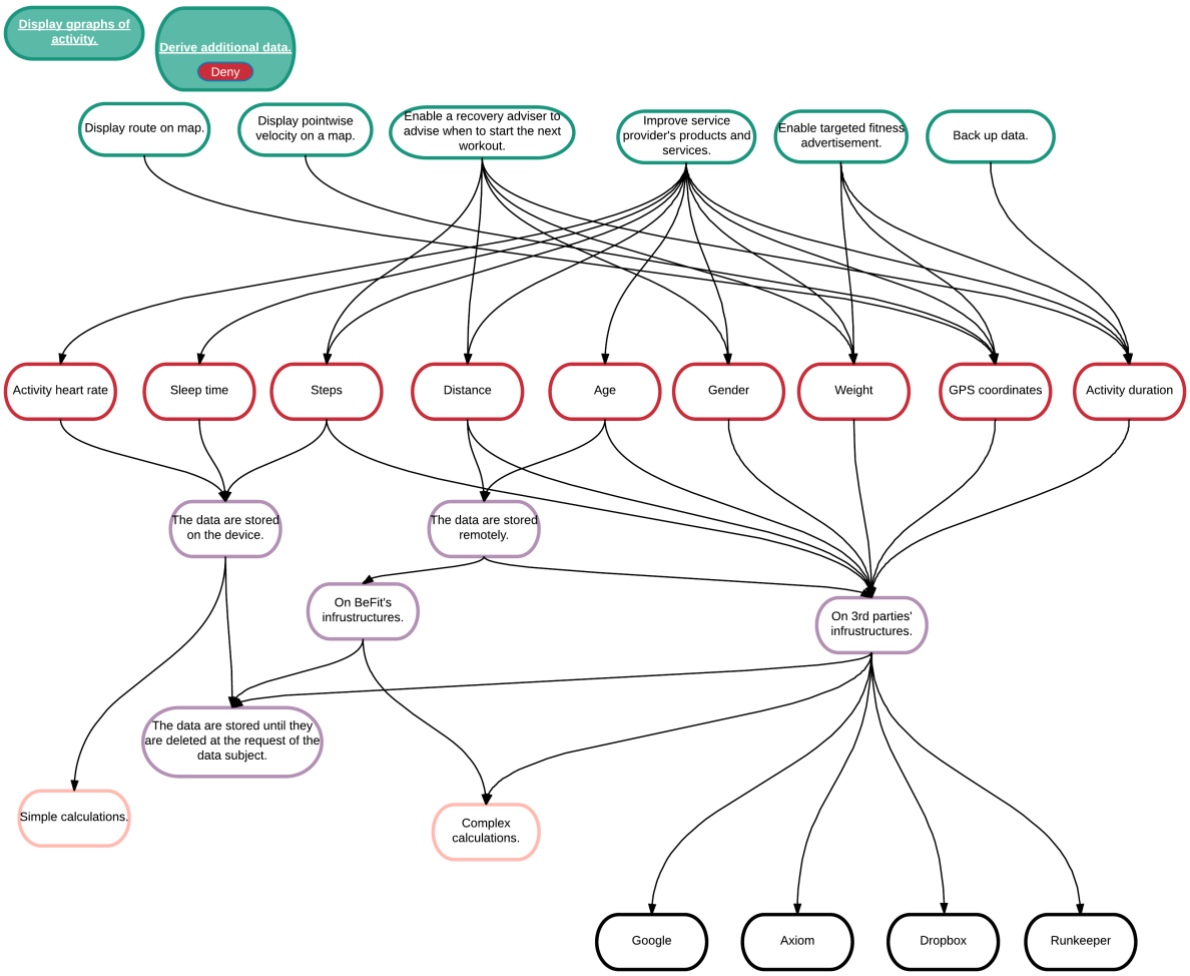

Figure 18: Possibility to withdraw consent by clicking „Deny“ button in the selected element of the graph.

The representation of consent information in a graph form has its pros and cons. The advantages of the graph lie in (i) the possibility of showing all the relations between purpose, data, storage, processing and sharing, (ii) giving good feedback to the user about what he or she has already consented to. The disadvantages of the graph approach are that, even with such a small amount of data to be visualized as in our use case, it can cause an information overload for the data subject. Another disadvantage of this approach is that it is difficult to adapt the graph for every display size without the need for scrolling.

6.3.2 Tabs

The second UI option is to represent data in more familiar way in the form of *tabs* (Figure 19). Here the user can browse the following tabs: data (what data 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). The user can customize his or her consent by turning on (giving consent) or off (withdrawing consent) the switchers opposite, in our example, the list items of the data tab. Users can also use the icons next to the switcher to create more fine-grained customization. There could also be an integrated video that provides users with an overview of the information on each page.

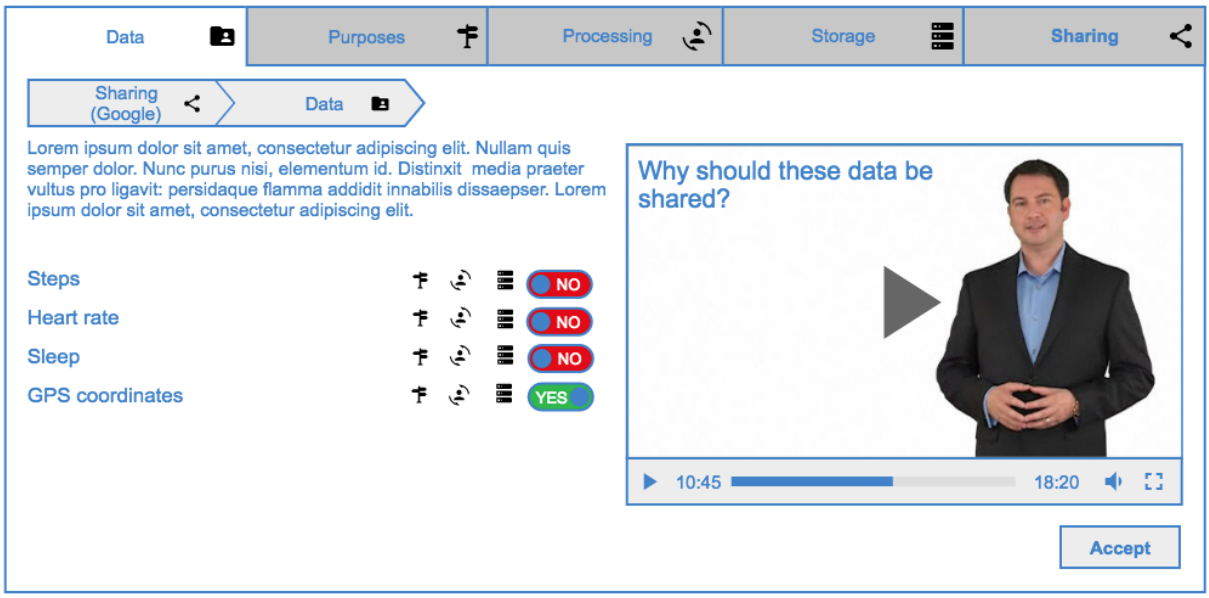

Figure 19: Dynamic consent request in the form of tabs.

The tabs UI has flexibility, can be made responsive and is not complex at first sight, so the data subject will not be discouraged from using the service. However, it is difficult to highlight what data were selected by the user, so the user can get lost easily and it is hard for him or her to know when he or she finished giving the consent.

6.3.3 Agent

The third UI version for the dynamic consent request is the one with an *agent* and pop-up speech balloons (Figure 20). As two other versions, this UI also aims to provide all the dynamic consent features relevant to our use case and the main information about the data processing.

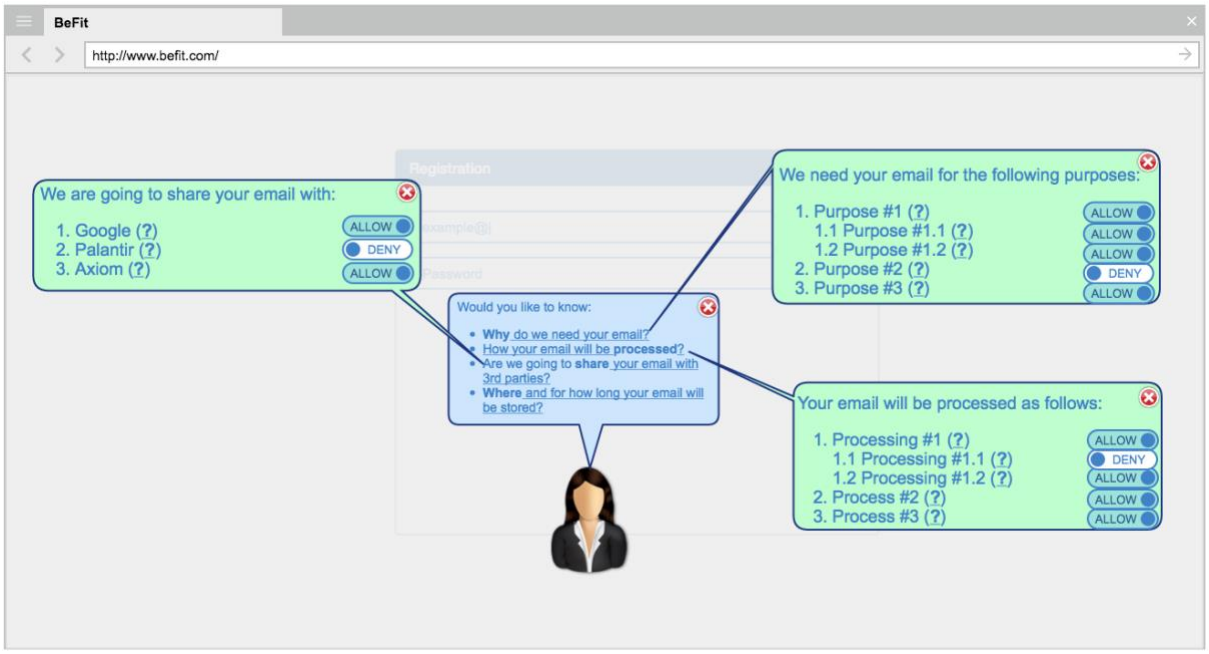

Figure 20: Dynamic consent request with an agent.

Similar to the UI with tabs, this UI is not complicated at first glance, but, here, as well, there is no good indication of what the user has already read. This UI version is not well suitable for every display size. The agent UI received the least positive feedback when presented to the consortium. However, there was positive reaction for usage of the agent UI on demand, for example, when there is a need for user's consent for a new purpose or a new data category.

6.4 First interactive UI wireframe for the user study

Since we wanted to involve real data subjects at the early stage of the UI development, we decided to prepare a user study in order to test the UI functionality, content placement and intended page behavior of one of the UI versions. Based on the feedback from the consortium partners and colleagues in the UI field of research, we decided to take the tabs UI as the basis for our first interactive wireframe but enrich it with the graph UI. The graph UI has limited functionality and its main purpose is visualization of unique paths the user can give his or her consent to. Figure 21 depicts our wireframe of the first UI version for BeFit's dynamic consent request. We would like to stress that this UI is just the first version, we plan to test other versions later in the course of the project.

To make our wireframe more realistic and more suitable for user studies, we developed its fully functional online version[21]. While creating this online version we followed Jackob Nielsen's usability heuristics for user interface design[22]. We used Angular Material[23] and D3.js[24] for the front-end development of the online version and Firebase[25], with its real-time database and hosting, for the server side.

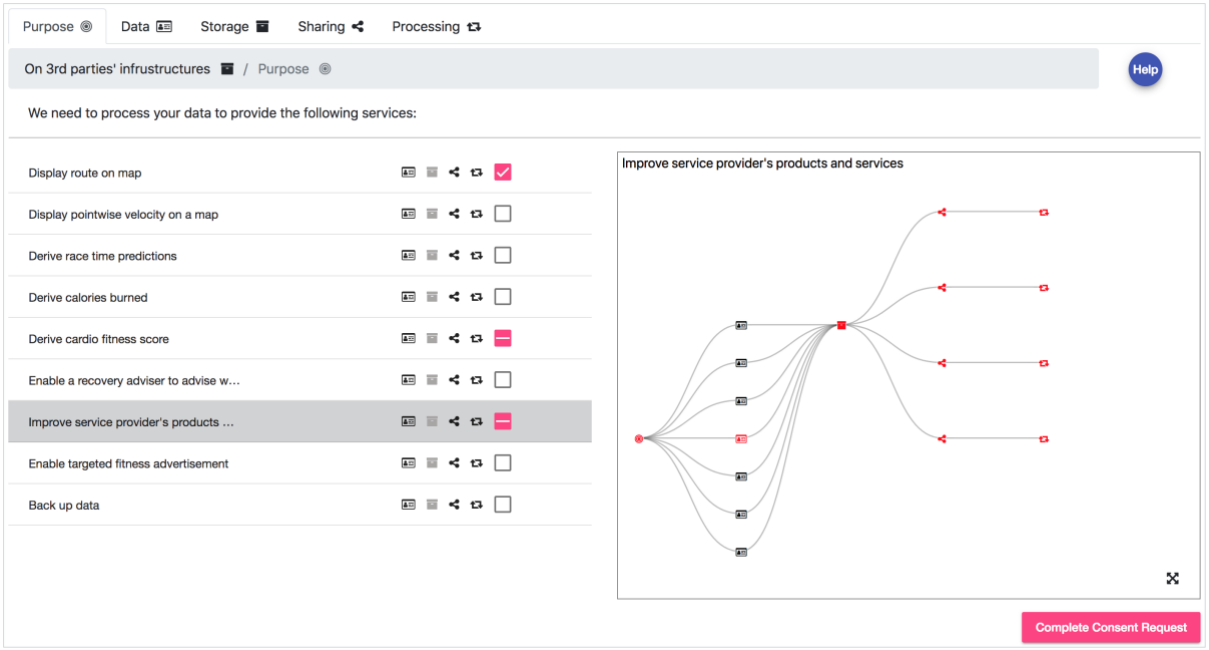

Figure 21: The wireframe of the first version of the dynamic consent request UI.

[21] BeFit | Consent Request. https://concent-request.firebaseapp.com/wizard, last accessed: 04/16/2018.

[22] 10 Heuristics for User Interface Design: Article by Jakob Nielsen. https://www.nngroup.com/articles/ten-usability-heuristics/, last accessed: 04/16/2018.

[23] Angular Material. https://material.angular.io/, last accessed: 04/16/2018.

[24] D3.js - Data-Driven Documents. https://d3js.org/, last accessed: 04/16/2018.

[25] Firebase. https://firebase.google.com/, last accessed: 04/16/2018.

Our first online interactive wireframe was developed based on the features of dynamic consent request from D1.3 adapted to BeFit's use case scenario. This wireframe provides the following functionality:

Categorization. We grouped information according to five categories, namely purpose, data, storage, sharing and processing. This grouping is realized in the form of tabs (Figure 22). In the tab *purpose,* we display the services that are offered by BeFit and that require personal data processing. The tab *data* lists personal data that could be processed by BeFit, if the data subject consents to data processing. In the *storage* tab we provide information on where BeFit stores data subject's personal data. The *sharing* tab gives insights into third parties with whom BeFit may share personal data of the data subject. In the *processing* tab we describe how personal data could be processed. To support the visualization, additionally to the name of the category on the tab, we added icons for each category.

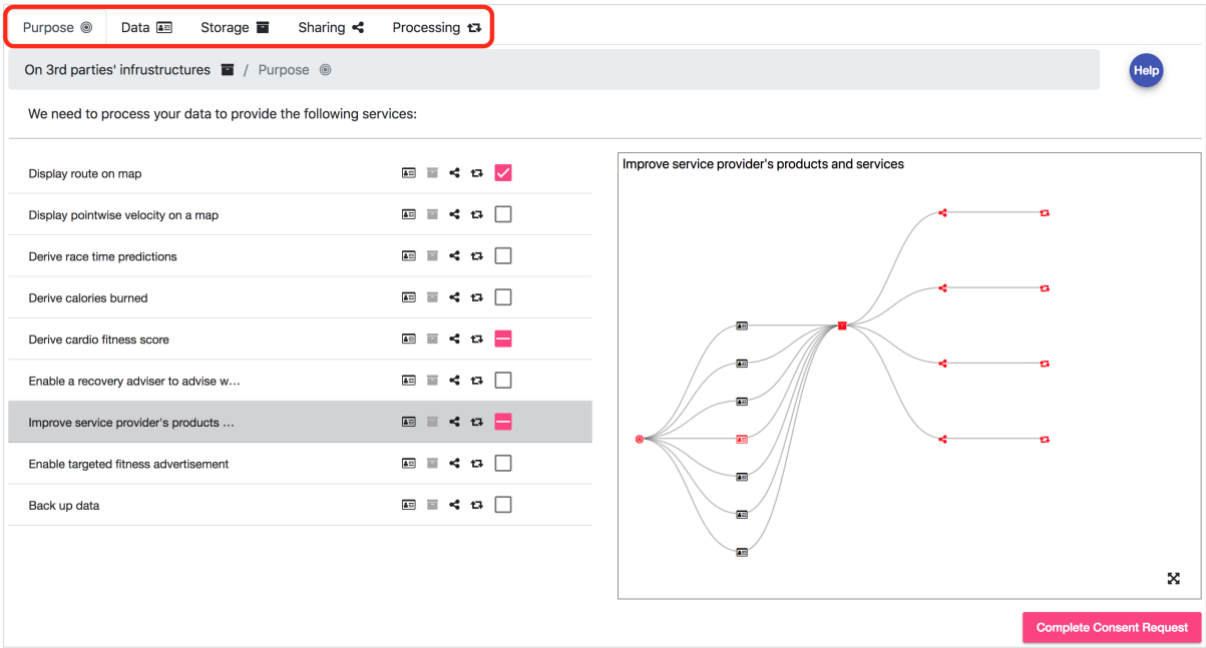

Figure 22: Categorization in the form of tabs (purpose, data, storage, sharing, processing).

Customization. The most important feature of our first version of the consent request UI is the full customization of data subject's consent. We do not offer an all or nothing approach. The user can fully adjust his or her consent specifically to his or her wishes. Our consent request gives the possibility to review information or give consent according to five categories mentioned in the categorization feature above. Any tab category can be a starting point of giving consent. The user is also 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. For example, he or she can allow BeFit to process his or her resting heart rate (*data*) to be displayed to him or her in BeFit's app (*purpose*) by performing on-device calculations (*processing*) and saving his or her data on his or her device (*storage*) without *sharing* it with anybody. The drill down feature is implemented by placing clickable icons of possible drill-down options near each item in the category/tab list (Figure 23). The user can drill down each item in the list by clicking on an icon that corresponds to the category he or she wants to select. In this way the user can create a unique path to consent to. The unique path is displayed and can be navigated in the breadcrumb under the tabs (Figure 23). The user gives his consent just by selecting checkboxes that correspond to his or her preferences. The check box is placed near each category item after the icons for drill-down options (Figure 23).

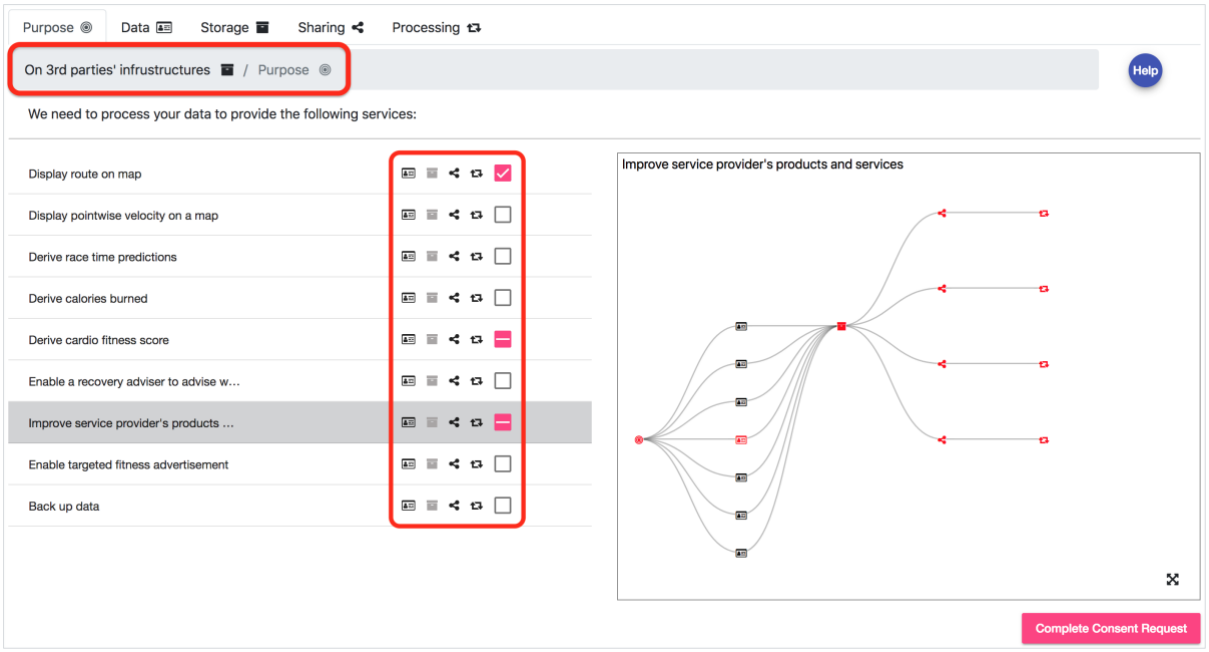

Figure 23: Customization of data subject's consent.

Innovation. As described in **D1.3 Policy, transparency and compliance guidelines V1**, one of the possible features of the dynamic consent is innovation – i.e., the user could help foster innovation by consenting to very general data processing for such purposes as service optimization and business intelligence. The purpose *"improve service provider's products and services"* is included into the list of purposes in our consent request (Figure 24).

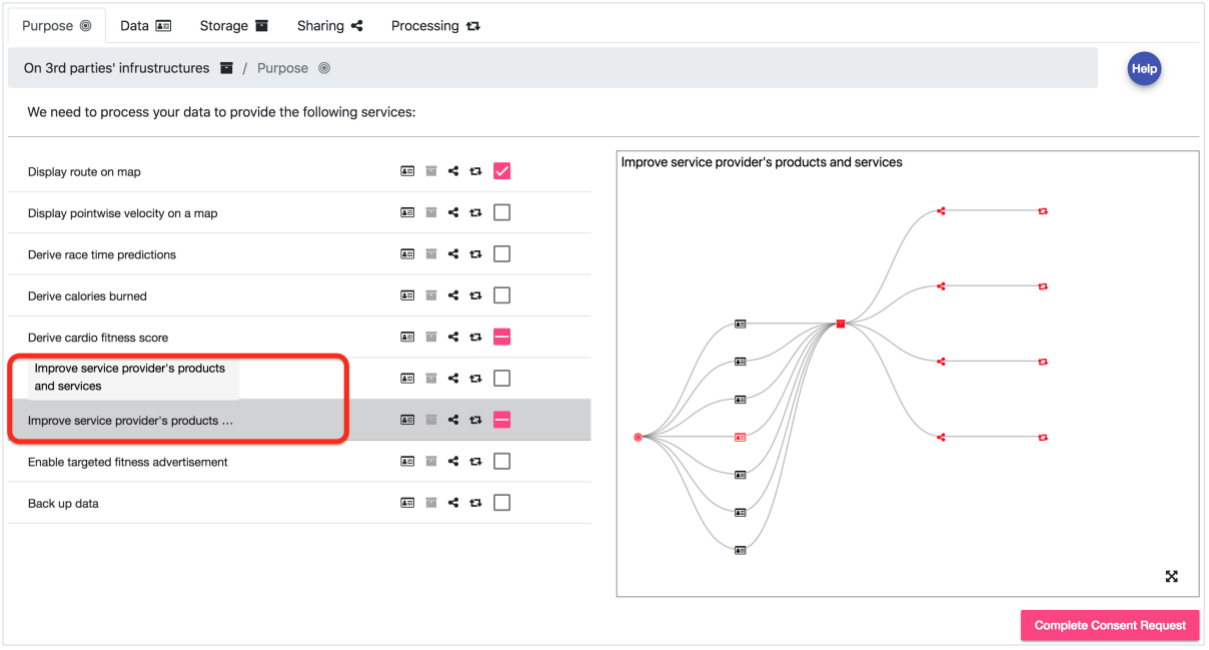

Figure 24: The purpose *"improve service provider's products and services"* is included into the consent request to foster innovation.

Revocation. The user can withdraw his or her consent by removing the selection in any checkbox at any time (Figure 25). In our use case the consent is given for the first time before using the device and the consent withdrawal in our interactive UI wireframe is tailored to this use case. If the user changes

his or her mind later, he or she can use privacy dashboard for consent revocation (**Error! Reference source not found.** and **Error! Reference source not found.**).

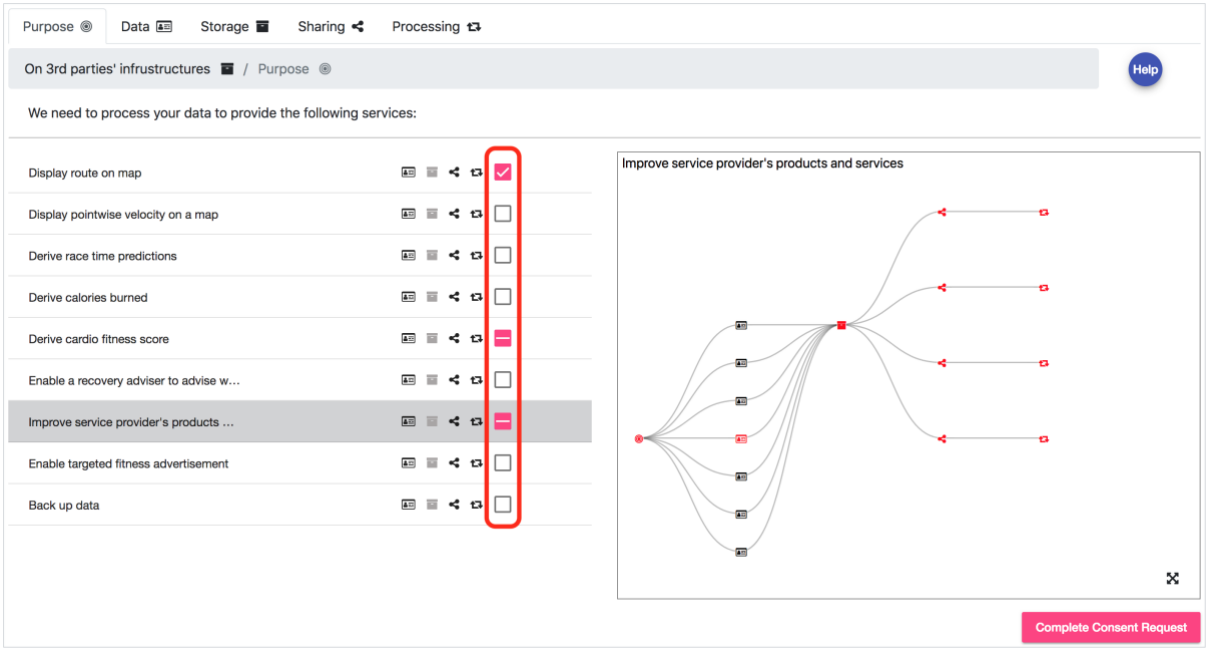

Figure 25: Consent withdrawal by removing the selection in the relevant checkbox.

Understandability. To increase understandability and ease of use of the consent request we are using plain language and standard icons for the content. Every action of a user is backed up by feedback. To help the data subject to understand the implications of his or her consent, our dynamic consent request is supported by a graph (Figure 26). The graph has a tree form and shows every possible unique path that goes through the selected item. The paths that the user consented to are highlighted in red. Each item in the graph is represented with the help of already mentioned icons. More information, in the form of a tooltip, is shown upon hovering over each icon.

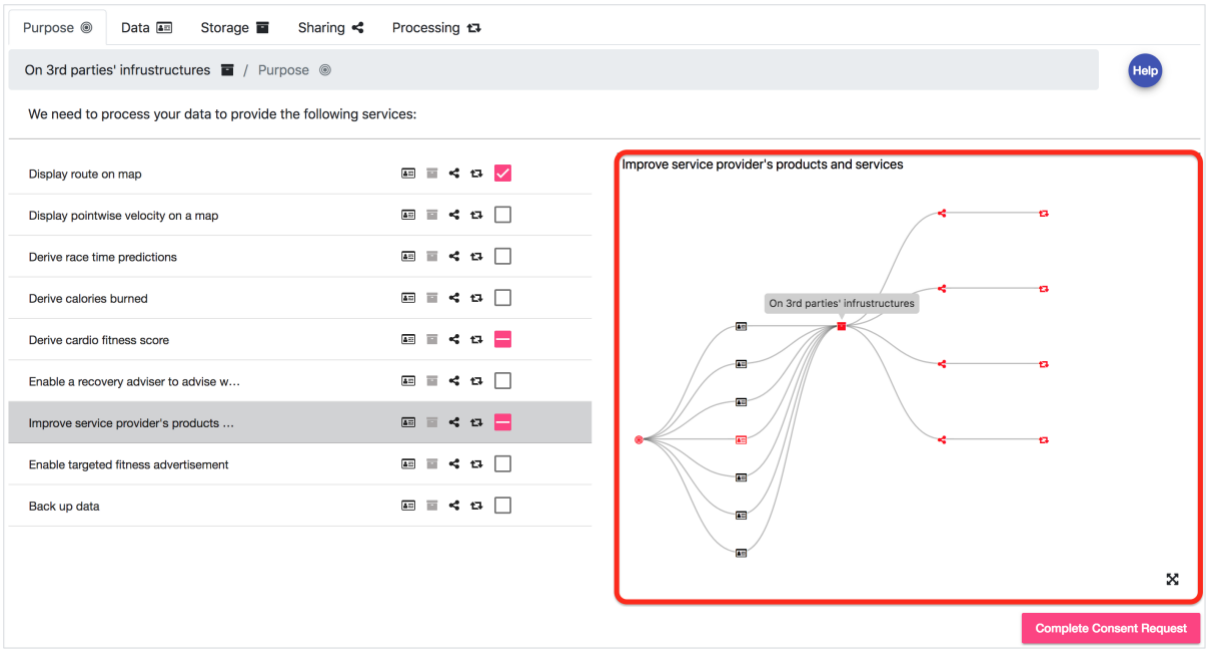

Figure 26: Graph could help the data subject understand the implications of his or her consent.

The user can also enlarge the graph to full-screen size (Figure 27) by clicking the corresponding button in the lower right corner.

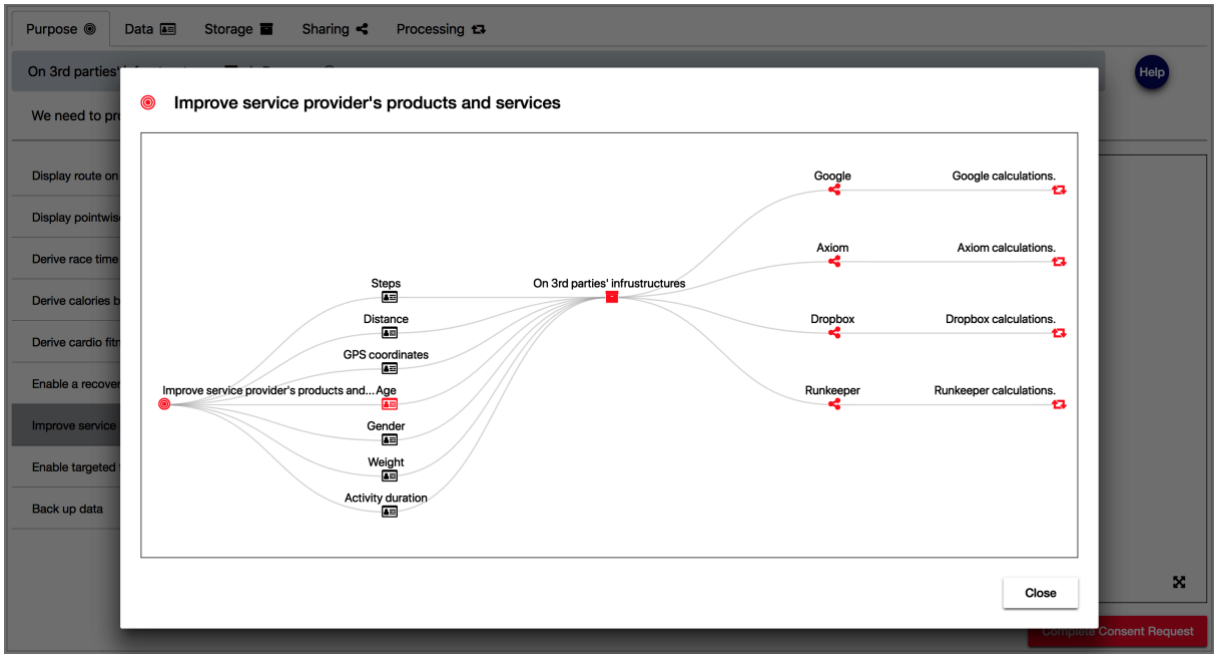

Figure 27: Full view of the graph.

After the user finishes consenting (by clicking "Complete Consent Request" button), he or she is presented with an overview of all the information that he gave his or her consent to be processed by BeFit (Figure 28).

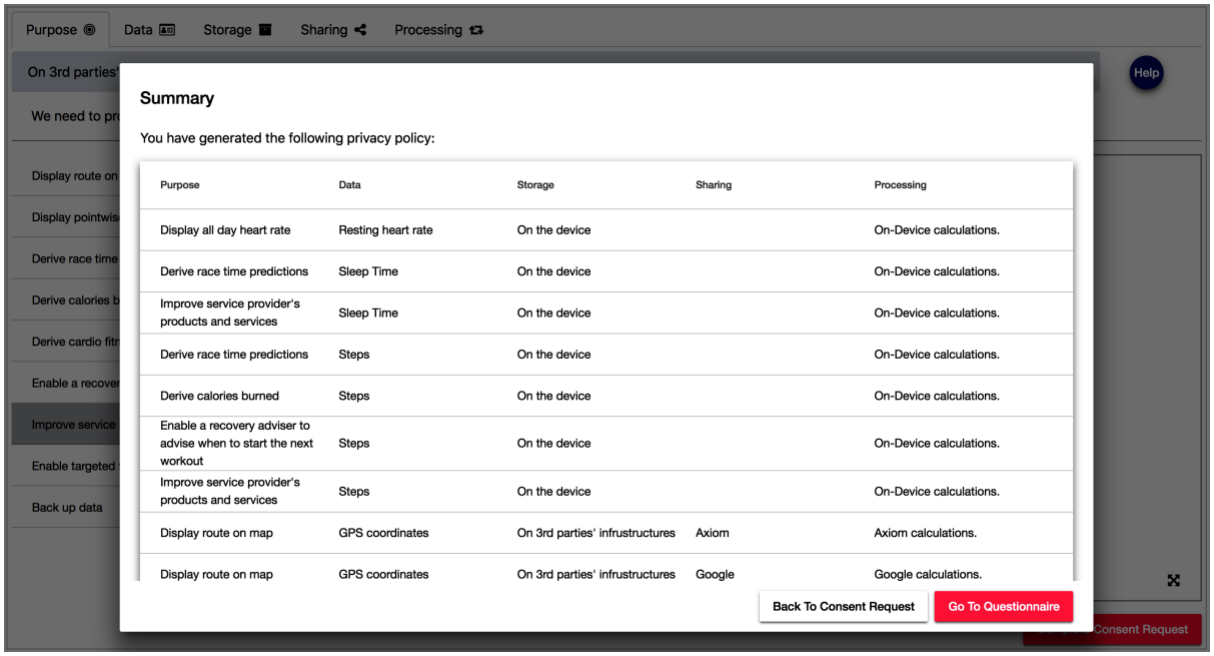

Figure 28: Summary of all the information that the data subject gave his or her consent to be processed.

To check the usability of our first UI for dynamic consent request we are now conducting a user study.

6.5 User study

For the study we selected a think aloud method (van Someren 1994, Seidman 2006, Charters 2003) where the participants are first presented with BeFit's use case and then they are asked to imagine themselves buying BeFit's wearable appliance for fitness tracking instead of Sue. The participants are then asked to activate the device and give their consent for the processing of their data by BeFit. In the beginning the participants complete a series of tasks of giving and withdrawing consent. After this exercise they just give their own consent, as they would have done this, if they bought the BeFit smart watch. The participants record their screen and their thoughts. Our online wireframe enables participants to give their consent from any place comfortable for them, making our user study more realistic. In the end of the assignment each participant fills in a questionnaire providing us with their demographic data as well as their impression of our dynamic consent request UI. The questions of both questionnaires can be found in the annexes. Immediately after finishing giving the consent, the participants are also asked to type in everything they remember consenting to.

Since the user study is in progress, the results are going to be published in **D4.2 Frontend Scalability and Robustness testing report V1**. After analyzing participants' videos and thoughts we hope to answer the following questions concerning the usability of our UI: (i) Are icons/labels understandable? (ii) Do users find the graph useful and understandable? (iii) Is the drill-down process easy to fulfill? (iv) Is giving consent as easy as withdrawal? (v) Was the consent informed? How much do users remember after giving consent (data, purpose, processing, storage, sharing)? (vi) How fast do users learn to give and withdraw consent? (vii) Do users mostly agree in bulk or use customization? (viii) Is the affordance of breadcrumb visible? (ix) Are users satisfied with the UI? (x) Is UI simplification needed? If yes, how can the UI be simplified?

Concerning the last question, we could preliminary (even before the detailed analysis of all user study results) assume that the data subjects will be overwhelmed with the consent information if they need to read and understand all the details. This means that simplification of the consent request and the reduction of the consent information details, that are mandatory for the data subject to read, most likely will be needed. In this case, we would need to cooperate with the legal experts, who could advise us on the consent information reduction and validate our proposed simplifications.

Based on the user study results, we are going to develop different versions of the improved UI to be further tested in our next user study. Since our current use case includes only the initial consent request (i.e., before the data subject starts using the device), we could expand the use case to include situations where the consent requests are contextualized, incremental and distributed over time. For example, we could add the case where the consent requests are triggered by the data subject's attempt to use new or more features offered by the device. Those additional functionalities would require user's consent to the data processing for new purposes or might even require data subject's permission to collect and process new data. The improved UI versions could be additionally adjusted to the proposed changes in our use case scenario and new features could also be tested in our next user study.

7 Conclusions & Future work

This deliverable presents the activities and efforts made within the context of WP4 of SPECIAL during the last eight months. We 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 (called privacy dashboard or dashboard) 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. Deliverable **D4.2 Frontend Scalability and Robustness testing report V1**, which is due at the end of month 18, will focus more on the remaining general requirements, i.e. performance, scalability, and security.

We presented a first prototype for the privacy dashboard and elaborated on its design. We presented multiple designs and prototypes for consent interfaces, we developed and partially evaluated in user studies during the last eight months. There, we already highlighted the next steps needed to improve the prototypes with regard to legal and usability requirements. We plan to pursue the design approaches presented in this deliverable and further evaluate those in user studies. The results of those user studies will be partially included in **D4.2 Frontend Scalability and Robustness testing report V1** and reiterated in **D4.3 Transparency dashboard and control panel release V2**, which is due in month 25.

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 in 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