UI prototypes: Policy administration and presentation version 1

Editors:	Simone Fischer-Hübner (KAU)
	Erik Wästlund (KAU)
	Harald Zwingelberg (ULD)
Reviewers:	Aleksandra Kuczerawy (KUL)
	Franz-Stefan Preiss (IBM)
	Dave Raggett (W3C)
Id	Identifier: D4.3.1
Type:	Deliverable
Version:	1.0 (Final)
Class:	Public
Date:	June 29, 2009

Abstract

Privacy Policies are an important prerequisite for user control in privacy-enhancing identity management. The transparency of privacy policies can be enhanced if users are informed about mismatches of a site's policy with the user's preferences. Investigating understandable and transparent privacy policies as well as simplified and usable privacy preference (data release policy) management "on the fly" are the objectives of the deliverable. For this, it is discussing icons presenting the content of policies and different User Interface (UI) prototypes for policy display and preference administration, which have been partly compared and tested in an Online user study. Finally, legal requirements for policy display in social network sites and how they translate to Human Computer Interaction (HCI) requirements are investigated.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n^o 216483 for the project PrimeLife.

SEVENTH FRAMEWORK PROGRAMME

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany
3.	Technische Universität Dresden	TUD	Germany
4.	Karlstads Universitet	KAU	Sweden
5.	Università degli Studi di Milano	UNIMI	Italy
6.	Johann Wolfgang Goethe – Universität Frankfurt am Main	GUF	Germany
7.	Stichting Katholieke Universiteit Brabant	TILT	Netherlands
8.	GEIE ERCIM	W3C	France
9.	Katholieke Universiteit Leuven	K.U.Leuven	Belgium
10.	Università degli Studi di Bergamo	UNIBG	Italy
11.	Giesecke & Devrient GmbH	GD	Germany
12.	Center for Usability Research & Engineering	CURE	Austria
13.	Europäisches Microsoft Innovations Center GmbH	EMIC	Germany
14.	SAP AG	SAP	Germany
15.	Brown University	UBR	USA

Disclaimer: *The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. Copyright 2009 by CURE, KAU and ULD.*

List of Contributors

This deliverable has been jointly authored by multiple PrimeLife partner organisations. The following list presents the contributors for the individual parts of this deliverable.

Chapter	**Author(s)**
Executive Summary	Simone Fischer-Hübner (Karlstad University)
Chapter 1 (Introduction)	Simone Fischer-Hübner (Karlstad University)
Chapter 2 (Background)	Simone Fischer-Hübner (Karlstad University)
Chapter 3 (Icons to Represent Content of a Privacy Policy)	Marit Hansen (ULD), Maren Raguse (ULD), Jan Schallaböck (ULD), Harald Zwingelberg (ULD) Section 3.1.1 Simone Fischer-Hübner (Karlstad University)
Chapter 4 (UI Prototype for Policy Display and Management)	Sections 3.1.2, 3.2 – 3.5: Christina Köffel (CURE), Peter Wolkerstorfer (CURE)
	Section 3.6: Maren Raguse (ULD)
Chapter 5 (Legal Requirements for Policy Display in SNS)	Maren Raguse (ULD)
Chapter 6 (Conclusions and Outlook)	Simone Fischer-Hübner (Karlstad University)
Appendix A (Extended PrivPref Structure and Example)	Hans Hedbom (Karlstad University), Thijs Holleboom (Karlstad University)
Appendix B (PrimeLife Online Test Questionaire)	Chrsitina Köffel (CURE), Peter Wolkerstorfer (CURE)

Executive Summary

PrimeLife aims at developing privacy-enhancing identity management systems for technically enforcing user control and information self-determination. An important prerequisite for user control in privacy-enhancing identity management are privacy policies, which can inform users about the personal data processing practices of a services side at the time when she is requested to disclose personal data to that services side. A user can in turn state her privacy preferences (data release policy) defining under which conditions she would like to release what data. The user's preferences can be compared the services side's policy, so that the user can be informed in case that her privacy preferences will not be met. In practice, privacy policies are however often containing complicated legal phases, which are not easily understood by end users. Besides, defining privacy preferences is a complex and error-prone task, which requires expertise about basic privacy principles. This deliverable by PrimeLife work package 4.3 addresses therefore the following research challenges: *How to make privacy policies easily understandable and transparent, and how to simplify privacy preference management for end users?*

For this, we first discuss related work, on which this deliverable is partly based. This includes particularly the Art. 29 Working Party Recommendation on "More Harmonised Information Provisions" suggesting a presentation of privacy policies on multiple layers. Besides, we define in a "background" chapter what information needs to be provided by a privacy policy and briefly present our approach on offering a set of three predefined privacy preference profiles (so-called "PrivPrefs"), from which end users can choose, including the most privacy-friendly ones of acting anonymous or for releasing only the minimal amount of data needed for the purpose of the requested service. For a simplified privacy preference management, our UI prototypes are based on the approach of allowing users to choose and adapt their privacy preferences "on the fly" (i.e., when a services side is requesting data from them) rather than demanding from them to define their preferences beforehand. Our concepts of PrivPrefs and "on the fly" preference management have also been previously presented in more detail in PrimeLife Deliverable D4.1.1 (HCI Research Report V1).

For increasing transparency of privacy policies, we discuss approaches, possibilities and limitations for expressing relevant policy statements in abbreviated form using so-called policy icons. A set of policy icons elaborated within WP4.3 is presented, and the need for a comprehensive approach with a fully specified "icon language" is discussed.

We then present two different UI (User Interface) prototype design approaches for policy display, where the first UI prototype approach also includes the functionality of privacy preference display and management "on the fly". The two UI prototypes were tested and compared within an Online study conducted at CURE. The online test showed that end users appreciate the functionality of privacy preference information and management. However, the study also showed that for both UI prototypes the information of what data were requested and for what purposes was differently understood by the test users: While for the first UI prototype it was clearer for the test users what data were requested, for the second prototype the test users understood better for what purposes the data were requested. The first two UI prototype designs presented all policy information (and in case of the first UI prototype, also all preference information) in one window. However, with the one-window approach it may be difficult for the users to differentiate between information on the services side's policy and information relating to the user's preferences. Therefore, alternative UI prototypes based on a multi-step approach comprising several windows for policy display and administration were developed and are also presented in this deliverable. The multi-step approach seems also to be more adequate for supporting the enforcement of the privacy principle of data

minimisation for transactions involving several service providers. It will therefore be refined and tested next.

Finally, this deliverable also elicits legal requirements for policy display UIs that will be needed for social network sites, particularly for enabling users acting as data controllers in social networks to inform other users about their (i.e. the data controllers') policies. This legal chapter at the end of this deliverable provides a basis for parts of our future work within WP4.3 on policy display user interfaces for social network sites.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Privacy-enhancing Identity Management systems, as those which are currently developed by the PrimeLife project, can provide powerful tools for technically enforcing user control and informational self-determination. Privacy-enhancing identity management implies that users can make informed decisions about the release of personal data, the selection of credentials for proving personal properties, and about their privacy and trust policy settings. For enabling users to understand the implications of data disclosures and thus to make well-informed decisions, there is a need for user interfaces (UIs) informing them in particular about the privacy policies of their communication partners. Such user interfaces should be informative while not being perceived as intrusive, and they should be intuitive, legally compliant and trustworthy.

According to Art.10 EU Data Protection Directive 95/46/EC (DPD), a privacy policy should inform data subjects at least about the identity of the data controller, the purposes for which the data are intended as well as any further information such as the categories of data and recipients concerned, her right of access to and the right to rectify her data, needed to guarantee fair personal data processing. Privacy policies whether posted on websites or contained within contractual texts often include long complicated legal statements, which are usually neither read nor understood by the end users. *Making privacy policies easily understandable and transparent is therefore an important challenge, which is addressed by PrimeLife work package 4.3* on “User Interfaces for Policy Display and Administration”. Gross et al. (Gross et al. 2006) have shown that the perceived clarity of a privacy policy increases positive reaction to the site and its goals. Hence, easily comprehensible and transparent privacy policies are not only a mean for enhancing user control, but can also serve the interests of the service providers.

Achieving better transparency of privacy policies is also the aim of privacy policy negotiation implemented within privacy-enhancing identity management systems. In the context of privacy policy negotiation, users define their release policies (or so-called privacy preferences) stating the users’ preferences regarding the disclosures of their personal data. At the services sides, a so-called data handling policy (or simply “privacy policy”) specifies how and what data are processed by the service in question. If personal data are requested from a user by a service provider, the PrimeLife user-side system can compare (“match”) the services side’s privacy policy with the user’s release policy (privacy preferences) and warn the user in case of a mismatch.

For ordinary users defining and adapting privacy preferences, in a way that they protect their privacy properly, is a complex and error-prone task which usually requires some expertise about basic legal privacy concepts and principles. In the non-electronic world no equivalent task exists, which means that ordinary users have no experiences in how to define and manage their privacy preferences. Without assistance, most users would very likely not define and use privacy preferences at all or could accidentally define or choose privacy preferences, which are not as privacy-friendly as the users would like them to be. As security and privacy protection are often secondary goals for ordinary computer users (Herzog 2007), it is indeed not realistic to assume that users will spend much time and effort on privacy configurations. Hence, *another major challenge which is also addressed by PrimeLife work package 4.3, is the simplification of privacy preference (release policy) management for end users.*

For achieving this, the user-side identity management system should provide options of predefined "standard" privacy preferences, from which a user can choose. As reported in the HCI (Human Computer Interaction) Research Report V1 (PrimeLife Deliverable D4.1.1, see (Fischer-Hübner et al. 2009)), we have in the PRIME and PrimeLife projects defined a set of three predefined privacy preference profiles (so-called "PrivPrefs"). For a simplified handling of privacy preferences, our UI prototypes are based on the approach of enabling end users to choose and customise the privacy preferences "on the fly" (i.e. when a services side is requesting data) rather than demanding from the users to select their preferences beforehand. The set of predefined privacy preferences should represent the users' privacy interests and thus also includes the most privacy-friendly options for acting anonymously (called "Anonymous") or for releasing as little information as needed for a certain service (called "Only Minimal Data").

The PrivPref concept, on which our mockups are based, is described in detail in D4.1.1 and will be summarised in chapter 2.

1.2 Objectives

The objective of this deliverable is to present and discuss initial UI prototypes and UI components produced by PrimeLife work package 4.3, which aim at addressing the challenges mentioned above, namely the challenges of providing user-friendly privacy policy displays and release policy (privacy preference) management to end users. This deliverable is reporting work in progress including alternative UI proposals, which have only been partly tested yet, and which need further iterations of subsequent improvements and tests. Results of this future work will be reported in the Deliverable D4.3.2 on "UI prototypes: Policy administration and presentation – Version 2", which will be due in project month 28.

Within the first project year, also UI Prototypes for dynamic and static policy display were produced and compared in an Online user study. This work, which focuses on alternative ways of showing UI overlays with short privacy notices, has already been reported in the HCI Research Report (D4.1.1) and is thus not included again in this deliverable.

1.3 Related work

The Article 29 Data Protection Working Party has investigated what information should be provided in what form to users in order to fulfil all legal provisions of the EU Data Protection Directive 95/46/EC for ensuring that individuals are informed of their rights to data protection (Art. 29 WP 2004). The Art. 29 Working Party recommends providing information in a "multi-layered format under which each layer should offer individuals the information needed to understand their position and make decisions". They suggest three layers of information provided to individuals: The short notice (layer 1) must offer individuals the core information required under Art. 10 DPD, which includes at least the identity of the controller and the purpose of processing. In addition, a clear indication must be given as to how the individual can access additional information. The condensed notice (layer 2) includes in addition all other relevant information required by Art. 10 DPD of the Directive such as the recipients, whether replies to questions by the data controller are obligatory or voluntary and information about the data subject's rights. The full notice (layer 3) includes in addition to layers 1 and 2 also "national legal requirements and specificities."

Our UI prototypes for policy display are based on the Art. 29 Working Party Recommendation. In addition, we investigate how this approach of multiple layers can be extended by adding standardised icons for privacy policies or policy elements to the top layer. Our work and further related work on privacy policy icons by (Rundle 2006) and (Mehldau 2007) are reported in chapter 3 of this deliverable.

The UI prototypes presented in this deliverable are only displaying the top-level view of multi-layered formatted policies. Intuitive and easily understandable presentations of condensed or full privacy policies need to be addressed by work package 4.3's future work. Some related ongoing work on presenting policy details in an easily understandable and comparable format by a so-called privacy label design was recently reported by (Kelly 2009).

Further previous work on privacy policy related HCI aspects comprises work on facilitating privacy policy authoring and management in organisations (Karat et al. 2005), (Karat et al. 2006), the usability of P3P[1] user agents (Cranor et al. 2006), and means for mediating information of P3P privacy policy compliance by websites to end users (Gideon et al. 2006), (Tsai et al. 2006), and on user interface designs for allowing end users to influence policies by dictating obligations (Pettersson et al. 2006). The related work on usability of P3P for end users is, however, not taking compliance with EU privacy legislation into consideration.

The Privacy Bird[2] is a P3P user agent that allows the user to specify her privacy preferences regarding a website's data handling policy. The privacy bird uses the traffic light metaphor for displaying information about the compliance of a site's policy with the user's preferences: If a site's policy meets the user's preferences, a small green bird icon in the browser's title bar emits a happy tweet after the page has been loaded. If the site violates the user's privacy preferences, the bird icon turns red and chirps a shrill warning when the page is first loaded. For sites that are not having a P3P policy, a yellow bird will appear. It is however questionable whether the traffic light is the right metaphor in this context, because having no privacy policy (symbolised by the yellow bird) can actually be regarded as worse than having a policy not matching the user's preferences (symbolised by the red bird). For allowing users to specify their privacy preferences, a set of three predefined preference settings is provided, which can be customised by the user during the installation process and via the privacy-bird menu. However, in contrast to the approach that we have taken, P3P does not permit to define more fine-grained privacy preferences, which could for instance be conditioned on individual data controllers and data values. Moreover, the privacy bird also does not allow changing privacy preference settings semi-automatically "on the fly".

1.4 Structure of this Deliverable

The remainder of this deliverable is structured as follows:

Chapter 2 ("Background") will provide legal definitions of roles that are revenant in the context of policies and explain how we define the content and concepts of privacy policies and privacy preferences in the context of this deliverable.

[1] Platform for Privacy Preference project, http://www.w3.org/P3P/

[2] http://www.privacybird.org/

Chapter 3 ("Icons to represent Content of a Privacy Policy") will present a set of icons for expressing relevant statements from privacy policies, which have been elaborated within task 4.3.2. Besides, the need for a comprehensive approach with a fully specified "icon language" is discussed.

Chapter 4 ("UI Prototypes for Policy Display and Management") will then present different UI prototypes for privacy policy display and preference management, which have been developed and partly tested by an online comparison study within the work of PrimeLife work package 4.3. Conclusions from the comparison tests are drawn and future directions for UI prototype development and testing within Work Package 4.3 are discussed.

Chapter 5 ("Legal Requirements for Policy Display in SNS") will then elicit the legal requirements for policy display UIs that will be needed in social networks sites (SNS) in addition to the "classical" policy UIs, which are used by SNS providers acting as data controllers, to inform their users about the SNS providers' privacy policies. This includes policy display UIs that can be used by social network users in certain situations to inform other social network users, about whom they process personal data, about their privacy policies. This chapter forms the basis for policy display UI prototypes for social communities that will be developed within the scope of task 4.3.2's future work, and is for this reason included as a form of "outlook" in the end of this deliverable.

Finally, Chapter 6 ("Conclusions") will draw overall conclusions and will provide an outlook to WP 4.3's future work in cooperation with other PrimeLife work packages.

Chapter 2

Background

In this chapter, we will first briefly provide some basic legal definitions of roles used in the context of policies, which we consequently also refer to in this deliverable. Then, we define what information needs to be contained in a services side *privacy policy* to be displayed to the user. Besides, we define what we in PrimeLife WP4.3 understand under the concept of *privacy preferences* (so-called “PrivPrefs”). This background information should help the reader to better understand the motivation and ideas behind the different icons and mockups introduced in the chapters 3 and 4 below.

2.1 Legal definitions of roles used in the context of policies

The Data Protection Directive 95/46/EC defines different roles to which rights and obligations are assigned, and which are therefore also used in the context of privacy policies. These definitions of roles are the following:

A *data controller* is a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purpose and means of the processing of personal data.

A *processor* is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

A *data subject* is an identified or identifiable natural person and personal data is any information relating to this identified or identifiable natural person.

A *third party* is any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

2.2 Privacy Policies and Preferences

2.2.1 Privacy Policies

Article 10 of the EU Directive 95/46/EC defines what privacy policy information needs to be provided to the data subject in the cases of collection of data from her:

> ***Art. 10 Data Protection Directive 95/46/EC***
> "*Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:*
>
> *(a) the identity of the controller and of his representative, if any;*
>
> *(b) the purposes of the processing for which the data are intended;*
>
> *(c) any further information such as*
>
> *the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.*"

Hence, a privacy policy must at least provide information about the identity of the controller as well as what types of data are collected for what data processing purposes (Art.10 (a), (b) DPD). If considered as "necessary", also the information stated under Art.10 (c) DPD should be provided.

In the UI prototypes introduced in chapter 4, we follow a multi-layered structuring of privacy policies as recommended by the Art.29 Working Party, where the privacy policy information displayed to the end user on top layer contains:

- What types of data are requested for what purposes;
- Whether requested data are declared by the service provider as obligatory for the provision of the service (obligatory data are marked with a "*" in our UI prototypes);
- The identity of the controller (i.e. name and contact address of the services side requesting data);
- Further information about data retention periods and possible recipients of the data ("third parties").

2.2.2 Privacy Preferences ("PrivPrefs")

Corresponding to the data controllers' duty to present a privacy policy, end users can in turn define data release policies, i.e. their privacy preferences stating under which conditions they would like to release what kind of data. During the process of policy negotiation, the user-side identity management system compares ("matches") the services side's privacy policy with the user's privacy preferences and the user can then be informed about any mismatches. As outlined in the introduction chapter 1, defining privacy preferences beforehand may be a complex and error-prone task for end users, requiring expertise about basic privacy concepts.

To simplify privacy preference management for end users, our approach within PrimeLife Activity 4 has been to specify a set of three predefined types of privacy preferences (so-called "PrivPrefs"), from which the end user can choose and which can be customised "on the fly". The concept of PrivPrefs and their "on the fly" customisation will be briefly summarised here and is defined in more detail in in the HCI Research Report V1 (D4.1.1, see (Fischer-Hübner et al. 2009)).

The first predefined PrivPref type called "Anonymous" defines the preference of releasing no personally-identifiable data at all, i.e. the preference of remaining anonymous. The second PrivPref "Only Minimal Data" defines the preference of releasing only the minimal data needed for a certain purpose. The question of what are minimal categories of data for a specific purpose, is in this context *not* defined by the contacted services side (i.e. the data controller), but should in general be defined by trusted third organisations, such as data protection commissioners. The third PrivPref called "Additional data" allows revealing more data than needed for a specific purpose (usually in return for certain benefits, e.g. to release an email address for receiving special offers as a bonus customer). For each combination of communication partner (i.e. data controller or services side) and purpose, one of these privacy preference (PrivPref) types can be assigned, meaning that this type of privacy preference will be applied if personal data is requested by that services side for that specific purpose. It should be noted that purposes can be hierarchically structured into a subset lattice (see also (Fischer-Hübner 2001, p.171)). The (sub) purposes "Shopping" and "Marketing" can be combined to a (super) purpose "Shopping and Marketing", for which a PrivPref can be assigned, if a user wants to access a website for this super purpose.

The PrivPrefs as defined in D4.1.1 can have the following structures:

("Anonymous", communication_partner, purpose)

("Only Minimal Data", communication_partner, purpose, [data categories]*)

("Additional Data", communication_partner, purpose, [data categories]$^{+}$)

In all PrivPrefs, the PrivPref type is specified as well as the combination of communication partner and purpose, for which the preference of this type should be applied. If the PrivPref is of the "Additional Data" type, the additional data categories that the user is willing to release "in addition" to the data typically strictly needed for the specified purpose are stored in the PrivPref. If the PrivPref is of the type "Only Minimal Data", the user can specify data categories in the PrivPref that she is regarding as "minimal" for the purpose in question. These data categories are complementing the list of data categories that are specified as "minimal" for a specific purpose by a trustworthy third party organisation (or more precisely: by the ontology provided by a trustworthy third organisation).

If for a combination of a services side and purpose, no PrivPref type has been assigned, the preference (PrivPref) type "Anonymous" (i.e. the most privacy-friendly option) is taken by default. If PrivPrefs have been defined for all sub purposes (e.g., "Shopping" and "Marketing") of a super purpose ("Shopping and Marketing"), alternatively the "most privacy friendly" PrivPref assigned to the sub purposes could be assigned.

Furthermore, as suggested above, these preference settings can be adapted "on the fly". If for example a user agrees to release data needed for a service (e.g., to reveal her address to a delivery service for the delivery of purchased electronic items instead of downloading them anonymously), the user will at the same time be asked whether she wants to change the PrivPref type for the respective services side and purpose from "Anonymous" to "Only Minimal Data" or override her preference only for this single event. This approach of offering predefined preferences, from which a user can choose and which she can adapt "on-the fly"', should simplify privacy policy management for the users.

Users can also be warned about excessive data requests if the PrivPref type "Only Minimal Data" has been chosen. For this, information (ore more precisely, an ontology) about the categories of data needed for certain purposes is needed, which as stated above should be provided by trustworthy third organisations such a data protection commissioners. To decide in general or automatically what data categories are needed for what purposes might however turn out to be not feasible, as specific cases will usually require specific exceptions (e.g., for the purpose "Shopping", usually the user's "shoe size" is not need – the situation is however different if the user wants to purchase shoes). Hence we can only warn users about "suspicions" of excessive data requests (which we phrased in our early mockups with "May not be minimal" (see chapter 4 below)).

The PrivPref Structure as described in the HCI Research report (D4.1.1) and as briefly presented above needs however further extensions. In addition to the data categories, it should be also possible for a user to fill in their PrivPrefs concrete data values that may be released if a service provider is contacted for a specific purpose (e.g., in case a user wants to reveal only a specific email address to a specific service provider and purpose). Furthermore, users should also be able to specify their preferences in terms of data retention periods. Our UI prototypes for PrivPref management as presented in Chapter 4 are based on this extended definition of PrivPref Structure, which we also specify more formally in form of an XML schema in Appendix A.

Chapter 3

Icons to represent Content of a Privacy Policy

3.1 Introduction

This chapter outlines aspects of improving the transparency of data processing for the user by supporting the display of a privacy policy through especially tailored icons. It describes the motivation for such an approach, as well as limitations (see section 3.2), addresses different approaches in this domain (see section 3.3), and gives an overview of elements that would need to be expressed through such a system of icons as well as a first attempt to implement such a set (see section 3.4).

The idea of expressing relevant statements from privacy policies in abbreviated form using icons was first published by Mary Rundle (Rundle 2006). Her idea was to introduce Creative Commons-like icons for the protection of private information. Creative Commons (http://creativecommons.org/) offer a set of licenses expressing an authors interest in publishing her work under certain conditions, such as permitting republication without changing the content (abbreviated the creative-commons-no-derivates, cc-nd, license) or permitting redistribution for non-commercial uses (cc-nc). Each of these licenses uses a modular concept of icons to express the core aspects of the license, which is then supported by a longer text in natural language ("human-readable") and a legal text ("lawyers-readable").

Similar to this idea, icons could in principle express core aspects of privacy policies, such as retention periods, steps and purposes of data processing, and possible recipients. For the given use case of this deliverable, the set of icons proposed in section 3.4 can be limited to express certain necessary information as other information will be already present in the information dialogue (see chapter 4). As the user has the option to choose in which purposes the data will be used for and which sets of recipients the data may be transmitted to, neither purposes nor different recipients need to be displayed. But in future steps this system may be extended to certain further use cases, for example to show limitations the sender of an e-mail or other messages wants the recipient to be aware of (e.g., retention period, right to further disseminate the messages content).

3.2 Motivation for and limitation of policy icons

In general, icons are used to visualize specific statements or properties. Well designed icons allow for quick comprehensibility for everybody who is not visually impaired.[3] In information and communication technology systems, icons are widely used, e.g., as visual elements in the user interface for using different functions in applications or as warning or information signs. Using icons to express the relevant information on what is going to happen to personal information released by a user could significantly enhance user experience, and might even support transparency, as will be shown.

In the area of privacy policies, some basic icons have been used to show a match or mismatch between the user's preferences and the web service's privacy policy, e.g., in the Privacy Bird. Moreover, the visual elements for privacy seals can be regarded as icons, which express that the legal compliance of a product or a service has been certified. These seals by themselves do not inform the users about specifics of the data processing, but usually they refer by a specific number to an audit report which can be looked up or which is already linked to the graphical representation of the privacy seal.[4]

Legislation on privacy still varies largely, especially between EU jurisdictions and the US or other countries. Therefore the information relevant for the user could also vary between those regulatory frameworks. For example, while in the US expressing the fact that personal information is deleted after being used for a specific purpose might be important for the users as otherwise data may be stored indefinitely the deletion is already mandated by the law within the EU.[5]

Driven by the fact, that privacy policies often are not read, due to their length as well as the legal diction, Art. 29 Working Party proposed the concept of layered privacy policies (Art. 29 WP 2004). They, however, didn't discuss the use of icons. Layered privacy policies offer the possibility to express only the most important statements of a privacy policy in the first layer and then give more details in further layers. Depending on the icons and their relation to data fields they can be very abstract (e.g., making clear that some data are stored) or very specific (e.g., visualizing a specific step of data processing, such as encryption). Clearly the use of icons alone, i.e., without a written privacy policy spelling out the details, cannot be a sufficient substitute of which information has to be given to the user. It is important to note that the documents from Art. 29 Working Party do not oppose the idea of icons. Further, catchy icons may be much more attractive and informative for a large group of people than texts in a very technical language or in legalese.

In the area of privacy, there are until now only very few icons for data processing and none of them standardised. As icons require the recipient to get used to their meaning, independent of their expressiveness, a wide acceptance of one set of icons is necessary, as they otherwise would not prove effective. Note that the meaning of icons is not limited to each specific icon on its own, but

[3] To ensure the accessibility also for ability impaired users, icons should be equipped with an explanatory text displayed in accordance with accessibility guidelines such as those published by the Web Accessibility Initiative of the world wide web consortium (see: http://www.w3.org/WAI/guid-tech.html last visited 23. June 2009). This would ensure that assistive technologies such as text-to-speech and Braille-bridges will be able to parse the information given. Earcons, brief sound patterns, could also be used to further raise the attention users. Matching from privacy policies and users preferences is also illsustraed with sound within privacy bird, online: http://www.privacybird.org/.

[4] See for example the European Privacy Seal, EuroPriSe: https://www.european-privacy-seal.eu/ and the Privacy Seal issued by the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): https://www.datenschutzzentrum.de/guetesiegel/.

[5] Even in the EU, such an icon might however raise awareness for the purpose limitation and data minimisation principles expressed in the Data Protection Directive 95/46/EC.

the combination of icons may be relevant for the interpretation. This also encompasses the meaning of missing icons: Think of a web service which presents a few icons on its privacy policy, but does not show an icon regarding any possible recipients of the user's data. Here the non-statement concerning a possible data transfer to a recipient could mean that there is no recipient at all or that a data transfer is not excluded but may happen from time to time, or even that there are regular recipients but the data controller has not put the icon on the web site although there may be a statement in the full privacy policy. This example shows the necessity of a detailed description of the "icon language" which may require to put up an icon on existing or non-existing data transfer and possible recipients.

At the same time, legal mechanisms would need to ensure that the meaning the user has learned to be expressed by the icons reflects the practise of the data processors and the data controllers. This can be done by using a trademark protection regime on the icons, where a license to use the trademark is only given to those binding themselves to processing within the expressed meaning. In the domain of governmental certification, also a specific law regulating the uses of certain icons could prove useful.

The domain of privacy statements is too complex to be fully explained by a small set of simple icons because they lack the – often needed – degree of detail. Imagine, e.g., an icon for data which is transferred to another party: The sole information that data are transferred is very limited. It is also necessary to state, which data are transferred to which party, plus the purpose for the transferral and further processing. Let alone the fact that, the retention period and other information are also necessary for users who want to understand what is being done with their data. In addition, the use of icons alone would only address people with good eyesight; here it is unavoidable to offer alternatives for, e.g., blind people.

3.3 Different approaches of icons

When discussing proposed sets of icons, it is important to understand their area of use. Different entities have to be distinguished:

1. the entity which sets the privacy policy which is to be expressed or abbreviated by icons;
2. the entity which decides on which icons are bound to the statements of the privacy policy and are displayed to the user;
3. the entity which interprets the icons

In the scenario which is most related to the Creative Commons model a user provides own (personal) data, e.g., via e-mail, a social network or a blog, and attaches the icons for the desired or allowed processing of these data. Here the user herself is the "data provider", and she sets the privacy policy. She also decides on the icons (coming from a standardized Creative Commons-like model) and displays them together with the data. Other users or organisations can see the data together with the icons and are obliged to handle the data according to the given policy.

In another scenario a web service as data controller sets the privacy policy and displays the icons on the web site. The web service's user interprets the icons to understand how her data will be handled. This scenario can also be modified in a way that the web service sets the (machine-readable) privacy policy which is interpreted by the user's software. This software uses the policy statements to display the appropriate icons which again are interpreted by the user herself.

Most of the discussed approaches were derived from the Creative Commons model (Rundle 2006, Mehldau 2007, Helton 2009, s.a. Bickerstaff 2008). Another model uses only a limited set of icons concerning the user's preferences and the web service's policies (Kelley 2009); here the icons only visualize the user's options in a text-based table. The mentioned icon sets are hardly comparable because they address very different data processing or privacy features and have their origin in very different legal environments. By now, none of the proposed icon sets for presenting privacy policies provides a comprehensive approach with a fully specified “icon language”. Such an “icon language” would need

- the definition of an “icon alphabet” as symbols to be used; this would contain icons as well as possible parameters (e.g., numbers representing the retention time),
- the specification of the “icon language grammar”, i.e., a set of formation rules that describe which combination of symbols from the “icon alphabet” are syntactically valid (“well-formed”); this includes the definition of mandatory and optional uses of icons as well as operators such as negation or other logical operators such as AND or OR,
- the specification of the semantics of well-formed terms, i.e., the meaning of icons alone and in combination (possibly in a defined order) plus possible parameters, and
- for practical use, the meaning should be immediately understandable, and – if possible – ill-formed terms could also be spotted right away.

The Mehldau approach provides the most sophisticated icon set and categorizes the icons according to the following classes: “What data?”, “How is my Data handled?”, “For what purpose?”, “For how long?” (Mehldau 2007). Many of these icons are quite well designed; however, for practical use there are numerous shortcomings, e.g., when describing data processing steps (from the second class) that data are first saved, then encrypted, parts of it are anonymised, some of the non-anonymised data are passed on to other parties, and then the data are erased from the original storage area – and all this could be combined with several data types, purposes and retention periods. Even if the icon set supports all these descriptions, the more complex cases won’t be easy to illustrate in a way which is easily graspable by non-experts.

Another question is hard to answer when using the mentioned icon sets in non-trivial cases: Is the privacy policy presented by the icons legally compliant with the EU law? Actually, it was obviously not the design objective of those icon sets to answer such a question, because the proposed icons aim at a neutral description of data processing instead of referring to a specific legal system. Here another interpretation layer may be necessary.

3.4 What needs to be expressed by the icon set

As stated above in section 3.2, iconography will not be able to replace full privacy policies nor may icons replace the necessary depth of explanations for the planed use of personal data (purposes) as it is necessary for an informed consent (cf. Art. 2 (h) Data Protection Directive 95/46/EC). But icons are able to offer valuable information on a first-glance basis for users and point to core issues related with the processing in a given case.

Early within the process of elaborating the icon set, it had been discussed to keep the number of icons low.[6] It was assumed that the possibility to combine or cross out icons and to add an indication for the layer of privacy in relation to the displayed subject could keep the number of necessary icons low. However, this initial aim soon proofed inefficient due to two reasons: First it became evident that there is too much varying but nevertheless relevant information to display and second in the opinion of the authors the largest user’s benefit would be to communicate, what will actually happen to the personal data e.g. how the information will be processed. Even though there are some basic types of data processing such as collection, storage, modification, transfer, and

[6] During the open space workshop organized by the EC-funded project PrivacyOS in Berlin in April 2009 there had been two sessions on the possible use of icons to resemble privacy related information, in particular the content of privacy policies. Minutes of the sessions are available online: https://www.privacyos.eu/wiki/index.php/PrivacyRightsAgreements (last visited 23 June 2009).

deletion such steps are necessary for nearly every form of data processing and thus respective icons would have minor expressiveness. As there are some kinds of processing where the interests of the data subjects are more at stake than with others, the icons set should rather intend to warn the user of possibly dangerous processing. It had thus been near at hand to create icons displaying processing steps such as profiling, cross site tracking, data aggregation and other complex procedures.

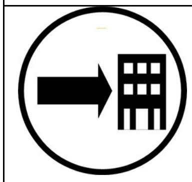
How much the diversity of the icon set influences the user-perception may be elaborated in future usability tests as well as looking for scenarios where only a reduced set of icons should be applied.

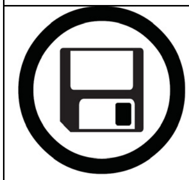
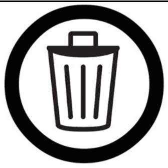
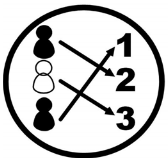
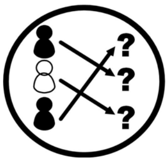
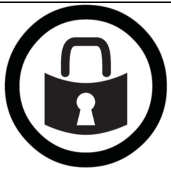
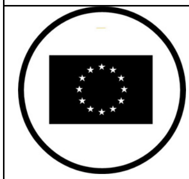
To focus the attention of the user it seems helpful to concentrate on icons that point out possible risks and other content users usually search privacy policies for or where the law provides specific requirements like for the processing of special categories of data, see. Art. 8 (2) (a) Data Protection Directive 95/46/EC. The selection of potentially dangerous processing steps is done without any prejudice or moral evaluation: While for example hidden profiling of users' behaviour or interests for purposes of targeted advertising will regularly be opposed by users, precise profiling techniques determine the true value of employee assessment or services that search for possible friends or partners with similar interest profiles. Thus the icon set attempts to cover potentially dangerous processing steps such as passing on personal data to third parties, profiling or collecting data from different sources to aggregate them.

As the set of purposes is a central element of privacy policies and also important for judging on the legitimacy of processing, it was also considered to create icons depicting purposes. But as there are a high number of purposes, it is hard to depict them in an easily understandable manner. Instead of depicting purposes some categories of recipients and data types were added to the icon set.

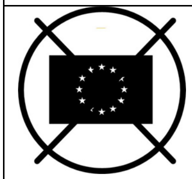
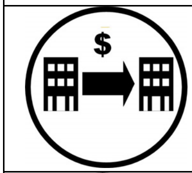
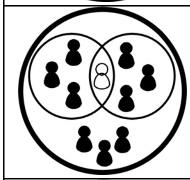
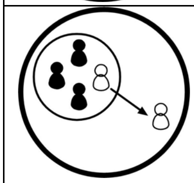
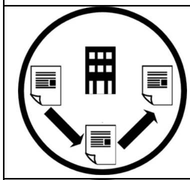
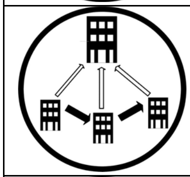
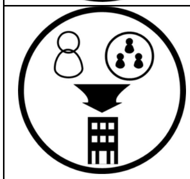
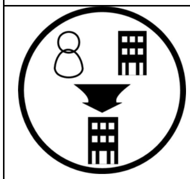
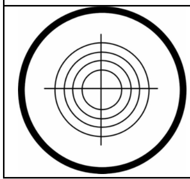
However, to make it more likely that the icons will be adopted, it is necessary to strike a balance and to include symbols that enable data controllers to show their efforts to preserve users' rights to privacy. For this purpose, processing steps which are perceived in a positive way such as encryption or anonymisation of initially personal data are included as well as the possibility to indicate that certain techniques are not deployed by crossing out an icon, thus negating its statement.

3.4.1 Icons representing data processing steps

Icon	***Short form***	***Explanation***
	Passed on	This symbol applies to any data processing step where data leaves the sphere of influence of the data controller. We suggest that this symbol is also applicable when data are processed by a data processor. While in the terms of the EC Data Protection Directive a data processor is not a third person and thus data are not "passed on", it nevertheless duplicates the data and increases the number of persons handling with these data and thus constitutes at least an abstract increase of risk for the data subjects, who are neither able to verify the credibleness of the data processor nor to check on the controls and restraints the data controller is supposed to exercise over the data processor. The sign may be combined with a symbol for indicating groups of recipients or the specific name of the receiving entity.

Icon	***Short form***	***Explanation***
	Storage	The data will be saved. An indication of the duration should be added. Icon: Mehldau 2007
	Deletion	Data will be deleted. Retention time should be indicated unless a storage period has been indicated with the Storage-Icon already in direct proximity. Icon: Mehldau 2007
	Pseudonymisation	The data will be pseudonymised. This step is usually beneficial for the protection of the user's privacy. However, the privacy policy should deliver details on who retains the data which enables a re-identification of the data subject and the conditions under which a re-identification may be carried out. Icon: based on Mehldau 2007
	Anonymisation	The data will be anonymised. The corresponding section in the privacy policy should declare within which processing stage the person related data will be anonymised. If possible, it should be indicated how well the anonymisation will exclude a direct link to the data subject, e.g., by giving the size of the anonymity set and informing on residual risks. The icon must not be used when the stored data still allows an identification of the subject or additional data are stored allowing a re-identification (see Pseudonymisation).
	Encryption	The data will be processed/passed on/stored after having been encrypted. The privacy policy should stipulate when the encryption takes place and which processing steps will be done unencrypted. It should also indicate which parties can decrypt the data and which encryption methods (algorithm, key length) are used. Icon: Mehldau 2007
	EC-law or equal protection	Legal regime for processing is European law, thus based on the protection of the Data Protection Directive 95/46/EC or the legal regime constitutes an adequate level of protection in the sense of Art. 25 of the Directive.[7] Must also be valid for any recipient of the personal information.

[7] Besides the EEA member countries (Norway, Liechtenstein and Iceland) are these Switzerland, Canada, Argentina, Guernsey, Isle of Man. Companies adhering to the US Department of Commerce's Safe Harbor Privacy Principles may require special attendance by the user in respect to the privacy policies details. See for the current status: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

Icon	***Short form***	***Explanation***
	Third Country	The legal regime of the processor or any recipient is neither European law or nor does it constitute an adequate level of protection accredited in accordance with Art. 25 (6) of the Data Protection Directive 95/46/EC.
	Financial interest	Financial interests of the data controller or of a recipient in processing the users data, in particular when the personal data are passed on against payment.
	Profiling	The data are used to create (group-)profiles of the users. Note again that this is basically neutral and may even be to the benefit of the user, e.g., for matchmaking within a dating or friend-finder scenario.
	Recognition, singularisation	The user may be (re-)recognized when accessing the service again. Applicable for any service that identifies the user in a manner that she may be singularized (e.g., with usernames, tokens, biometrics). The icon is also applicable when the service is only able to recognize that the same user or machine accesses again e.g. by setting cookies or storing IP addresses and particularly IPv6 addresses.
	Tracking, click stream	The users' interaction within the service or website is recorded.
	Cross site tracking	User may be tracked across services from different providers by virtue of third-party advertisements, Google analytics, etc.
	Data aggregation with personalized third party information	User data will be enriched with person related data collected from a third party, e.g., personalized credit rating information collected from a credit agency is processed. It is not necessary that this information will be stored when this data are processed otherwise like within a decision making process.
	Data aggregation with profile data	User data will be enriched with information from profiling processes. E.g. credit rating by virtue of information on the neighbourhood, general statements on user behaviour ("persons buying diapers are interested in picture-books")
	Targeted services	Based on the collected data targeted services will be provided tailored according to the users profile.

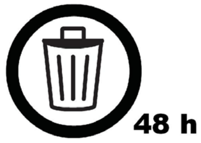
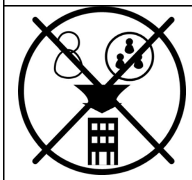
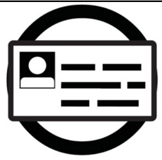
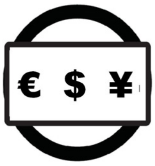
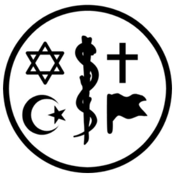
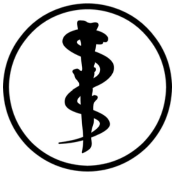
Icon	*Short form*	*Explanation*
	Duration	Durations may be indicated next to any of the icons using the units s, min, h, d and in additional m for month and y for years. See example for indicating a retention period.
	Negation	A crossed out icon means that the indicated processing step will not be carried out. Negation offers data processors to accentuate that they intentionally abstain from certain processing steps or that their mode of operation exceeds the demands of legal compliance.

Table 1 Icons on processing steps

3.4.2 Icons representing data types

Icon	*Short form*	*Explanation*
	Name, Address	Name and (physical) address are processed. Icon: Mehldau 2007
	E-mail address	E-mail address is processed. It has to be discussed whether there should be a distinction between disposable e-mail addresses with a validity for only a short time and those ensuring long-term reachability. Icon: Mehldau 2007
	Payment data	Person related payment data. Data required for payment processes such as credit card or bank account number, tax ID and other billing information but not information used in anonymous payment methods such as a prepaid PIN or Paysafecard number.
alternative ideas:   (3rd alternative diary with a lock)	Sensitive data	Special categories of data in the sense of Art 8 Data Protection Directive are processed. These include the processing of data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. Icon: Religions are in chronological order of appearance.

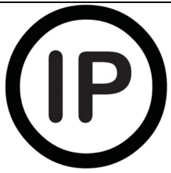
Icon	*Short form*	*Explanation*
	technical data	Technical data are stored such as the IP address, Referer, and information on the user's browser or operating system. Icon: Mehldau 2007

Table 2 Icons indicating data types processed

3.4.3 Icons representing groups of recipients

The following table shows first examples of icons to indicate specific group of recipients.

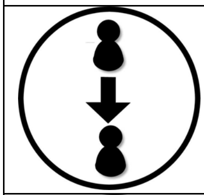
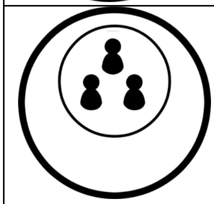
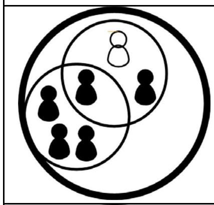
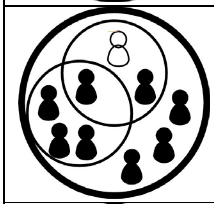
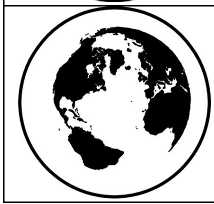
Icon	*Short form*	*Explanation*
	Data processor	Data processors are a separate entity from the data controller and handle the data for the data controller. (see also section 2.1 on the legal definition)
	Friends / within a group	In contexts where user groups are defined this icon symbolizes that the information will be distributed within such a group. In the field of social networks such a group may be referred to as friends. The group may be self-chosen (e.g., friends in a SNS, group in a SNS) or assigned by a third party (e.g., the department one works in).
	Acquaintances	Acquaintances such as friends of friends. Useful for social networks. The groups need to be closer specified by the provider.
	Whole network	All users of a given service or network get access to the data. Depending on the regulations on the access to the network this may come close to publishing the data (e.g., social networks where anyone may join).
	Data will be published	The information will be published, e.g., in papers or openly visible on the Internet.

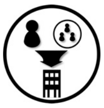
Table 3 Icons representing groups of recipients

3.4.4 Icons representing purposes

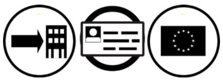
Icons representing purposes of data processing were introduced by Rundle (2006) excluding the sale of data or the use for marketing purposes and by Mehldau (2007) indicating the use of personal data for statistics, advertisement or shopping. But due to the freedom of contract and the wide variety of thinkable business cases that somehow involve processing of personal data – either as an integral element or as information necessary to perform the contract – it currently does not seem possible to produce a set of icons that is able to accurately represent the variety of purposes. Thus the written text of the privacy declaration needs to be referred to for explaining the intended use of personal data. However, the icons representing the relevant processing steps may help to point the user's attention to the relevant sections within the written policy.

3.5 Use of the icons in relation with the privacy policy

The icons should be placed where the data are collected, e.g., on paper forms or on the page containing the online form. Ideally they will link to the relevant sections of the privacy policy. In paper based environments this might function like footnotes, in online environments they will directly refer to the relevant paragraph of the privacy policy enabling a quick reference.



For the adoption by commercial companies it will be essential to have a low threshold for the implementation in real life business. The Art. 29 Working Party published their Working paper 100 (Art. 29 WP 2004) introducing the concept of multi-layered notices in November 2004. Within nearly five years only very few of such notices could be observed. This may be due to the fact that conventional privacy policies drafted as a legal text already existed and due to the fear that conflicts between the layers or omitting some information in the more abstract layers could influence the validity of the policy as a whole or may possibly even cause liability of the data controller. Using icons the threshold for making the relevant sections of the policy is lowered as it is not necessary to redraft the legal document. As for the beginning the icons may simply be inserted into the existing privacy policy like an initial in old handwritten books (see example for **data aggregation with profile data**). This will indicate the relevant sections where the processing step is described or further information on the recipients or legal regime may be given. As an additional eye catcher the relevant wording could be made bold as it has been done here to exemplify the procedure.



General information on the meaning of the icon as described in the tables above or in an abbreviated form could be given once the mouse is hovered over the respective icon (tooltip or mouse-over functionality). Further icons may be combined. In the example chosen for this paragraph the data controller would use this text to describe that she **passes on name and address data** to a data processor where both are under the **legal regime of the EC Data Protection Directive**.

3.6 Future work

The icons presented above are only a first iteration in the development cycle. The proposed icon set together with a more elaborated syntax and semantics specification will require further refinement and testing. A next step will include matching the icons to a selection of typical privacy policies in the web and offline world. This test will show whether the most important processing steps contained within the legal texts can be represented. A matching with a full privacy policy will also provide the basis for further usability tests These will show how the chosen models will be perceived and understood by users and whether some of the basic elements need further refinement.

Chapter 3

UI Prototypes for Policy Display and Management

This chapter will introduce prototypes designed to display the services sides's privacy policies and user's privacy preference information. The prototypes as presented in the following will be introduced and the composition of its content will be explained. Furthermore, two of these prototypes have been tested with users in an online evaluation. Therefore the setup of the test as well as the results will be explained in detail in this chapter. Possible implications for the further development of privacy policy interfaces will be discussed as well. Finally, alternative prototypes based on a multi-step approach are presented. These UI prototypes will be tested in the next part of the project.

4.1 Development of the UI Prototypes

4.1.1 UI Prototypes resulting from mockup meetings

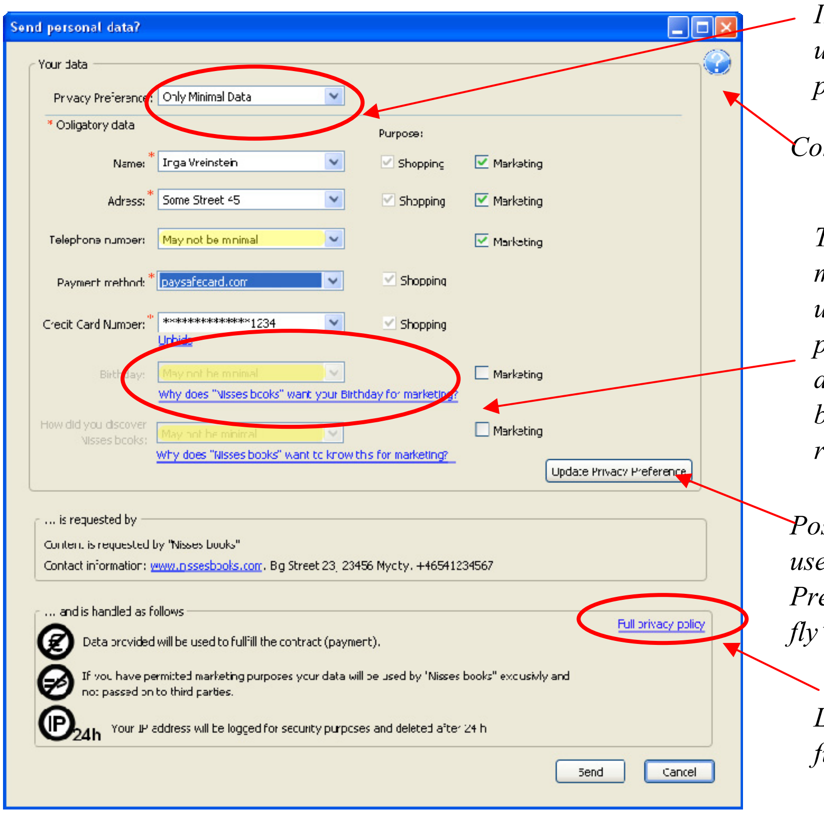
As a result of Activity 4 mockup meetings and subsequent refinements, some first prototypes for policy display and management were developed under the lead of Karlstad University. These prototypes were designed to not only display the services side's privacy policy, but also to show the user's current privacy preferences and to inform about mismatches between the user's preferences and the services side's policy. Besides, the UI prototypes enable the user to update her privacy preferences "on the fly".

Indications about a mismatch should be displayed in an informative and rather non-alarming way, because previous tests with similar policy management mockups developed in the PRIME project had shown that prominent warnings about mismatches may scare users with the result that they may even change their preference settings to more "generous" settings that are matching the services side's policy just in order to get rid of the warnings.

Our prototypes follow the multi-layered approach for displaying policies as recommended by the Art.29 Working Party (Art. 29 WP 2004). We have, however, so far only prototyped the top layer displaying the information that need to be provided to the data subjects according to Art.10 EU Directive 95/46/EC (including the requested personal data, whether it is obligatory or voluntary to provide this data, the identity of the data controller, purposes, data retention periods, as well as information about possible third parties). The condensed privacy policy can be viewed by clicking the link “Full privacy policy”. Besides, policy icons have been added to the top layer to better illustrate how the requested data will be handled by the services side. Note, however, that the icons used in our prototypes are older versions, which have meanwhile been replaced by improved icons as presented in chapter 3 of this document. However, we show here the old icons versions, as they were used in one of the prototypes, which was tested in the Online comparison study about that we report later in this chapter.

Two alternative mockups have been developed for the two cases where the user has chosen the predefined privacy preference “Only Minimal Data”. These mockups are presented in the following section 4.1.1.1. Another UI prototype for the case where the user has chosen the predefined privacy preference “Anonymous” will be shown in section 4.1.1.2.

4.1.1.1 UI prototypes for the Privacy Preference “Only Minimal Data”



Send personal data?

Your data

Privacy Preference: Only Minimal Data

* Obligatory data

Purpose:

Name:* Irga Vreinstein ☑ Shopping ☑ Marketing

Adress:* Some Street 45 ☑ Shopping ☑ Marketing

Telephone number: May not be minimal ☑ Marketing

Payment method:* paysafecard.com ☑ Shopping

Credit Card Number:* **************1234 ☑ Shopping

Unhide

Birthday: May not be minimal □ Marketing

Why does "Nisses books" want your Birthday for marketing?

How did you discover Nisses books: May not be minimal □ Marketing

Why does "Nisses books" want to know this for marketing?

Update Privacy Preference

... is requested by

Content is requested by "Nisses books"

Contact information: www.nissesbooks.com, Bg Street 23, 23456 Mycity, +46541234567

... and is handled as follows

Full privacy policy

Data provided will be used to fullfill the contract (payment).

If you have permited marketing purposes your data will be used by "Nisses books" excusivly and not passed on to third parties.

24h Your IP address will be logged for security purposes and deleted after 24 h

Send Cancel

Information about the user’s current privacy preference

Context-sensitive help

The text “May not be minimal” infoms the user that her preferences of minimal data disclosure may not be fulfilled if she releases these data

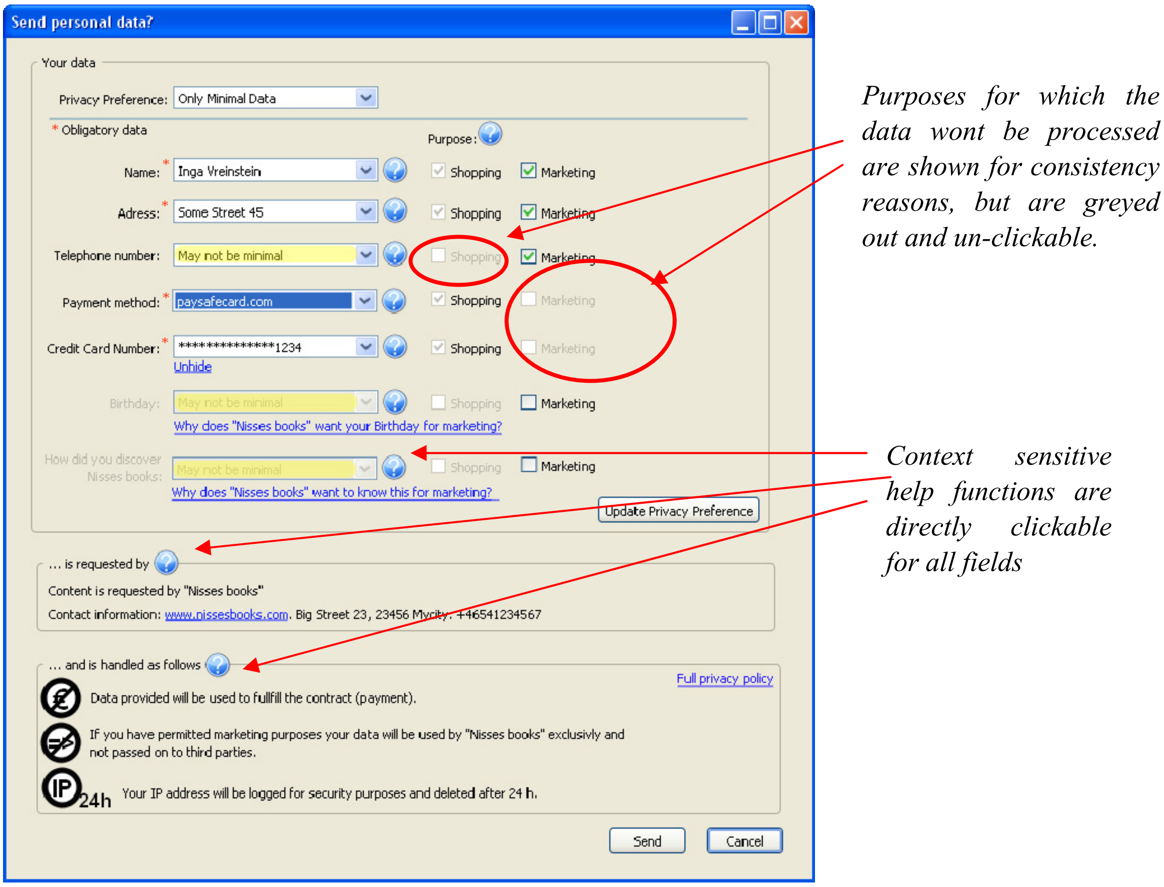
Possibility to update the user’s Privacy Preferences ”on the fly”

Links to the condensed or full privacy policy

Figure 1. First UI Prototype for Policy Display and Management for the Preference “Only Minimal Data”

Figure 1 depicts one of the mockups for Policy Display and Management where the user’s current privacy preference is “Only Minimal Data”, i.e. the user wants to release only the minimal data needed for the requested service. The current Privacy Preference is displayed at the top of the “Your data” section. This section also displays what data is requested by the services side for what purposes. Purposes for which the user can “opt-in” have empty boxes placed before them, which the user can click (e.g., in Figure 1, the user has already opted in that her name, address and telephone number can be used for marketing). Purposes that are not optional have greyed-out clicked boxes before them, which cannot be un-clicked. Data that are obligatory, i.e. data that are according to the services side’s policy mandatory for the service, are marked with a red asterix. Data fields in the drop-down boxes are pre-filled with the values that are stored in the user’s current privacy preference. The pre-filled values can however be changed by the user (e.g., the user could in this example choose an alternative delivery address or credit card number). If more data is requested by the services side than what is assumed to be minimal[8], the information “May not be minimal” in grey letters with yellow background colour is shown in the data fields. This shall inform the user about the fact that her preferences of minimal data disclosure may not be fulfilled if she provides this type of data. If this concerns data fields marked as obligatory by the service provider’s policy, this can particularly mean that there may be a mismatch between the user’s preferences “Only Minimal Data” and the services side’s policy. As it is not possible to automatically decide for all cases whether certain data categories will be needed for certain purposes, we have chosen the wording “May not be minimal” to inform the user about the possibility of excessive data requests without definitively stating that the data request is really “not minimal”. If more data is requested than what we assume to be minimal, there may also be a link displayed, where the user can click to be informed why the services side would like to know this data. For instance, a vendor might be interested in the customer’s birth date for target marketing and might in return send present vouchers over a certain amount to the customer at her birth date. With this information, a customer may do more informed decisions about providing additional data and opting in for marketing or not.

If the user has made any changes in the “Your data” fields (such as in our case, where she has opted in for marketing), the field “Update Privacy Preference” will be clickable to allow the user to change her privacy preferences or to store them under a new name “on the fly”.



Send personal data?

Your data

Privacy Preference: Only Minimal Data

* Obligatory data

Purpose:

Name:* Inga Vreinstein ☑ Shopping ☑ Marketing

Adress:* Some Street 45 ☑ Shopping ☑ Marketing

Telephone number: May not be minimal □ Shopping ☑ Marketing

Payment method:* paysafecard.com ☑ Shopping □ Marketing

Credit Card Number:* **************1234 ☑ Shopping □ Marketing
Unhide

Birthday: May not be minimal □ Shopping □ Marketing
Why does "Nisses books" want your Birthday for marketing?

How did you discover Nisses books: May not be minimal □ Shopping □ Marketing
Why does "Nisses books" want to know this for marketing?

Update Privacy Preference

... is requested by

Content is requested by "Nisses books"

Contact information: www.nissesbooks.com. Big Street 23, 23456 Mycity. +46541234567

... and is handled as follows

Full privacy policy

Data provided will be used to fullfill the contract (payment).

If you have permitted marketing purposes your data will be used by "Nisses books" exclusivly and not passed on to third parties.

Your IP address will be logged for security purposes and deleted after 24 h.

Purposes for which the data wont be processed are shown for consistency reasons, but are greyed out and un-clickable.

Context sensitive help functions are directly clickable for all fields

Figure 2. Second UI Prototype for Policy Display and Management for the Preference “Only Minimal Data” (denoted as Prototype A in the conducted comparison study)

[8] To decide what data categories are regarded as “minimal” for a certain purpose, an ontology provided by a trustworthy third organization, is used (see section 2.2.2 for more details).

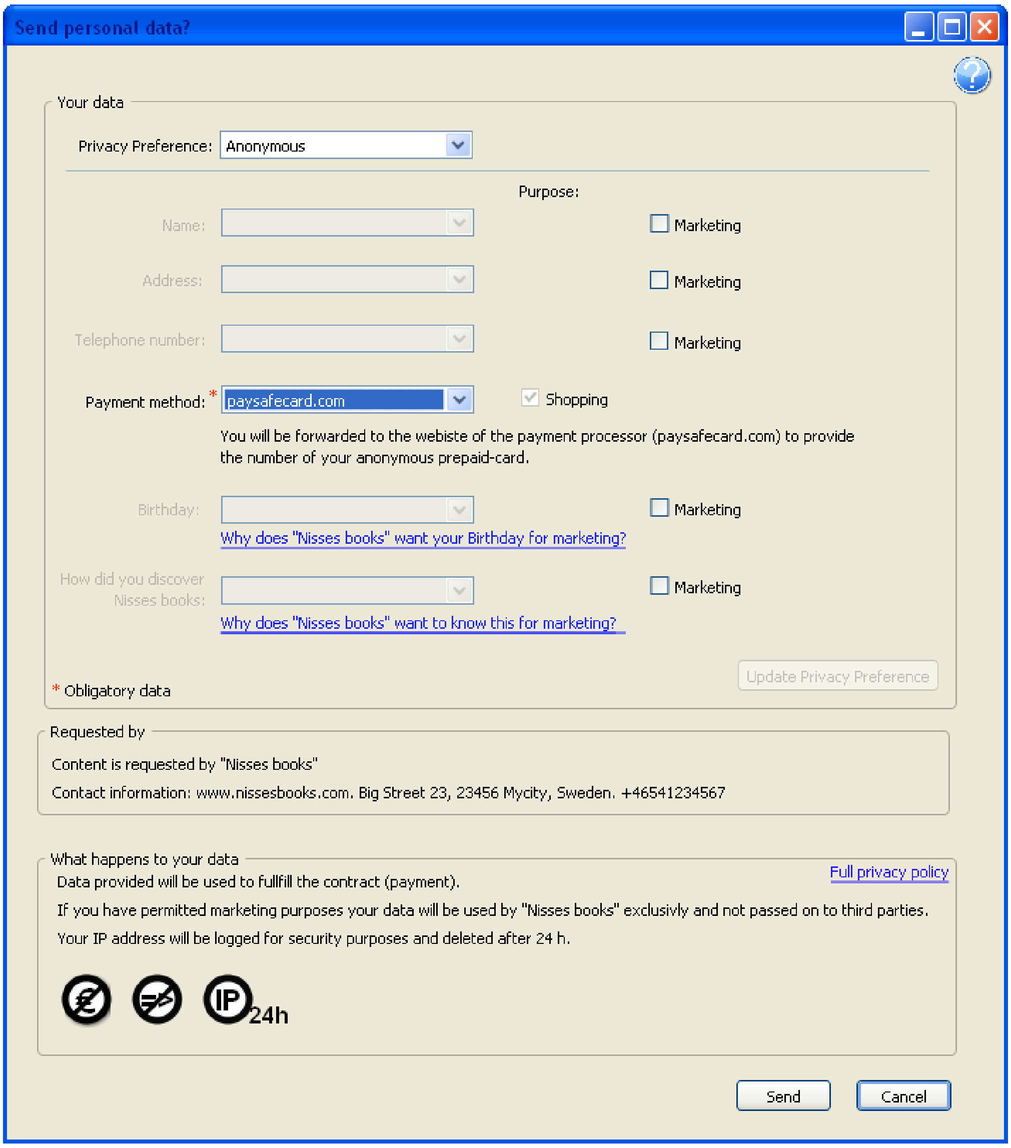
Figure 2 shows an alternative policy display and administration mockup for the privacy preference "Only Minimal Data", which implements further design proposals by CURE. One main difference between the prototypes is basically the way how context-sensitive help is offered. In the prototype depicted in Figure 1, the user can simply click the question mark with the effect that the mouse pointer's shape changes to a question mark, and then, after the user clicks a field, the help appears. In the prototype depicted in Figure 2, help options are directly shown for each field. This might illustrate the help options better for users that are not familiar with context-sensitive help functions as offered by the prototype depicted in Figure 1. On the other hand, the "Your data" area gets more crowded. Another difference is that for consistency reasons, purposes, for which data wont be used, are shown, however in grey letters with an un-clicked greyed-out box before to them.

This second UI prototype was chosen as one of the prototypes for the Online tests and comparison study conducted by CURE, which will be described below. In this study, this prototype will be denoted as "Prototype A".

4.1.1.2 UI prototype for the Privacy Preference "Anonymous"

Figure 3 below shows another UI prototype that has been developed for the case that the user's current privacy preference is "Anonymous", i.e. the user's preference is not to release any personal data. As no personally identifiable data is required for the purpose Shopping, the respective data fields (Name, Address, Telephone Number, etc.) are greyed-out. The anonymous prepaid card method "paysafecard.com"[9] is filled in as the payment method. Prepaid paysafecards can be anonymously purchased at kiosks or gasoline stations. They use a one time card number, which cannot be associated with the (anonymous) buyer of the card. Hence, if paysafecard is used for online payments, no personally identifiable data of the user is released to the services side. If no anonymous payment method was offered by the services side, the user would be informed about a mismatch with her privacy preference to be anonymous.

[9] http://www.paysafecard.com/de/



Send personal data?

Your data

Privacy Preference: Anonymous

Purpose:

Name: ☐ Marketing

Address: ☐ Marketing

Telephone number: ☐ Marketing

Payment method: * paysafecard.com ☑ Shopping

You will be forwarded to the webiste of the payment processor (paysafecard.com) to provide the number of your anonymous prepaid-card.

Birthday: ☐ Marketing

Why does "Nisses books" want your Birthday for marketing?

How did you discover Nisses books: ☐ Marketing

Why does "Nisses books" want to know this for marketing?

* Obligatory data

Update Privacy Preference

Requested by

Content is requested by "Nisses books"

Contact information: www.nissesbooks.com. Big Street 23, 23456 Mycity, Sweden. +46541234567

What happens to your data

Full privacy policy

Data provided will be used to fullfill the contract (payment).

If you have permitted marketing purposes your data will be used by "Nisses books" exclusivly and not passed on to third parties.

Your IP address will be logged for security purposes and deleted after 24 h.

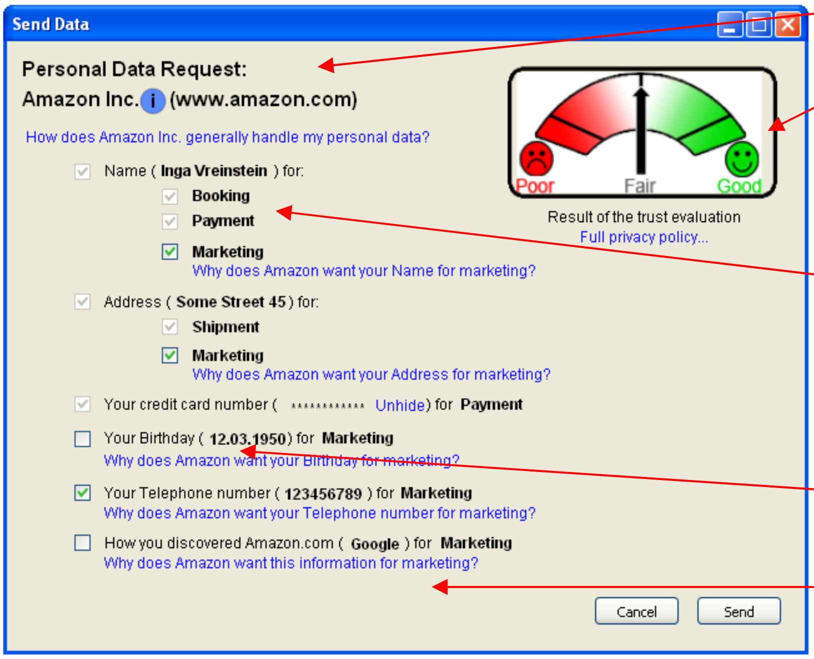
Figure 3. UI Prototype for Policy Display and Management for the Preference "Anonymous".

In the prototypes, the field "Update Privacy Preference" is greyed-out, as long as the user does not make any changes to the field in the "Your data" area.

4.1.2 Alternative UI Prototype for policy display

In order to gather a deeper insight into the users' preferences and tendencies and to obtain clear decisions on certain interface aspects, it was decided at the Activity 4 meeting in April 2009 in Kiel to develop an alternative prototype. Given the choice of two prototypes containing the similar information, the users should be able to express their preferences for one of the prototypes more clearly. Especially the possibility to compare the interfaces against each other gives the participants the opportunity to decide on certain aspects of the interface. Furthermore a clear tendency for future developments can be gathered.

To enable a direct comparison, CURE developed an alternative prototype (see Figure 4, which will be called "Prototype B" in this document). To obtain reliable results and to offer a valuable alternative for the display of the information disclosed, a completely different approach was chosen. Therefore this prototype rather disregards the chosen privacy preferences but focuses on the display of the information sent and the purposes it is disclosed for. Since previous studies have indicated that users especially appreciated and relied on the graphical display of the privacy evaluation results, this feature was included in the interface. Furthermore expandability was a major point for designing the prototype. The interface was designed to be flexible and adaptable to different amounts of disclosed information. To reduce the users' mental load, the prototype was therefore designed to only expand vertically. For this reason, it is also concentrated on displaying only the major information such as data disclosed and the trustworthiness of the provider. A concept that has also been adopted by the prototype designed by Karlstad University, are the greyed-out boxes, indicating that this information is required by the provider in order to complete the transaction. Additionally the user is provided information about the recipient of the data and the purposes of use in both prototypes.



Send Data

Personal Data Request:
Amazon Inc. (www.amazon.com)

How does Amazon Inc. generally handle my personal data?

☑ Name (Inga Vreinstein) for:
☑ Booking
☑ Payment
☑ Marketing
Why does Amazon want your Name for marketing?

☑ Address (Some Street 45) for:
☑ Shipment
☑ Marketing
Why does Amazon want your Address for marketing?

☑ Your credit card number (************ Unhide) for Payment

□ Your Birthday (12.03.1950) for Marketing
Why does Amazon want your Birthday for marketing?

☑ Your Telephone number (123456789) for Marketing
Why does Amazon want your Telephone number for marketing?

□ How you discovered Amazon.com (Google) for Marketing
Why does Amazon want this information for marketing?

Cancel Send

Result of the trust evaluation
Full privacy policy...

Information about the provider

Graphical display of the evaluation of the trustworthiness of the provider

The purposes the name is used for. The greyed-out boxes indicate that this data has to be sent to complete the transaction (non-clickable)

Contextual help

Vertical expandability only

Figure 4. The alternative prototype developed by CURE (Prototype B).

4.2 Test Setup and Background

As indicated before the main objective of the test was to gather user opinions to determine trends and usability issues in PET user interfaces. To reach a larger number of users within a short period of time, a similar approach as the Virtual Usability Laboratory (Fischer-Hübner et al. 2009) that has already proven to be efficient has been chosen.

The test was designed in accordance to (Nielsen 1994) as an online questionnaire, where the users had the possibility to first examine and evaluate the prototypes individually and then make a direct comparison between them (within-subjects design). Since the prototypes were not functional (i.e. screen mockups), the users were given the images of the interfaces and asked to imagine their usage.

To avoid biasing of the results by potential influences of the sequence of the prototypes shown, two versions of the questionnaire with counterbalanced sequencing have been created. Both prototypes were designed to display exactly the same amount and type of information (except the privacy preferences) to enable an optimal comparison.

The questionnaire did not only contain possibilities to express the first impression the user got from the interface, it also contained a MicroPET-USEs, a condensed version of the PET-USEs (Fischer-Hübner et al. 2009). The PET-USEs are a scale to measure the usability of privacy related aspects in user interfaces. They were developed by KAU as part of Activity 4 in PrimeLife and are further described in D 4.1.1. The scale is very modular and can therefore also be applied in a condensed version as in the current case.

Furthermore questions concerning the displayed policies and the term "privacy preferences" were asked for both prototypes. After the evaluation of the single prototypes separated from each other, the users were asked to compare the prototypes against each other. The direct comparison of the interfaces contained questions concerning their appearance, display of the data, structure of the information, trustworthiness, treatment of the personal data, understandability of the interfaces, information conveyed and the users' overall preferences. Another question was asked on whether both interfaces contained the same amount of information. For statistical reasons also demographic data and the users' interest in protecting their personal data were asked. The entire questionnaire can be seen in Appendix A.

4.3 Test Conduction

The questionnaire was available for participation on CURE's survey-website. Because of temporal constraints, the questionnaire was available to the users for one week (Tuesday, 19th May 2009 to Tuesday, 26th May 2009). Access to the questionnaire was restricted by invitation, i.e. the users got an invitation by e-mail containing a link to the questionnaire. The study was conducted in German, although the images of the prototypes were presented in English. The 44 questions were separated by topic on 4 pages.

The 71 contacted participants were selected from CURE's test user database and were invited by e-mail. The e-mail invitation also included basic background information to the PrimeLife project. Several of the invited users have already been contacted for previous surveys and have volunteered to answer further questionnaires. The users did not obtain any kind of compensation for their participation.

4.4 Results

Eliminating the incomplete questionnaires (some users did not fill out the entire questionnaire) we obtained 18 fully filled-in forms, resulting in a response rate of 14 % (of 71 users contacted). Given the relatively short time for answering the questionnaire this rate can still be considered as good.

As mentioned above to avoid biasing, two versions of the questionnaire with different sequencing of the prototypes were created. Overall 11 users answered the questionnaire showing Prototype B (CURE) first and 7 participants filled in the questionnaire starting with Prototype A (KAU). The results indicate that there might be a slight positive bias for Prototype A, when Prototype B was displayed first. Nevertheless this bias can be disregarded since it follows the overall tendency and is therefore not statistically significant.

4.4.1 Demographic Information

All study participants were native German speakers, and three participants reported issues connected to the English language. These annotations contained recommendations to translate the interface to German and one participant indicated that the interface is not easy understandable for non-native speakers.

It was especially taken care of that an equal number of male and female members of CURE's test user database were contacted. Nevertheless a slight majority of male participants replied. Overall we could acquire 10 male (55.5 %) and 8 female (44.4 %) participants. The average age of the participants was 39.9 years (median 39.5 years) which indicates that also a larger number of middle-aged users participated in the survey (see Figure 5). In fact the largest age group of users was aged between 31 and 40 years. Also a respectable number of elderly users (2 users older than 60 years) participated in our survey. Therefore we can conclude that the entire age range of the PrimeLife Personas is well represented in this study.

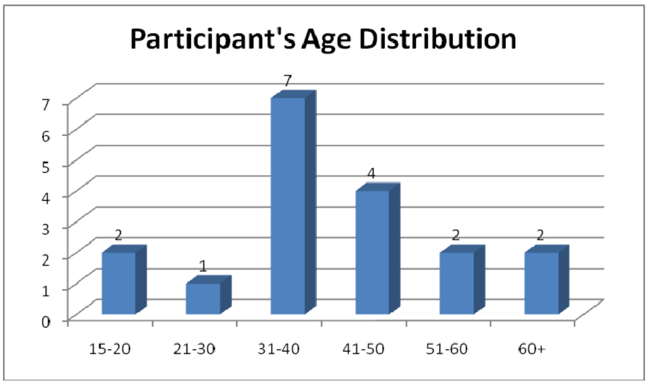


Figure 5. Age distribution of the participants

The distribution of the users' profession and salary is in accordance to the aforementioned distribution of ages. Therefore the majority of participants (11 participants, 61.1 %) works as an employee. Three participants reported on being either pupils or students. Other professions represented in the study were worker, retiree and being unemployed. The distribution of the participants' education is shown in Figure 1Figure 6. Almost halve of the volunteers (44.4 %) were higher educated (i.e. university).

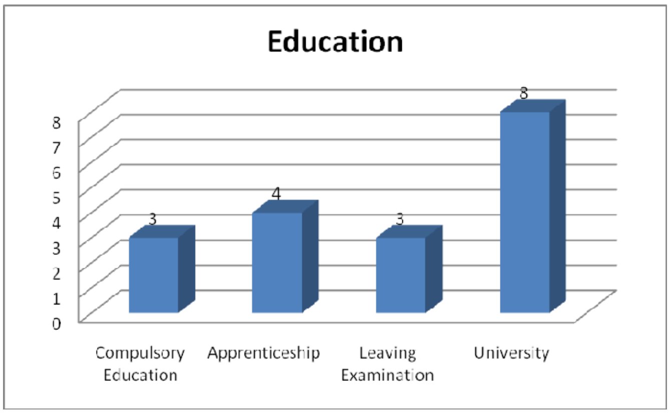


Figure 6. The distribution of the level of education, as indicated by the participants

The users were also enquired about their interest in data protection and whether or not they care about protecting their personal data. The vast majority of the participants indicated to either be very interested (10 participants, 55.5 %) or at least somehow interested (6 participants, 33.3 %) in protecting their private information. Only one user indicated only being mildly interested and one user stated that she is not at all interested in protecting her privacy.

4.4.2 MicroPET-USEs

For the MicroPET-USEs the users were asked questions concerning security, consistency, trust and confidence in the handling of the data. These questions were posed for both prototypes to gather the individual differences. The users had the possibility to answer on a 7-scale Likert Scale ranging from the positive attribute to the negative one.

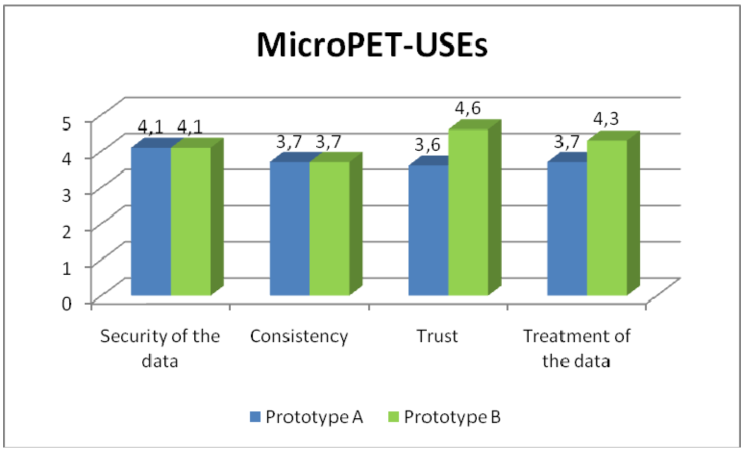


Figure 7. The results of the MicroPET-USEs

The results for both prototypes are indicated in Figure 7. (For MicroPET-USEs, lower values indicate a positive ranking). As can be seen, the users were quite uncertain concerning the security of the data. It seems that the users did not have the impression that their data is secure using both interfaces. The results concerning consistency appear more positive and are shortly above the average for both interfaces. When looking at the results for the trustworthiness and the treatment of the data, the first differences between the two prototypes can be detected. Prototype A appears both, more trustworthy and more reliable in the treatment of the data than Prototype B. This especially conforms to the direct comparison between both interfaces as presented later in this chapter.

4.4.3 Purpose of the Interface

When enquired about whether they know what the interface is about, 77.7 % of the users replied to having a good idea of the interface for Prototype A and 72.2 % of the participants indicated to know what Prototype B should be used for.

When the users were asked to specify what they think the interface is supposed to be used for, they indicated several possible usage scenarios (see Figure 8). For both interfaces 4 users each indicated that the information is used for buying a product or paying for it. Interestingly double as many users stated that they get information about what the data is used for and how it is used in case of Prototype B than for Prototype A. This could indicate that Prototype B conveys the purpose of the interface more clearly than Prototype A. The drop down boxes as used in interface A together with the larger scaled interface could be an indicator to the users that information is required and could further draw their locus of attention away from the purpose, etc. In conformance to the previous findings, more users feel that Prototype A has a main objective to gather personal data from the users in order to either use them for profiling or to sell them to third parties.

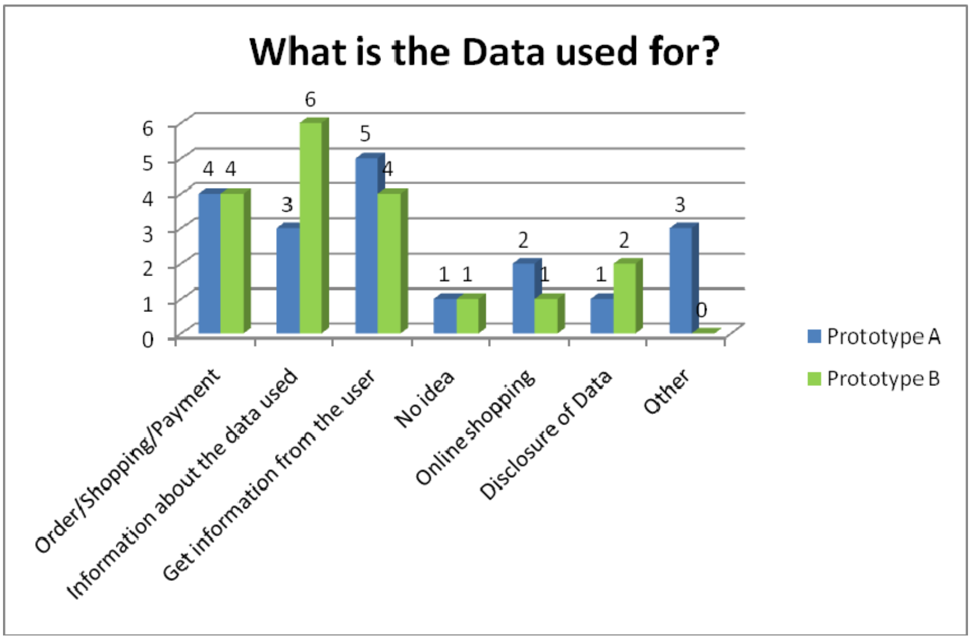


Figure 8. Assumed use of the data

According to the survey participants, Prototype B could also be rather a questionnaire to gather information/feedback for the provider. Other uses of Prototype A are according to the participants in the area of online shopping.

In Figure 9, the users' assumption of the type of data that are disclosed is indicated. Prototype A seems to be clearer on the disclosure of personal and financial information such as name, address and credit card number. Prototype B seems to rather indicate that also the telephone number and the date of birth are disclosed at all the time. Summarizing it appears that Prototype A indicates more clearly what data is required (obligatory, i.e. name, address and credit card number), whereas Prototype B rather invokes the picture of a more comprehensive data disclosure.

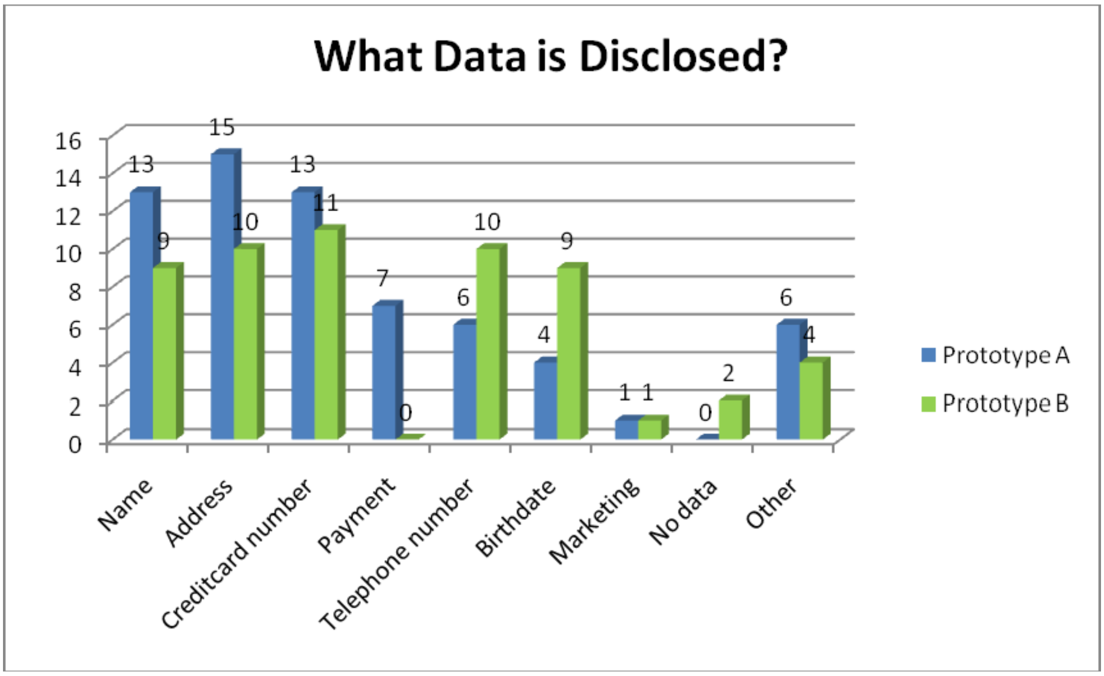


Figure 9. Type of data disclosed according to participants

4.4.4 Privacy Preferences

In the course of the questionnaire the participants were also asked about their understanding of the term "Privacy Preferences". Figure 10 indicates the users' definitions. The majority of users of Prototype A indicated that they think the term states the possibility for the user to limit or restrict the information disclosed. Prototype B does not invoke many associations with the term, resulting in 7 users (38.9 %) stating that they did not know what the term should mean. This is likely caused by the fact that Prototype B was designed disregarding privacy preferences and therefore did not contain any information about them. The differences between the two prototypes indicate that the users have noticed the possibility to chose privacy preferences in Prototype A and that they also have an idea on how they can be used.

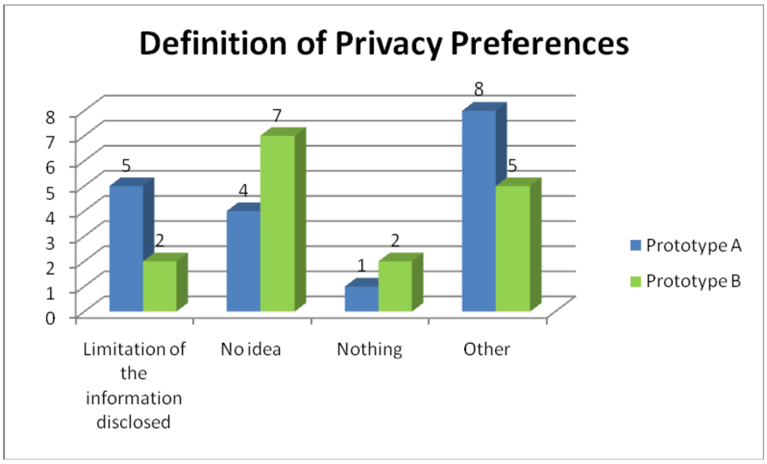


Figure 10. The users' definition of the term "Privacy Preferences"

Other statements associated to the term in connection with Prototype A that were only made by one user each:

- The user can choose a profile such as "only minimal data"
- The disclosed data is further used
- The user has options for shopping and different buying behaviours
- Sensitive information is sent over the internet
- The entered data can be sorted and reviewed before sending it
- Indication that the data is handled trustworthy
- The website the information is sent to is not secure

Statements connected to Prototype B that were only expressed by one user each are as follows:

- No third person gets access to the data
- Self-chosen security signs
- Technical platform for exchanging data that is below the data protection directive
- Preferred settings of a website
- How safe the data is treated

Overall all users indicated that they would like to use privacy preferences for different purposes. While only two thirds of the users wanted to use the application for staying anonymous while shopping, almost 90 % (for both prototypes) indicated that they would like to have privacy preferences in order to be warned when too much information is requested. Therefore it seems that users in fact want to be informed when personal information is requested, but do not fully understand the terms in use. Furthermore this positively supports the decision on using privacy preferences in future mockups.

4.4.5 Greyed-out Boxes

To get a better understanding of the users' mental model and to get insights into the users' comprehension of the prototype, the participants were asked to describe what the greyed-out check boxes meant to them. This aspect was also a major amendment to both prototypes to indicate that this information is obligatory and cannot be changed. In case of Prototype A, 7 users made this right assumption and 9 users made the right statement for Prototype B (see Figure 11).

A quite common assumption was that the greyed-out boxes indicate that the information is already known to the provider and therefore this information cannot be "un-sent". Only few users stated that they have no idea what the greyed-out boxes should mean. Nevertheless these findings indicate that in fact sophisticated help mechanisms are needed to make the interfaces more understandable.

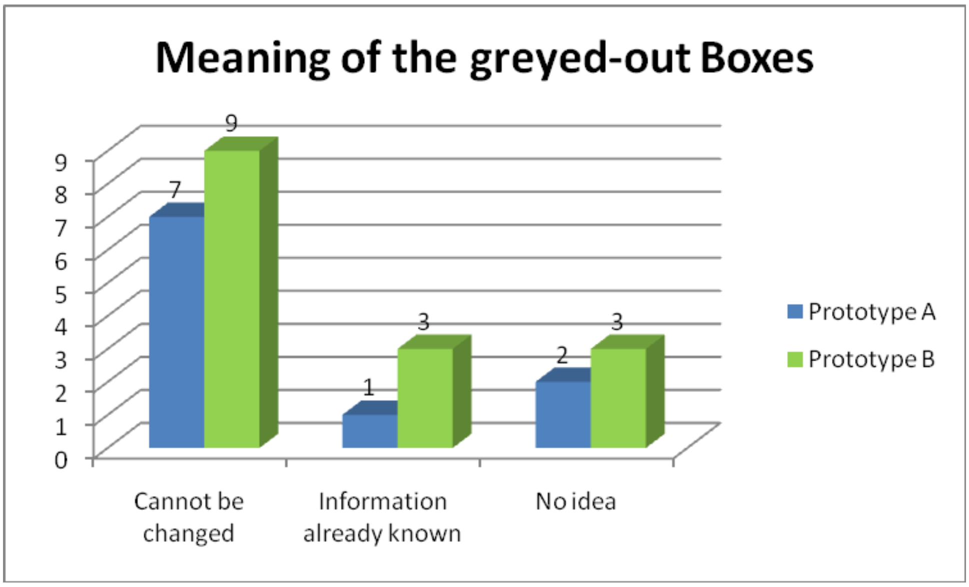


Figure 11. The users' perception of the greyed-out boxes

Prototype A has provoked a series of different definitions (all stated by one user each):

- The information is not filled in
- This indicates what information is not allowed to be used
- The information is invalid
- It indicates the purpose the data is used for (e.g. shopping, marketing)
- Selection of interest
- These field are not obligatory
- Advertising, shopping

Prototype B has shown fewer problems in the comprehension. Only three phrases (not available, invalid and purpose of the site) were stated in addition to the ones as indicated in Figure 11.

4.4.6 Direct Comparison

When asked whether or not both interfaces contained the same (amount of) information, exactly 50 % of the participants indicated that the interfaces contain different types of information. Four of those users stated that the major difference between the two prototypes is that Prototype A contains more information or the information displayed is more obvious. Two more users stated that the major difference is that Prototype A appears to permit user-entered information such as name and address in the drop down fields. As other discrepancies the options available and the difference between the data were stated. One comment was caused by an oversight – a user did not realize that both interfaces contained information about the birthday.

In the overall ranking of different aspects the users were asked to vote for the prototype they prefer according to the stated feature. As indicated in Figure 12, the majority of users preferred Prototype A over Prototype B. Despite this clear decision, Prototype B still appears to have high rankings concerning nice appearance, clearly structure and it might also be quite understandable. Nevertheless the results clearly indicate that the users prefer Prototype A for several reasons, also including its overall appearance.

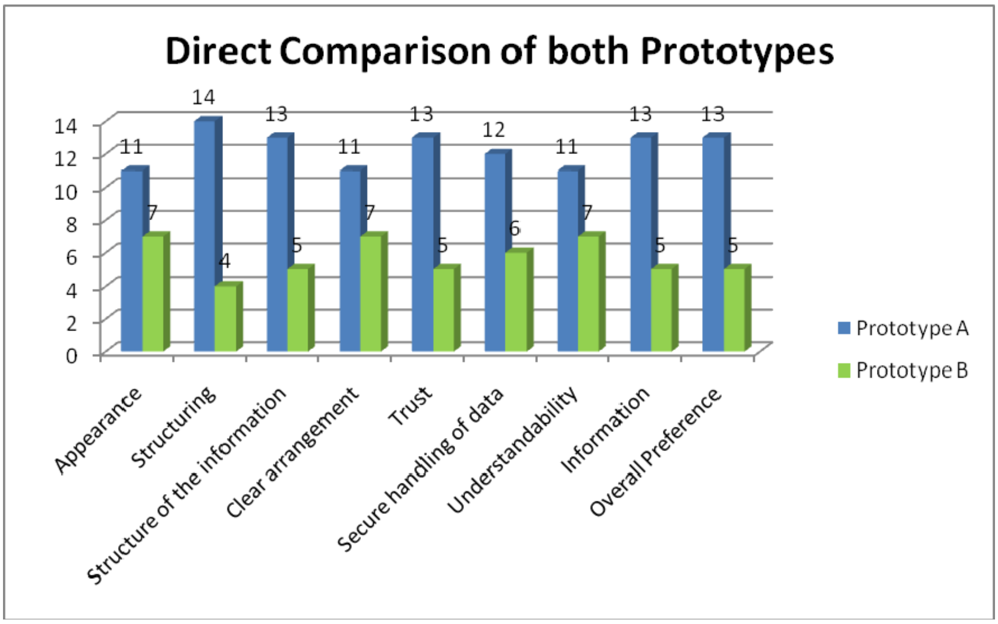


Figure 12. The direct comparison of both prototypes

As a part of the direct comparison of the two interfaces the users were also asked to state advantages one prototype has when compared to the other one. For Prototype A these advantages were as follows:

- Reliability (2 users)
- Structure (2 users)
- Better display (2 users)
- Absense of smileys (2 users)

Other reasons such as more precise display, more information, clear display of security warnings have also be indicated by one user respectively.

The major advantages of Prototype B compared to Prototype A are as follows:

- Better structuring (4 users)
- The scale as indicator for the security of a website (4 users)

Other mentionings were the lower number of gray boxes, usability and the term “may not be minimal” that was not understood by one user. Two users also mentioned that it is not clear why data can be entered into one interface and not in the other one. This fact might have also influenced the evaluation of the two interfaces.

4.5 Discussion and Conclusions from the Tests

The results of the questionnaire clearly indicate that the users prefer Prototype A over Prototype B. Especially in the direct comparison between both prototypes the 18 representative users have favoured Prototype A over Prototype B for several reasons. Nevertheless there are cases where the users have valued Prototype B because of different features over Prototype A. These aspects should be considered when implementing the next iteration of the interface.

Some inconsistencies surfaced through the evaluation. For example, the drop down boxes have caused confusion amongst the participants, which also led the users to the assumption that the two interfaces were in fact different. Nevertheless no user explicitly stated that the major difference between the interfaces were the selectable privacy preferences and the displayed information about a mismatch between the user's preferences.

A very controversial part of Prototype B is the display of the trust evaluation results. While at least three users stated that the graphics including the smileys appear immature and childish, four users positively mentioned the result in the evaluation. They even indicated that they relied on the evaluation result to get a good overview of the trustworthiness of the evaluated provider. Previous experience (through the evaluation of previous prototypes) (Fischer-Hübner et al. 2009) has indicated that the users in fact valued the graphical display to get an overall impression of the website. Therefore further investigation on the appreciation of the graphical display of privacy evaluation results should be conducted.

As already stated above, the overall tendency indicates that the users will much rely on additional inputs in form of help and tutorials. This was especially made clear in case of the greyed-out check boxes. Although the majority of the participants associated them with the right functionality, it appears that part of the population is not entirely familiar with this concept. These misconceptions could be counteracted by tutorials that assist the user upon first using the system and help-files that clarify all possible questions.

Concerning the purpose of the interface, the users associated more positive aspects to Prototype B. This indicates that although the users preferred Prototype A because of the structuring and the optical appearance, the purpose of the interface is much clearer for Prototype B. It appears that the minimalistic design that only focuses on major areas of the interface (i.e. whom am I sending what and why?) allows the users to get a better overall image of the interface. Therefore it is suggested to incorporate these aspects in the future design of the interface, e.g. by reducing the amount of information displayed.

Prototype A appears to give the users a better overview of the data disclosure. The users seem better informed about what data has to be disclosed (i.e. is required by the provider) and what information is optional.

The current study has also demonstrated a good application of the MicroPET-USEs. Although the results of the MicroPET-USEs indicate a clear trend and better results for Prototype A, they are not entirely conform to the direct comparison of the prototypes. Therefore further investigation is recommended in order to more closely adapt the MicroPET-USEs to the users' needs.

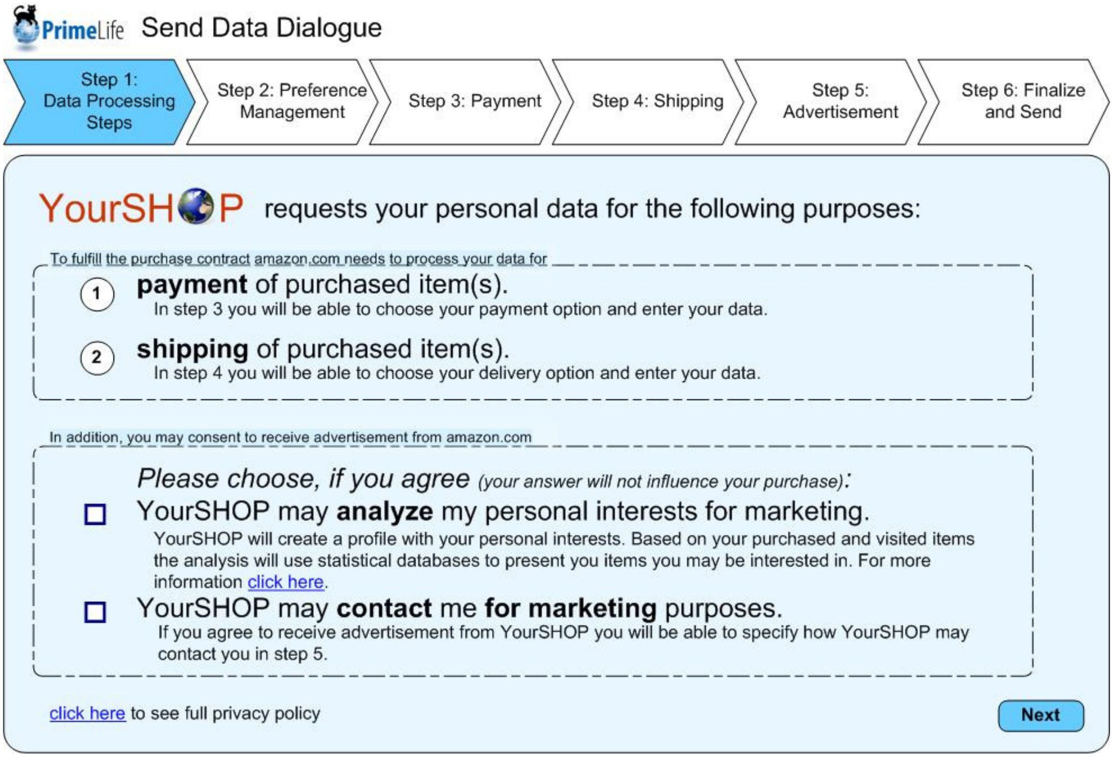
Summarizing the evaluation has indicated that Prototype A is more appreciated by the users. Nevertheless improvements, especially to make the interface appear trustworthy and professional at the same time have to be made. Additional need is indicated in the clarification of used privacy terms such as "Privacy Preferences". It appears that users do not have a comprehensive mental model concerning privacy-related terms and the loss of personal data, an assumption that is also supported by current research such as (Bratus et al. 2008).

4.6 Future Work

In this section, an alternative approach to the "one-window" UI prototypes presented above is shown. It has been elaborated by PrimeLife partner ULD taking further legal aspects as well as some of the test results reported above into consideration. Within the scope of our future work, these alternative mockups will be further refined and tested.

Presenting all relevant information and options in one window aims at providing transparency at one glance. However, displaying complex steps such as server side policies and data requests and the matching with the user's privacy preferences (or data handling policies) may overstrain average users. In the current "one-window" approach it is especially difficult for the user to differentiate between server side policies (and data requests), the user side "PrivPrefs" and the management thereof. In addition, in the current prototypes the solution to obtain the user's consent for marketing is not adequate to fulfil the legal requirement of an "informed" consent: in order for the consent to be in conformity with the law it is not sufficient to only present a check-box and the word "marketing". For an informed consent the data subject must be provided with a general description of the intended data processing, and possible third party recipients of the data (if applicable). Using the term "marketing" does not make sufficiently clear whether the user consents only to being contacted for marketing purposes by the data controller or whether the user consents also to being profiled in order to allow personalized advertisement. As the latter data processing step is frequently carried out by many online shops but also other websites, this should be reflected in the prototype. We are therefore suggesting to test whether a multi-step *Send Data* dialogue will increase comprehensibility and transparency for the user in comparison to the "one-window" approach.

First mockups, which will however need some further refinements before testing them, are presented below. Refinements will include icons to summarize the privacy policy.



PrimeLife Send Data Dialogue

Step 1: Data Processing Steps
Step 2: Preference Management
Step 3: Payment
Step 4: Shipping
Step 5: Advertisement
Step 6: Finalize and Send

YourSHOP requests your personal data for the following purposes:

To fulfill the purchase contract amazon.com needs to process your data for

1 **payment** of purchased item(s).
In step 3 you will be able to choose your payment option and enter your data.

2 **shipping** of purchased item(s).
In step 4 you will be able to choose your delivery option and enter your data.

In addition, you may consent to receive advertisement from amazon.com

Please choose, if you agree *(your answer will not influence your purchase)*:

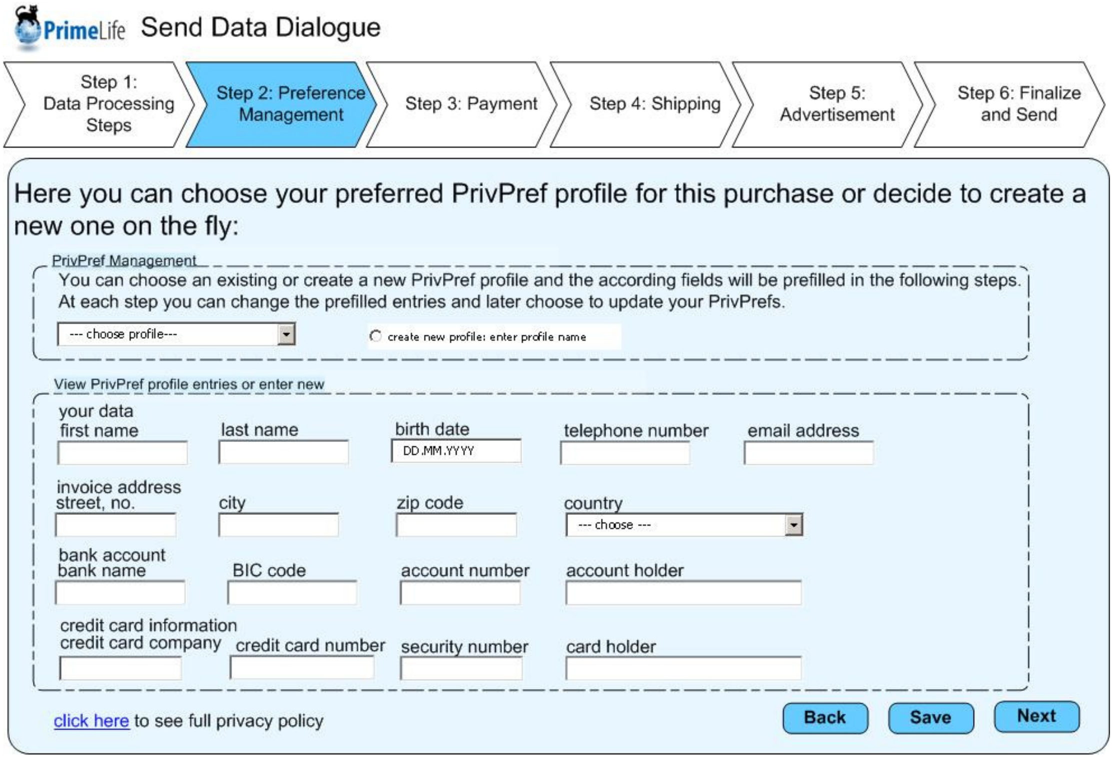
□ YourSHOP may **analyze** my personal interests for marketing.
YourSHOP will create a profile with your personal interests. Based on your purchased and visited items the analysis will use statistical databases to present you items you may be interested in. For more information click here.

□ YourSHOP may **contact** me **for marketing** purposes.
If you agree to receive advertisement from YourSHOP you will be able to specify how YourSHOP may contact you in step 5.

click here to see full privacy policy

Figure 13: Step 1 "Data Processing Steps"

Step 1 presents an overview of the services side data request focusing on the purposes specified by the services side. It differentiates between on one hand such purposes which are part of the closed contract or transaction and where processing personal data is necessary to fulfil the contract and on the other hand such purposes which are not covered by a legal provision or a closed contract and which therefore require the data subject's consent. The obligatory data requested from the services side is indicated by adding (*) to the according data item in the following steps (see figures on steps 3 to 6 below).



PrimeLife Send Data Dialogue

Step 1: Data Processing Steps
Step 2: Preference Management
Step 3: Payment
Step 4: Shipping
Step 5: Advertisement
Step 6: Finalize and Send

Here you can choose your preferred PrivPref profile for this purchase or decide to create a new one on the fly:

PrivPref Management

You can choose an existing or create a new PrivPref profile and the according fields will be prefilled in the following steps. At each step you can change the prefilled entries and later choose to update your PrivPrefs.

--- choose profile--- ○ create new profile: enter profile name

View PrivPref profile entries or enter new

your data

first name: last name: birth date: DD.MM.YYYY telephone number: email address:

invoice address

street, no.: city: zip code: country: --- choose ---

bank account

bank name: BIC code: account number: account holder:

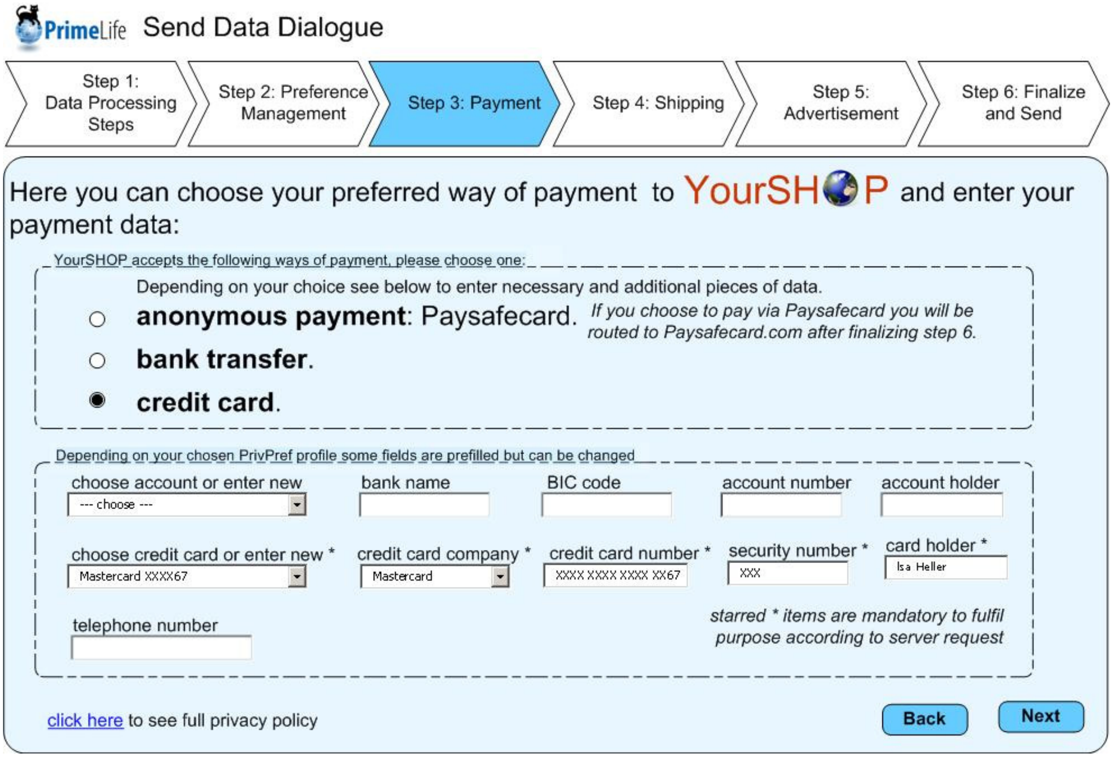
credit card information

credit card company: credit card number: security number: card holder:

click here to see full privacy policy

Figure 14: Step 2 "Preference Management"

Step 2 presents the currently existing PrivPref profiles stored in the user's PrivPref Manager on the user's client. It allows choosing one of the existing profiles and thereby prefilling data fields in Steps 3 and 4 according to the profile settings. If the user picks an existing profile the corresponding data items are displayed below. The user can change each data item and thus manage her PrivPref profile on the fly. Additionally, the user may choose to create a new profile.



Here you can choose your preferred way of payment to YourSHOP and enter your payment data:

YourSHOP accepts the following ways of payment, please choose one:

Depending on your choice see below to enter necessary and additional pieces of data.

○ **anonymous payment**: Paysafecard. *If you choose to pay via Paysafecard you will be routed to Paysafecard.com after finalizing step 6.*

○ **bank transfer**.

● **credit card**.

Depending on your chosen PrivPref profile some fields are prefilled but can be changed

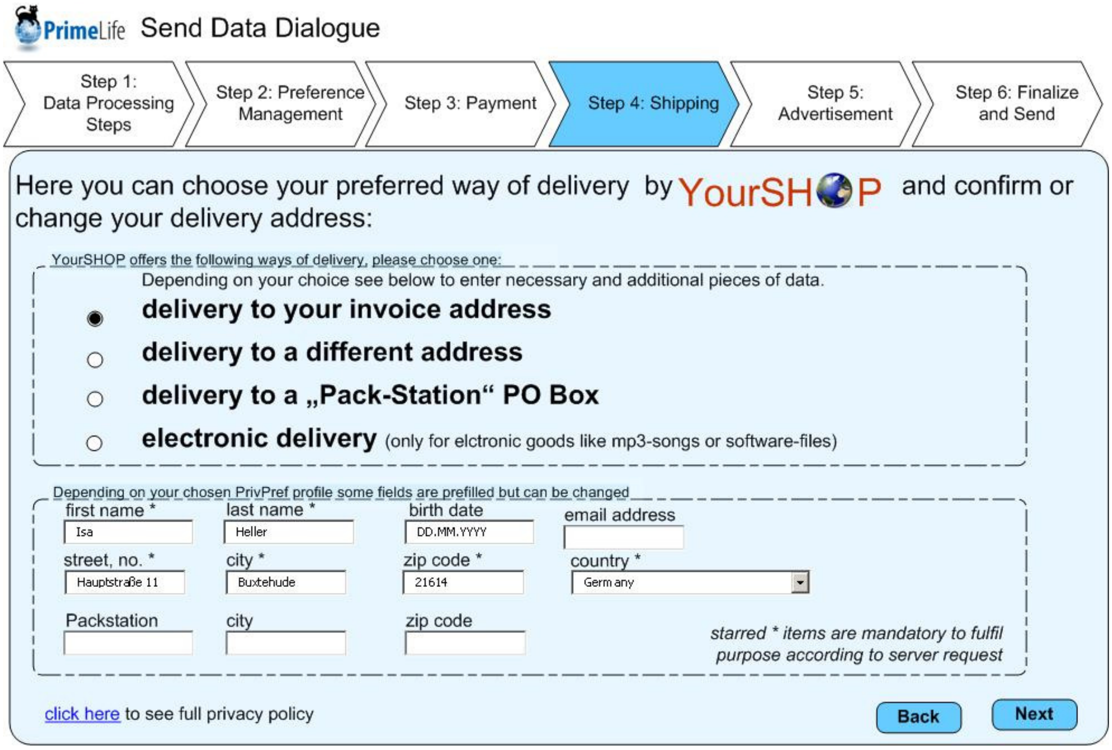
choose account or enter new	bank name	BIC code	account number	account holder
--- choose ---				
choose credit card or enter new *	credit card company *	credit card number *	security number *	card holder *
Mastercard XXXX67	Mastercard	XXXX XXXX XXXX XX67	XXX	Isa Heller
telephone number				

*starred * items are mandatory to fulfil purpose according to server request*

click here to see full privacy policy

Figure 15: Step 3 "Payment"

In Step 3 the user can further specify which way of payment she prefers and what data to send to the requesting server and data controller. The fields are prefilled according to the PrivPref profile chosen and the entries can be changed. Starred (*) items are requested by the server and are mandatory. If this request mismatches with the chosen PrivPref profile, this will be indicated. This could be done by means of highlighting mismatches by colouring the respective fields or by means of an overlay mask which will only display the mismatching data items.



PrimeLife Send Data Dialogue

Step 1: Data Processing Steps | Step 2: Preference Management | Step 3: Payment | **Step 4: Shipping** | Step 5: Advertisement | Step 6: Finalize and Send

Here you can choose your preferred way of delivery by YourSHOP and confirm or change your delivery address:

YourSHOP offers the following ways of delivery, please choose one:

Depending on your choice see below to enter necessary and additional pieces of data.

● **delivery to your invoice address**

○ **delivery to a different address**

○ **delivery to a „Pack-Station“ PO Box**

○ **electronic delivery** (only for elctronic goods like mp3-songs or software-files)

Depending on your chosen PrivPref profile some fields are prefilled but can be changed

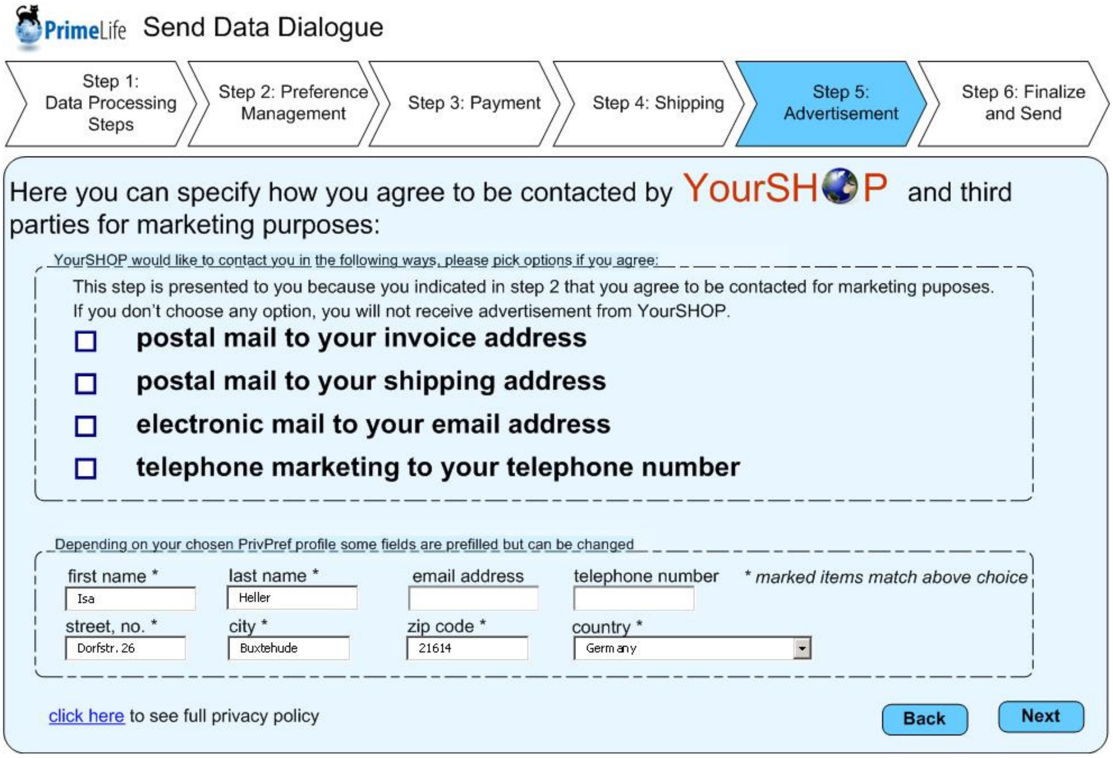
first name *	last name *	birth date	email address
Isa	Heller	DD.MM.YYYY	
street, no. *	city *	zip code *	country *
Hauptstraße 11	Buxtehude	21614	Germany
Packstation	city	zip code	

*starred * items are mandatory to fulfil purpose according to server request*

click here to see full privacy policy

Figure 16: Step 4 "Shipping"

In Step 4 the preferred way of delivery can be picked. According to the choice made the requested data items will be starred * below and prefilled following the chosen PrivPref profile. Mismatches of server side data request and the privacy preferences of the user will be indicated.



PrimeLife Send Data Dialogue

Step 1: Data Processing Steps | Step 2: Preference Management | Step 3: Payment | Step 4: Shipping | **Step 5: Advertisement** | Step 6: Finalize and Send

Here you can specify how you agree to be contacted by YourSHOP and third parties for marketing purposes:

YourSHOP would like to contact you in the following ways, please pick options if you agree:

This step is presented to you because you indicated in step 2 that you agree to be contacted for marketing puposes. If you don't choose any option, you will not receive advertisement from YourSHOP.

□ **postal mail to your invoice address**

□ **postal mail to your shipping address**

□ **electronic mail to your email address**

□ **telephone marketing to your telephone number**

Depending on your chosen PrivPref profile some fields are prefilled but can be changed

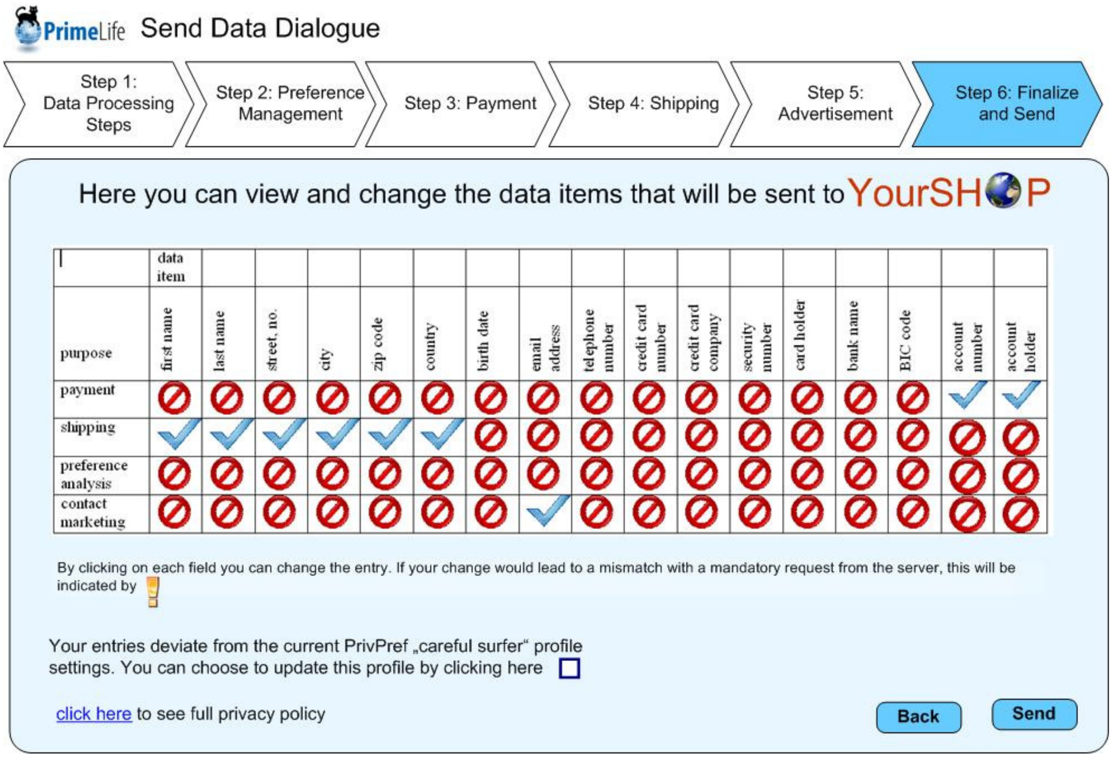
first name *	last name *	email address	telephone number
Isa	Heller		
street, no. *	city *	zip code *	country *
Dorfstr. 26	Buxtehude	21614	Germany

** marked items match above choice*

click here to see full privacy policy

Figure 17: Step 5 "Advertisement"

Step 5 will only be displayed if the user indicated her consent to receiving marketing from the data controller (and possibly third parties) in Step 1. The user can opt-in to the requested ways of being contacted and the data items requested from the server for the picked way(s) of contacting the user will be starred * below. The user can change the prefilled entries. Currently the mockup does not contain an option to differentiate between marketing by the data controller and third parties.



Here you can view and change the data items that will be sent to YourSHOP

	data item																
purpose	first name	last name	street, no.	city	zip code	country	birth date	email address	telephone number	credit card number	credit card company	security number	card holder	bank name	BIC code	account number	account holder
payment	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✓	✓
shipping	✓	✓	✓	✓	✓	✓	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘
preference analysis	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘
contact marketing	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✓	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘

By clicking on each field you can change the entry. If your change would lead to a mismatch with a mandatory request from the server, this will be indicated by !

Your entries deviate from the current PrivPref „careful surfer" profile settings. You can choose to update this profile by clicking here □

click here to see full privacy policy

Figure 18: Step 6 "Finalize and Send"

In Step 6 the result of the previous choices of prefilled entries are presented. This step should also list the entered data for each field which would be submitted to the requesting server. The user can choose to save changes made to existing PrivPref profiles.

Overall the dynamic approach is intended to make clearer which purposes of data processing the requesting server (data controller) is stating and differentiate between purposes which are part of fulfilling a contract and such purposes which require the data subject's consent. As many websites use such a multi-stepped approach already, it is likely that users will easily adapt to the additional steps involved.

Furthermore, a clear separation between server side policies (request) and user side preferences and the management thereof shall be achieved.

By guiding the user through several steps and giving her short explanations of her options the mockup aims at providing more transparency on what and where the user can choose to change data items.

Moreover, another advantage is that this multi-step approach seems also to be more adequate for supporting the enforcement of the privacy principle of data minimisation for transactions, where more than one service provider is involved. For example, for an e-Shopping transaction, the principle of data minimisation will be best supported if the e-Shop, payment and shipping providers receive only the data needed for completing their tasks. This means instead of sending payment and address information to the e-Shop, the e-Shop should only learn what items have been ordered, while the payment provider receives the payment information and the shipping provider the address details for delivery. Such complex data disclosure scenarios may be handled in a more user-friendly manner with a multi-step approach than with one-window user interfaces.

In addition, the mockup fulfils the requirement of obtaining an "informed" consent.

Chapter 4

Legal Requirements for Policy Display in SNS

This chapter will give an overview of the privacy rights and obligations of the parties concerned with provisioning and use of social network services, summarizing the findings from H1.2.2 *Analysis of privacy and access control issues in social networks and collaborative workspaces and selection of use cases for further research*. In addition, legal aspects of policy display will be presented. In a next step, these legal obligations and rights will be mapped to design requirements for HCI and especially policy display in social network sites (SNS).

The objective of this chapter is thus to elicit the legal requirements for policy display UIs, that will be needed in SNS in addition to "classical" policy UIs, with which SNS providers in their roles as data controllers inform their users about their privacy policies. This includes for instance policy display UIs that can be used by SNS users in certain situations to inform other SNS users, e.g. about whom they process personal data or about their privacy policies.

Even though such specific UI prototypes for SNS have not been developed yet, we have included this chapter in this deliverable, as it will be the basis of policy display UI prototypes for SNS to be developed within the scope of Work Package 4.3's future work.

5.1 Privacy rights and obligations in SNS – findings from H1.2.2

The rights and obligations regulated in the Data Protection Directive (95/46/EC) – DPD – are assigned to roles defined therein. The DPD differentiates between the data controller, the processor, the data subject, and third parties. All of these parties can be involved in the data processing taking place during the provisioning and use of a social network service.

A *data controller* is a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purpose and means of the processing of personal data.

A *processor* is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

A *data subject* is an identified or identifiable natural person and personal data is any information relating to this identified or identifiable natural person.

A *third party* is any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

In order to analyze which party has to comply with the obligations regulated in the DPD it is necessary to analyze the existing roles in a social network service. In H1.2.2 social network sites have been defined as ICT mediated services that allow individuals to

1. construct a public or semi-public profile within a bounded system,
2. articulate a list of other users with whom they share a connection, and
3. view and traverse their list of connections and those made by others within the system.

Widely used examples of SNS comprise Facebook, Friendster, LinkedIn, MySpace, Bebo, Orkut, Hyves, StudiVZ, Cyworld, QQ or Skyrock. Several data processing steps can be differentiated in SNS usage and analyzed with regard to the existing legal grounds and duties:

- collection of registration data,
- collection of profile data,
- making available profile data,
- making available personal data about other people in one's own profile,
- using profile data for personalized advertisement,
- using personal data for other services (e.g. search engines or Facebook applications).

The SNS provider collects, disseminates and stores the personal data entered by the user during the registration process and when extending the user profile. Further data processing by the SNS provider may include analyzing the personal data for providing personalized advertisement on the platform.

The SNS user enters data about herself in her profile. In addition, users can enter and thus make available personal information about other individuals who may or even may not be users of the same SNS. This data can be information entered on other users' walls, on group pages or on one's own profile, or uploaded as photos of other people.

Third parties using the data can be search engine providers accessing the profile data and presenting the data as search query results. Furthermore, some SNS enable access of so called widgets and other applications of third party application providers to user profile data. Such services may e.g. offer applications which run within the SNS's environment such as small games, calculating a horoscope based on personal data such as the user's birthday. While it is possible that such additional services are offered by the SNS provider these applications are increasingly ran by third parties.

The following figure exemplifies possible relations in a SNS scenario.

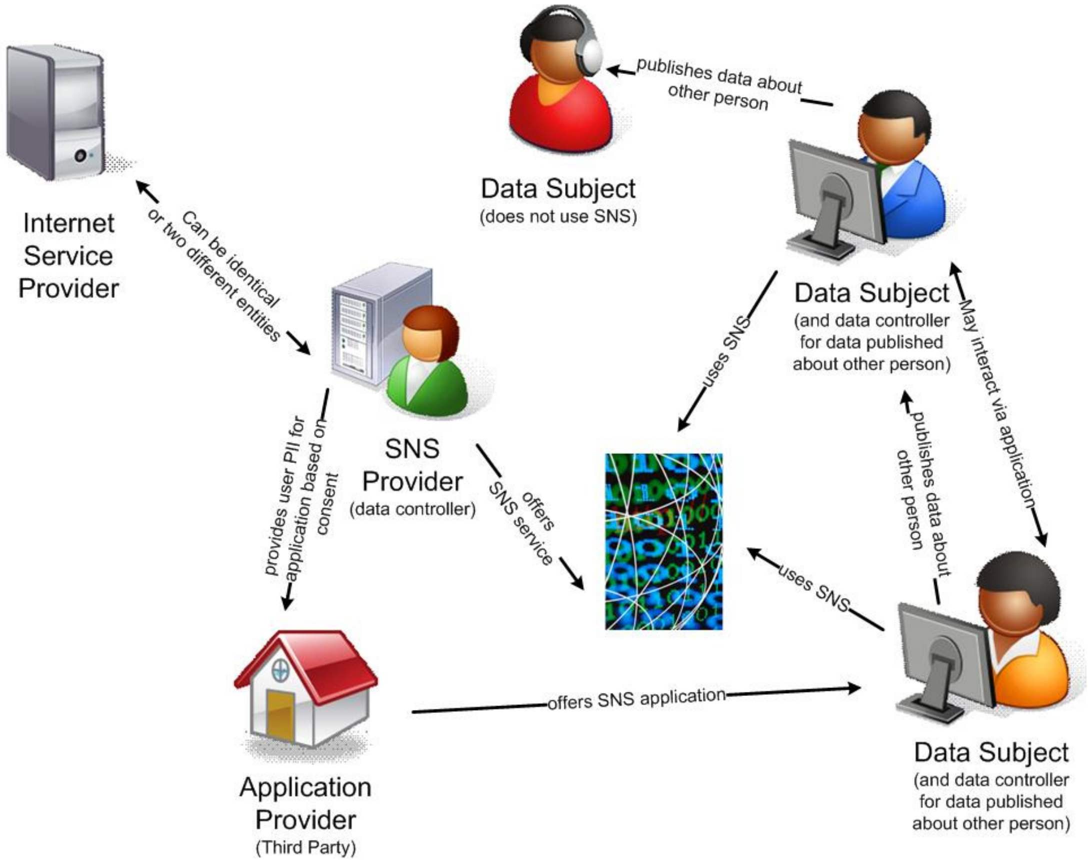

Internet Service Provider
Can be identical or two different entities
Data Subject
(does not use SNS)
publishes data about other person
Data Subject
(and data controller for data published about other person)
May interact via application
SNS Provider
(data controller)
provides user PII for application based on consent
offers SNS service
uses SNS
uses SNS
publishes data about other person
offers SNS application
Application Provider
(Third Party)
Data Subject
(and data controller for data published about other person)

Figure 19:Relations in SNS

Determining who is data controller of data processed in SNS requires an analysis of who is the one processing personal data and deciding on the purposes and means of such processing. A certain level of decision-making power on the purposes of data processing is necessary to be regarded a data controller. A SNS user exercises a decision-making power on whether or not she wants to provide a particular piece of information in her profile or on other sites of the SNS and on which application she decides to use.[10] The overall design of the SNS, the technical means of data processing and the decision-making power to provide the SNS service (as a business case and with the goal of financial revenue) is governed by the SNS provider.

A SNS user can be qualified as the controller but only of those processing operations for which she can really determine the purpose and way of processing. Thus, the user can be attributed the controllership with regard to the information that she decides to provide and processing operations she initiates. Especially for data entered by the SNS user which is referring to other individuals she must be regarded data controller under the below described circumstances.

The SNS provider can be attributed the controllership with regard to the information provided by the users and the processing operations carried out as the provider determines the purpose of the entire service. Such a situation of joint controllership may be given e.g. when a user publishes a picture of herself and friends which is accessible for all users of the SNS or accessible by search engines.

It must be possible to legitimize the data processing occurring in SNS for the respective data controllers. Thus, a legal provision or the data subject's consent must allow the specific

[10] H1.2.2 *Privacy in Social Software*, p. 66.

processing. While for data which individuals post about themselves on their profile or other sites of the SNS, this decision resembles the execution of the right of informational self-determination (that is, if the data subject is able to assess the consequences of the processing), this is not the case for data SNS users post about other people who may even be unaware of information referring to them being posted.

If the national legislation of the EU member states does not provide a legal ground for the processing, it is necessary to obtain the data subject's consent. Thus, from an HCI perspective, the SNS must provide information to the SNS user and in that scenario data processor at the instance when she is about to publish personal data about other individuals (and the household exemption does not apply, see below).

5.2 Specific legal questions with HCI implication

Art. 3 – Household exemption

The main question currently being discussed in Activity 4 is whether users that process other users' data in virtual communities should or must have a privacy policy and how such policies should look like. This is of importance for task 4.2.3, as the data track is also storing negotiated policies for data released to communication partners, as well as for task 4.3.2 (policy negotiations in virtual communities). The first question arising in this context is whether Art. 3 DPD (so called household exemption) can be applied with the consequence that the other articles of the Directive do not apply? In other words: Does the processing of other peoples personal data in virtual communities equal data processing for purely private purposes? The household exemption applies only if the users publishing third person's data have restricted access to their profile to self-selected friends and when they do not mainly use the SNS for commercial goals.[11] If the user allows access to her profile by groups she does not know or control the scope of publishing data on her profile which equals publishing it on the entire web (for example in Facebook the network of a user's hometown may in some cases have several million members, for example the New York network). In this case, the processing can no longer be regarded to take place for purely personal or household activities. From a practical perspective, this conclusion requires technical tools to assist the user and to clarify the "status" of her profile and the data processing initiated therein. The SNS provider should provide general information about when the household exemption applies and when it does not and should also inform the user of what consequences this has (that is, if the user is regarded a data controller, she has to comply with the obligations of the DPD). In addition, the SNS provider should, each time a user wants to join a network in which the user does not control the number of members and is about to allow access to her profile to all network or group members, or when she sets her access control settings to "access to all SNS users" inform the user of the consequences (changing legal obligations as the data controller such as the obligation to rectify false data or to answer to information requests). Such information could for example be given by means of a pop-up window.

Art. 10 and 11 and the content of privacy policies

If we assume that an individual processing data of another individual in a virtual community is a data controller, how far can Art. 10 DPD really be applied? This is important to know, as Art. 10 DPD defines the content of privacy policies. If Art. 10 DPD applies fully, then it however means that if an individual, Alice, is processing data about another individual, Bob, then Alice has to inform Bob about her identity when she asks him to provide personal data about himself. On the other hand, Alice also has privacy interests to stay anonymous or pseudonymous within transactions. Therefore, for instance, in eBay both seller and buyer can act pseudonymously. How

[11] Opinion of Art. 29 Working Party on SNS, of 12 June 2009, page 6.

can we solve the conflicting interests of Bob of being informed of the identity of a data controller and of Alice of being not identified?

Art. 10 does not apply to all kinds of data processing as defined in Art. 2 (b) DPD. According to Art. 2 (b) DPD processing of personal data shall mean any operation or set of operations which is performed upon personal data, such as collection, recording, organizing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Art. 10 DPD applies only in cases where personal data is *collected from the data subject*. If this provision should have been applicable to all forms of data processing the term "processing" would have been used. The use cases regulated in Art. 10 DPD are probably not the typical SNS use cases: Art. 10 DPD applies in cases where a transaction or the conclusion of a contract is conducted online and the data subject provides information herself. In SNS the profile owner publishes (not collects) data about third parties without their prompt knowledge or contribution. Art. 10 DPD may however apply in cases where e.g. a SNS user takes a photo - taking a photo means data collection; data collection can be defined as the purpose-bound acquisition of data on the data subject - with the intention to publish it in her SNS profile (and no household exemption applying to that profile). In this case Art. 10 DPD applies fully. Art 10 DPD differentiates between two kinds of information the data controller has to give to the data subject. Under all circumstances (no exemption is regulated), the data controller has to give the following (minimum) information (unless the data subject already has this information):

- identity of controller and representative,
- purpose of processing

In addition, "further information" must be given only in so far as such further information is "necessary". Further information comprises:

- recipients or categories of recipients of the data
- whether replies to the questions are obligatory or voluntary, as well as the consequence of a failure to reply,
- the existence of a right of access to and the right to rectify the data concerning the data subject.

Giving this additional information is considered "necessary" if the person whose data is to be collected needs this information to rightly and comprehensively assess the consequences of her contribution to the data collection and to make a decision aware of the legal position. Germany decided to include the general obligation to provide information about recipients or categories of recipients into Art. 4 (3) 3. Federal Data Protection Act.

However, we have to look into Art. 11 DPD whether the therein regulated information obligations may be applicable (with very similar consequences as if Art. 10 DPD were applicable):

Art. 11 DPD applies in cases where the data have not been obtained from the data subject.
In these cases the data subject shall be informed at a later point in time (not upon collection): when the data relating to her is recorded or when a disclosure to third parties is envisaged. Thus, Art. 11 DPD is applicable when a SNS user is about to enter (and subsequently record and publish to third parties) data about the data subject in her profile that she did not collect from the data subject herself (again: if the household exemption applies, the entire provisions of the directive and thus also Art. 11 is not applicable).

Generally, the data controller has to give the following (minimum) information (unless the data subject already has this information):

- identity of controller and representative,
- purpose of processing

In addition, "further information" must be given only in so far as such further information is "necessary". Further information comprises:

- the categories of data concerned
- recipients or categories of recipients of the data
- the existence of the right of access to and the right to rectify the data concerning the data subject.

Unlike in Art 10 DPD there exists an exemption from the obligation to inform the data subject. In Art. 11 (2) DPD it is stated that the information obligation shall not apply where […] the provision of such information proves impossible or would involve disproportionate effort. For an effort to be ”disproportionate”, and thus to trigger the exemption, it is not the overall effort for providing the information to the affected data subjects. Instead the disproportionality has to be assessed taking into account the data subject’s legitimate interest to receive the information as well as the effort to provide this information. Considering the fact that in the context of SNS Art. 11 DPD applies only where access to the profile is not limited to self-selected friends, the data recorded in such profiles and disclosed to (an unlimited number of) third parties may be very sensitive and at the same time accessible to a vast and uncontrolled number of individuals. On the other hand, implementing an information tool seems possible for SNS providers who have to offer this mechanism to their profile users who want to publish data about other individuals.

Data subject’s consent

If no legal grounds exist for the data processing, the data subject’s consent must be obtained by the data controller prior to the intended data processing. If a user intends to publish data about other users to an unlimited number of SNS users, she has to obtain that person’s consent prior to e.g. uploading the photo.

5.3 Conclusions and future work

In certain cases, SNS users act as data controllers and have to display policy information to other users when they collect or publish data about them. Publishing data about other users may require obtaining that user’s consent. SNS providers should inform users about those obligations and provide them with settings that allow them to carry out their obligations as data controllers where applicable.

Within the scope of PrimeLife Activity 4’s future work, we will develop user interfaces that SNS providers can display to SNS users at specific occasions (e.g., when a user enters a SNS with no restrictions on the number of users, or when a user opens access control to all SNS users). The purpose of these UIs will be to inform the SNS users about their legal obligations in their roles as data controllers in an understandable and noticeable manner. Besides, message templates which users can use to display policy information to other users in certain situations will be developed.

Chapter 5

Conclusions and Outlook

This deliverable has addressed the two major challenges of how to make privacy policies more comprehensible and transparent and how to simplify the process of privacy preference management for end users. For this, user interfaces must be developed that are informative, comprehensible while legally compliant, but also flexible to handle both simple and complex interactions involving data disclosures to several data controllers or for several purposes and possibly different retention periods.

In the central part of this deliverable, we have presented alternative UI prototypes for privacy policy display and privacy preference management "on the fly". An online comparison user study of two alternative prototypes for policy display in one window (called prototype A and B in the study) was conducted, where the first one (prototype A) also provided privacy preference information and preference management "on the fly". One design difference was the ability of the interface to extend horizontally (prototype A) or vertically (prototype B) with the number of data processing purposes that needed to be displayed. Results of the comparison study showed that end users appreciate the existence of privacy preference information provided by prototype A. Test users clearly showed a preference for prototype A in terms of appearance, comprehensibility, trust and other criteria. Interesting is however that while users understood better what types of data were disclosed in prototype A, it was more clear for them in prototype B for what purposes the data were disclosed. A challenge for our future work will be to elaborate new designs proposals that take advantage of the positive features of both prototypes.

An alternative multi-step approach for policy administration and presentation was presented as well, because with the one-window approach it may be difficult for the users to differentiate between information on the services side's policy and information relating to the user's preferences. Furthermore, the multi-step approach seems also to be more adequate for supporting the enforcement of the privacy principle of data minimisation for transactions involving several service providers. For those reasons, further development, design refinements and testing of multi-step approaches for policy display and management will be part of our future work.

Our future work on UI prototypes within work package 4.3, will also include further work on icons representing content of privacy policies, which can complement text-based policy elements and increase their comprehensibility. For this, the set of icons presented in this deliverable has to be tested "stand-alone" and in combination with the next versions of prototypes.

For the future work of work package 4.3, the cooperation with other work packages and activities in PrimeLife will be important.

First of all, for our future UI prototype developments, the close cooperation with PrimeLife Activity 5 will be essential, as the policy display and management user interfaces will translate the functionality provided by the policy languages developed within Activity 5.

Furthermore, the development of UI prototypes for policy display for SNS applications based on the legal requirements, which were elicited in this deliverable, need to be done in cooperation with WP1.2, so that the UI prototypes serve the purposes of the WP1.2 prototypes for selective access control in social networks.

Finally, the UI concepts developed in WP4.3 should be combined and tested with UI concepts developed in the other work packages in Activity 4, namely those for credential selection (developed by WP4.1) and trust evaluation (developed by WP4.2).

Appendix A

Extended PrivPref Structure and Example (specified in XML)

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="PrivacyPreferenceList" type="ListType" />
  <xs:complexType name="ListType">
    <xs:sequence>
      <xs:element maxOccurs="unbounded" name="Preference" type="ItemType" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ItemType">
    <xs:choice>
      <xs:element name="Anonymous" type="TypeAnonymous" />
      <xs:element name="MinimalData" type="TypeMinimalData" />
      <xs:element name="AdditionalData" type="TypeAdditionalData" />
    </xs:choice>
  </xs:complexType>

  <xs:complexType name="TypeAnonymous">
    <xs:sequence>
      <xs:element name="Contact" type="xs:anyURI" />
      <xs:element name="Purpose" type="xs:anyURI" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="TypeMinimalData">
    <xs:sequence>
      <xs:element name="Contact" type="xs:anyURI" />
      <xs:element name="Purpose" type="xs:anyURI" />
      <xs:element minOccurs="0" maxOccurs="unbounded" name="DataItem"
type="dataItemType" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="TypeAdditionalData">
    <xs:sequence>
      <xs:element name="Contact" type="xs:anyURI" />
      <xs:element name="Purpose" type="xs:anyURI" />
      <xs:element minOccurs="1" maxOccurs="unbounded" name="DataItem"
type="dataItemType" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="dataItemType">
    <xs:sequence>
```

```
      <xs:element name="Data" type="pii" />
      <xs:element name="Retention" type="xs:date" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="pii">
    <xs:sequence>
      <xs:element name="Category" type="xs:anyURI" />
      <xs:element name="Value">
        <xs:simpleType>
          <xs:union>
            <xs:simpleType>
              <xs:restriction base="xs:integer" />
            </xs:simpleType>
            <xs:simpleType>
              <xs:restriction base="xs:string" />
            </xs:simpleType>
            <xs:simpleType>
              <xs:restriction base="xs:date" />
            </xs:simpleType>
            <xs:simpleType>
              <xs:restriction base="xs:double" />
            </xs:simpleType>
            <xs:simpleType>
              <xs:restriction base="xs:anyURI" />
            </xs:simpleType>
          </xs:union>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
```

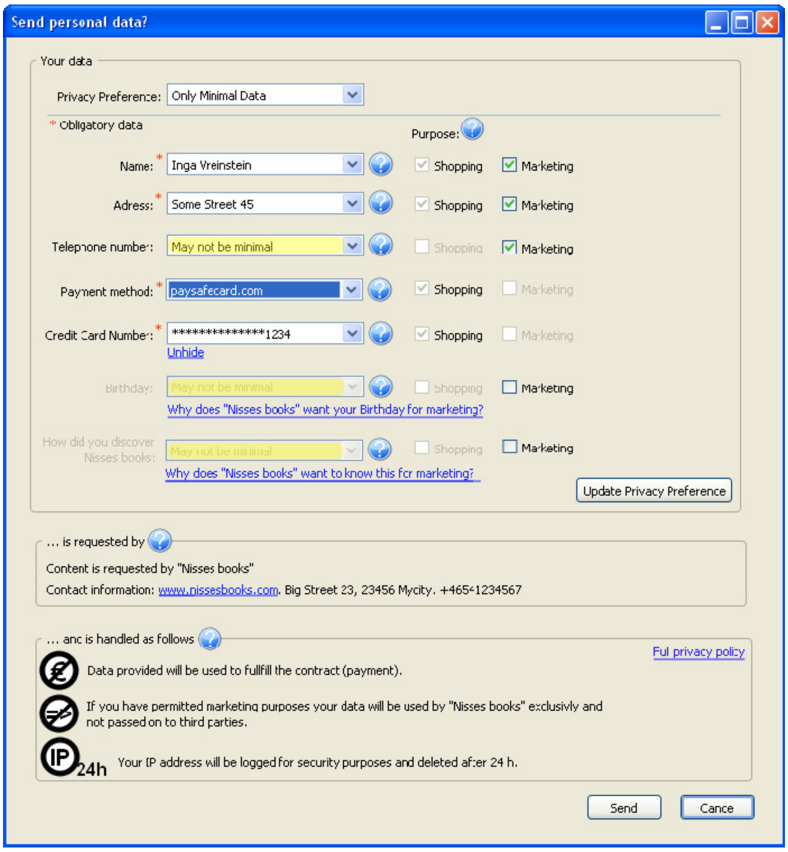
```
<?xml version="1.0" encoding="utf-8"?>

<PrivacyPreferenceList xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="C:\Users\hansh\Documents\XSDFile2.xsd">

<Preference>
<MinimalData>
 <Contact>http://www.w3.com</Contact>
 <Purpose>http://www.w3.com</Purpose>
       <DataItem>
          <Data>
               <Category> https://www.prime-project.eu/ont/PIIBase#country </Category>
               <Value>Sweden</Value>
          </Data>
        <Retention>2009-12-31</Retention>
       </DataItem>
</MinimalData>
</Preference>

<Preference>
<Anonymous> <!-- No Data allowed -->
 <Contact>http://www.w3.com</Contact>
 <Purpose>http://www.w3.com</Purpose>
</Anonymous>
</Preference>

<Preference>
<AdditionalData>
 <Contact>http://www.w3.com</Contact>
 <Purpose>http://www.w3.com</Purpose>
       <DataItem>
          <Data>
               <Category> https://www.prime-project.eu/ont/PIIBase#given </Category>
               <Value>Nils Erik</Value>
          </Data>
        <Retention>2009-12-31</Retention>
       </DataItem>
       <DataItem>
          <Data>
               <Category> https://www.prime-project.eu/ont/PIIBase#family </Category>
               <Value>Swedenson</Value>
          </Data>
       <Retention>2010-06-01</Retention>
</DataItem>
</AdditionalData>
</Preference>

<Preference>
<MinimalData>
 <Contact>http://www.w3.com</Contact>
 <Purpose>http://www.w3.com</Purpose>
<DataItem>
          <Data>
              <Category> https://www.prime-project.eu/ont/PIIBase#birthDate
</Category>
              <Value>2000-10-12</Value>
          </Data>
        <Retention>2009-12-31</Retention>
       </DataItem>
       <DataItem>
          <Data>
              <Category> https://www.prime-project.eu/ont/PIIBase#email </Category>
              <Value>nils@anyprovider.any</Value>
          </Data>
       <Retention>2010-06-01</Retention>
</DataItem>
</MinimalData>
</Preference>


</PrivacyPreferenceList>
```

Appendix **B**

PrimeLife Online Test Questionnaire

B.1 Prototype A

Please evaluate the following user interfaces by the given criteria.



Send personal data?

Your data

Privacy Preference: Only Minimal Data

* Obligatory data

Purpose:

Name:*	Inga Vreinstein	☑ Shopping	☑ Marketing
Adress:*	Some Street 45	☑ Shopping	☑ Marketing
Telephone number:	May not be minimal	□ Shopping	☑ Marketing
Payment method:*	paysafecard.com	☑ Shopping	□ Marketing
Credit Card Number:*	**************1234 Unhide	☑ Shopping	□ Marketing
Birthday:	May not be minimal Why does "Nisses books" want your Birthday for marketing?	□ Shopping	□ Marketing
How did you discover Nisses books:	May not be minimal Why does "Nisses books" want to know this fcr marketing?	□ Shopping	□ Marketing

Update Privacy Preference

... is requested by

Content is requested by "Nisses books"

Contact information: www.nissesbooks.com. Big Street 23, 23456 Mycity. +46541234567

... anc is handled as follows

Ful privacy policy

Data provided will be used to fullfill the contract (payment).

If you have permitted marketing purposes your data will be used by "Nisses books" exclusivly and not passed on to third parties.

24h Your IP address will be logged for security purposes and deleted af:er 24 h.

Send Cance

1. **Please write down any spontaneous comments to the above user interface**

   ____

2. **What do you think the user interface is used for?**

____

3. **What personal information is sent?**
   ____

4. **How safe do you think that your personal data is, using this program?**
   safe o o o o o o o unsafe

5. **Please evaluate the consistency of the user interface?**
   consistent o o o o o o o inconsistent

6. **How trustworthy do you think the user interface is (e.g. would you enter your personal data in the designated fields and send them)?**
   trustworthy o o o o o o o dubious

7. **How do you think your data is treated?**
   responsible o o o o o o o irresponsible

8. **Do you know what this user interface is about?**
   o Yes
   o No

9. **What do the grayed-out boxes mean (checked and unchecked)?**
   ____

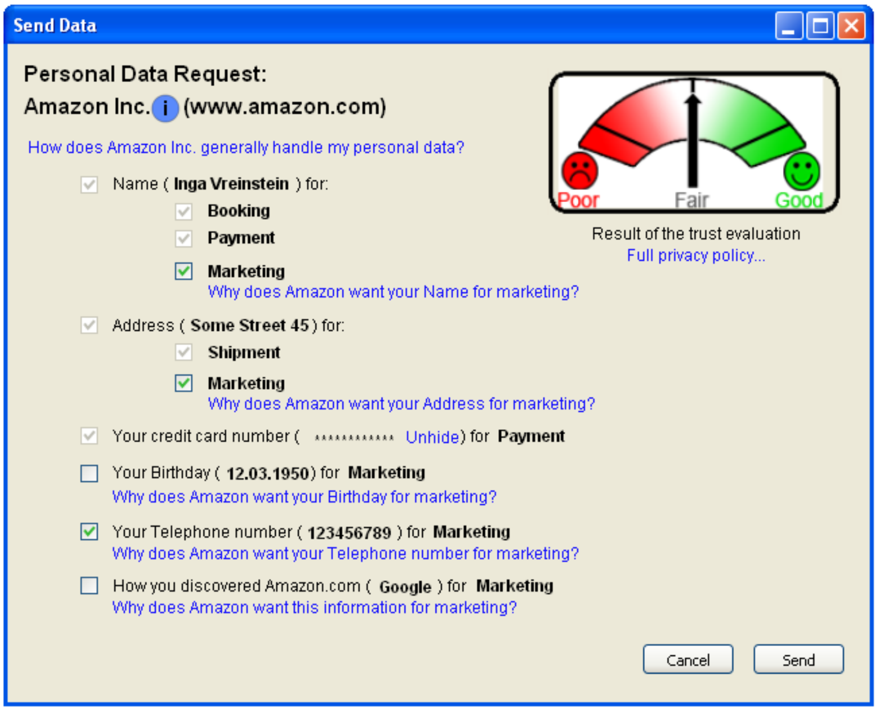
10. **What does Privacy Preference mean to you in this context?**
    ____

11. **Would you use the Privacy Preferences to get informed about the possibility of anonymous shopping?**
    o Yes
    o No

12. **Would you use the Privacy Preferences to be warned whenever too much data is requested from you for a certain purpose?**
    o Yes
    o No

B.2 Prototype B

Please evaluate the following user interfaces by the given criteria.



Personal Data Request:
Amazon Inc. (www.amazon.com)

How does Amazon Inc. generally handle my personal data?

☑ Name (**Inga Vreinstein**) for:
☑ **Booking**
☑ **Payment**
☑ **Marketing**
Why does Amazon want your Name for marketing?

Result of the trust evaluation
Full privacy policy...

☑ Address (**Some Street 45**) for:
☑ **Shipment**
☑ **Marketing**
Why does Amazon want your Address for marketing?

☑ Your credit card number (************ Unhide) for **Payment**

□ Your Birthday (**12.03.1950**) for **Marketing**
Why does Amazon want your Birthday for marketing?

☑ Your Telephone number (**123456789**) for **Marketing**
Why does Amazon want your Telephone number for marketing?

□ How you discovered Amazon.com (**Google**) for **Marketing**
Why does Amazon want this information for marketing?

13. Please write down any spontaneous comments to the above user interface

____

14. What do you think the user interface is used for?

____

15. What personal information is sent?

16. How safe do you think that your personal data is, using this program?
safe o o o o o o o unsafe

17. Please evaluate the consistency of the user interface?
consistent o o o o o o o inconsistent

18. How trustworthy do you think the user interface is (e.g. would you enter your personal data in the designated fields and send them)?
trustworthy o o o o o o o dubious

19. How do you think your data is treated?
responsible o o o o o o o irresponsible

20. Do you know what this user interface is about?
o Yes
o No

21. What do the grayed-out boxes mean (checked and unchecked)?

____

22. What does Privacy Preference mean to you in this context?

____

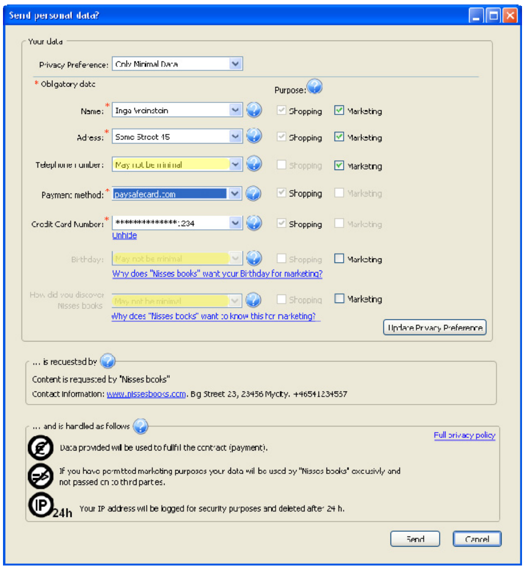
23. **Would you use the Privacy Preferences to get informed about the possibility of anonymous shopping?**
o Yes
o No

24. **Would you use the Privacy Preferences to be warned whenever too much data is requested from you for a certain purpose?**
o Yes
o No

B.3 Comparison of the Prototypes

In the following we ask you to compare the previously seen user interfaces and indicate your preferences.

Prototype A



Send personal data?

Your data

Privacy Preference: Only Minimal Data

* Obligatory data

Purpose:

Name:* Inga Vreinstein ☑ Shopping ☑ Marketing

Adress:* Some Street 15 ☑ Shopping ☑ Marketing

Telephone number: May not be minimal □ Shopping ☑ Marketing

Payment method:* paysafecard.com ☑ Shopping □ Marketing

Credit Card Number:* *************234 ☑ Shopping □ Marketing
Unhide

Birthday: May not be minimal □ Shopping □ Marketing
Why does "Nisses books" want your Birthday for marketing?

How did you discover Nisses books May not be minimal □ Shopping □ Marketing
Why does "Nisses books" want to know this for marketing?

... is requested by

Content is requested by "Nisses books"
Contact Information: www.nissesbooks.com, Big Street 23, 23456 Mycity, +46541234567

... and is handled as follows

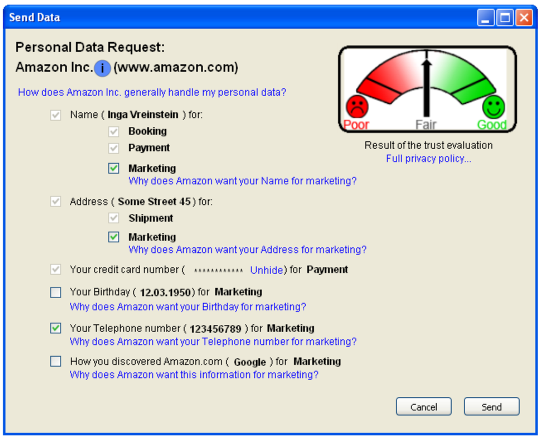
Full privacy policy

Data provided will be used to fulfil the contract (payment).

If you have permitted marketing purposes your data will be used by "Nisses books" excusivly and not passed on to third parties.

24h Your IP address will be logged for security purposes and deleted after 24 h.

Prototype B



Send Data

Personal Data Request:
Amazon Inc. (www.amazon.com)

How does Amazon Inc. generally handle my personal data?

☑ Name (**Inga Vreinstein**) for:
☑ **Booking**
☑ **Payment**
☑ **Marketing**
Why does Amazon want your Name for marketing?

☑ Address (**Some Street 45**) for:
☑ **Shipment**
☑ **Marketing**
Why does Amazon want your Address for marketing?

☑ Your credit card number (************ Unhide) for **Payment**

□ Your Birthday (**12.03.1950**) for **Marketing**
Why does Amazon want your Birthday for marketing?

☑ Your Telephone number (**123456789**) for **Marketing**
Why does Amazon want your Telephone number for marketing?

□ How you discovered Amazon.com (**Google**) for **Marketing**
Why does Amazon want this information for marketing?

Result of the trust evaluation
Full privacy policy...

25. **According to your opinion, do the prototypes contain the same information?**
o Yes
o No

   a. **If no, what are the differences, what information is missing?**

____

26. **What prototype do you prefer because of the appearance?**
o Prototype A
o Prototype B

27. **Which prototype do you prefer because of the display of the data?**
o Prototype A
o Prototype B

28. **Which prototype do would you prefer because of the structuring of the information?**
o Prototype A
o Prototype B

29. **Which prototype appears more clearly arranged?**
o Prototype A
o Prototype B

30. **Which prototype appears more trustworthy?**
o Prototype A
o Prototype B

31. **Which prototype appears more secure (treating your personal data)?**
o Prototype A
o Prototype B

32. **Which prototype is more understandable structured?**
o Prototype A
o Prototype B

33. **Which prototype informs you better?**
o Prototype A
o Prototype B

34. **What advantages does prototype A have compared to prototype B?**
____

35. **What advantages does prototype B have compared to prototype A?**
____

36. **Which prototype do you prefer because of the overall appearance?**
o Prototype A
o Prototype B

37. **Do you have further comments?**
____

B.4 Demographic Information

Finally we want to ask you a few statistical questions.

38. **What is your gender?**
o Female
o Male

39. **How old are you?**
____

40. What is your highest level of education?

o Compulsory education
o Apprenticeship, college
o Leaving examination
o University
o Other

41. What is your profession?

o Freelancer
o Self-employed
o Employee
o Workman
o Pupil, student
o Retiree
o Other, working
o Other, unemployed

42. How much is your monthly net salary?

o Less than 1.500 Euro
o 1.500 to 2.200 Euro
o 2.200 to 2.900 Euro
o More than 2.900 Euro
o Not specified

43. Do you care about data protection?

o Yes, very much
o A bit
o Rather not
o No, not at all

Bibliography

(Art. 29 WP 2004) Art. 29 Working Party: Opinion 10/2004 on More Harmonised Information Provisions, WP 100, 11987/04/EN, November 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf

(Art. 29 WP 2009) Art. 29 Working Party: Opinion 5/2009 on online social networking, WP 163, 01189/09/EN, June 2009, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

(Bickerstaff 2008) Bickerstaff , R, 2008, Towards a Commons Approach to Online Privacy – a "Privacy Commons", presentation at SCL Information Governance Conference 2008, London, May 2008, http://www.healthymedia.co.uk/scl-2008-may-governance/pdf/scl-2008-05-privacy-commons-roger-bickerstaff.pdf

(Bratus et al. 2008) Bratus, S., Masone, C., and Smith, S. W. 2008. Why Do Street-Smart People Do Stupid Things Online?. IEEE Security and Privacy 6, 3 (May. 2008), 71-74.

(Cranor et al. 2006) Cranor, L.F., Guduru, P., and Arjula, M., User Interfaces for Privacy Agents, in ACM Transactions on Computer-Human Interaction 13(2), June 2006.

(Fischer-Hübner 2001) Fischer-Hübner, S., "IT-Security and Privacy-Design and Use of Privacy-Enhancing Security Mechanisms", Springer Scientific Publishers, Lecture Notes in Computer Science, LNCS 1958, May 2001, ISBN 3-540-42142-4.

(Fischer-Hübner et al. 2009) Fischer-Hübner, S., Köffel, C., Wästlund, E., Wolkerstorfer, P. (Editors). 2009. HCI Research Report - Version 1, PrimeLife-Deliverable D4.1.1.

(Gideon et al. 2006) Gideon, J., Egelman, S., Cranor, L., Aquisti, A., Power Strips, Propylactis, and Privacy, Oh My!, Proceedings of the Symposium of Usable Privacy and Security (SOUPS 2006), July 14-16, 2006, Pittsburgh, PA , ACM Digital Library.

(Gross et al. 2006) Gross, J., Sheffield, J., Anderson, A., Yu, N. Engendering Trust: Privacy Policies and Signatures", Poster Proceedings of the Symposium of Usable Privacy and Security (SOUPS), July 14-16, 2006, Pittsburgh, PA .

(Helton 2009) Helton, A, 2009, Privacy Commons Icon Set, 2009, http://aaronhelton.wordpress.com/2009/02/20/privacy-commons-icon-set/

(Herzog 2007) Herzog, A., 2007, Herzog, A. Usable Security Policies in Runtime Environments. Linköping Studies in Science and Technology, Dissertation No. 1075. Linköping University, 2007.

(Karat et al. 2005) Karat, C.-M., Karat, J., Brodie, C., and Feng, J., Privacy in Information Technology: Designing to enable privacy policy management in organizations, International Journal Human-Computer Studies 63 (2005), pp. 153-174.

(Karat et al. 2006) Karat, C.-M., Karat, J., Brodie, C., and Feng, J., Evaluating Interfaces for Privacy Policy Rule Authoring, in Proceedings of the SIGCHI conference on Human Factors in computing systems CHI 2006, April 22-27, 2006, Montreal, Canada.

(Kelley 2009) Kelley, P., G., 2009, Designing a Privacy Label: Assisting Consumer Understanding of Online Privacy Practices, Conference on Human Factors in Computing Systems, Proceedings of the 27th international conference extended abstracts on Human factors in computing systems

(Mehldau 2007) Mehldau, M., 2007, Iconset for Data-Privacy Declarations v0.1, 2007, http://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf

(Nielsen 1994) Nielsen, J. 1994. Usability inspection methods. In Conference Companion on Human Factors in Computing Systems (Boston, Massachusetts, United States, April 24 - 28, 1994). C. Plaisant, Ed. CHI '94. ACM, New York, NY, 413-414. DOI= http://doi.acm.org/10.1145/259963.260531

(Pettersson et al. 2006) Pettersson J.S., Fischer-Hübner, S., Pearsson, P., Casassa Mont, M., How Ordinary Internet Users can Have a Chance to Influence Privacy Policies, Short paper Proceedings of the 4th Nordic Conference on Human-Computer Interaction - NordiCHI 2006, Oslo, 14 - 18 October 2006, ACM Press.

(Rundle 2006) Rundle, M., 2006, International Data Protection and Digital Identity Management Tools, presentation at IGF 2006, Privacy Workshop I, Athens, 2006, http://identityproject.lse.ac.uk/mary.pdf (iconset cf. slide 8)

(Tsai 2006) Tsai, J., Egelman, S., Shipman, R., Pu, K.Ch., Cranor, L., Symbols of Privacy", Poster Proceedings of the Symposium of Usable Privacy and Security (SOUPS 2006), July 14-16, 2006, Pittsburgh, PA .