

## D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

**Deliverable Number:** D37.3

**Work Package:** WP 37

**Version:** Final

**Deliverable Lead Organisation:** KAU

**Dissemination Level:** PU

**Contractual Date of Delivery (release):** 30/09/2014

**Date of Delivery:** 30/09/2014

### Editor

Simone Fischer-Hübner (KAU), John Sören Pettersson (KAU)

### Contributors

Julio Angulo (KAU), Simone Fischer-Hübner (KAU), John Sören Pettersson (KAU), Jessica Edbom (KAU), Mia Toresson (KAU), Henrik Andersson (KAU)

### Reviewers

W Kuan Hon (QMUL), Daniela Soares Cruzes (SINTEF)

## Executive Summary

This deliverable on “End user perceptions of privacy-enhanced transparency and accountability” presents the final research results on HCI (Human Computer Interaction) concepts for making privacy-enhanced transparency and accountability comprehensible and perceived as useful. It summarises and refines HCI requirements and principles that were elicited during the first two project years.

In order to propose a concise set of HCI principles and guidelines for cloud service chain transparency tools, the HCI requirements and related HCI principles obtained from the different research activities are grouped into general categories related to required functionality of possible accountable and transparent tools. This categorisation is on a high functional level and is of a general applicability for tools developed to make cloud service chains transparent and service providers accountable.

This deliverable first provides a concise overview of HCI requirements elicited during the 1st project year and puts them into relation with HCI principles and proposed design solutions. It then presents results of research research that we conducted in the second project year, which allowed us to amend and refine these HCI requirements and principles. For this, this deliverable also presents results and conclusions from studies conducted during the second project year on certain specific topics. The deliverable presents results in regard to the evaluation of policy icons, in particular our illumination of the challenges in the development and evaluation of cloud-specific policy icons for illustrating and highlighting policy aspects that are intransparent for cloud subjects. It also reports about the results of usability evaluations of user interfaces for A4Cloud tools for cloud subjects, in particular a usability test of the A4Cloud Data Track tool and a workshop with everyday users of internet services about transparency tools.

An overall conclusion is that while users would like to have more control over their data, they lack a clear actionable approach to enforce this control and do something practical about it. At the same time, the designs discussed in this deliverable show that workable tools are possible to construct also for first-time users even if all functions, label texts, and icons will not be fully understood immediately.

For the more detailed work that will be pursued in the project's last year, some conclusions from the WP C-7 work should be considered:

(1) While a user interface object such as an icon may work well in A4Cloud prototypes it might not be generally applicable for the same function in other systems. Prototypes including introductions to their use, build up a context guiding test users to specific understanding of words and icons. Such contextual features should be reported so that what are workable UI solutions are presented with information on the contextual background.

(2) Wording of icon legends, tooltips, etc. should be given more attention as should also other means of quick introductions about specific A4Cloud topics such as data processors' responsibilities, data logs and data stored at services sides, comprehension of and actionability on incident notifications.

## Contents

<b>1. Introduction</b>	<b>8</b>
1.1. Project Scope . . . . .	8
1.2. Aims and Scope of the Deliverable . . . . .	8
1.3. Relation to other A4Cloud Work Packages and Deliverables . . . . .	9
1.4. Methodology . . . . .	9
1.5. Outline . . . . .	11
<b>2. Preliminary HCI Requirements and Principles</b>	<b>12</b>
2.1. Introduction and background . . . . .	12
2.2. Ex ante transparency . . . . .	14
2.3. Exercising data subject rights . . . . .	21
2.4. Obtaining consent . . . . .	22
2.5. Privacy preference management . . . . .	24
2.6. Privacy policy management . . . . .	25
2.7. Ex post transparency . . . . .	26
2.8. Audit configuration . . . . .	27
2.9. Access control management . . . . .	27
2.10. Privacy risk assessment . . . . .	28
<b>3. Users' Perceptions of Policy Icons</b>	<b>29</b>
3.1. HCI Requirements, Principles and Icon Design Proposals . . . . .	29
3.2. Privacy Icons in the LIBE Committee's compromise proposal . . . . .	31
3.3. Professional designers' suggestions . . . . .	36
3.4. Discussion of evaluation methods . . . . .	39
<b>4. Users' Perceptions of A4Cloud Tools</b>	<b>45</b>
4.1. Introduction and background . . . . .	45
4.2. Data Track usability evaluation . . . . .	46
4.3. Workshop with individual cloud customers . . . . .	53
<b>5. Concluding Remarks</b>	<b>59</b>
5.1. Additional HCI Requirements and Principles . . . . .	59
5.2. Pertinent takeaways for the future HCI development work in A4Cloud . . . . .	61
<b>Appendix A. Icon questionnaires</b>	<b>66</b>
A.1. First Icon Questionnaire (EU Parliament Icons) . . . . .	66
A.2. Second Icon Questionnaire (Designers' Icons) . . . . .	71
<b>Appendix B. Usability evaluations material - Tasks and questions</b>	<b>75</b>
<b>Appendix C. Workshop with individual cloud customers</b>	<b>78</b>
C.1. Questionnaire - Part 1 . . . . .	78
C.2. Questionnaire - Part 2 . . . . .	80

## D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

---

C.3. Feedback by Workshop participants . . . . .	83
--	----

## List of Figures

1. Methods used during project year one for eliciting HCI requirements and principles	13
2. Example of well understood PrimeLife policy icons . . . . .	29
3. Icon proposals (alpha version) by Aza Raskin informing about how disclosure requests by law enforcement are handled [Ras10]. . . . .	30
4. The first page of Annex 1 . . . . .	32
5. a) and b) are symbols presented on the second page of Annex 1 . . . . .	33
6. Two of three Contract Termination icons are dimmed . . . . .	38
7. Outline of the three answer sheets on designers' icons. . . . .	40
8. The popup to select pay within EU but in advance or later at the American hotel.	43
9. The trace view interface of the Data Track tool . . . . .	46
10. Personal data about a user stored at the services' side (collected explicitly or collected/derived implicitly about the user). . . . .	47
11. Some results from the first round of testing. . . . .	49
12. Example step of the introduction tour and of a tooltip in a data item. . . . .	50
13. Heat map of participants' average eye gaze on the dialog showing data at the service's side. . . . .	52
14. Frequency distribution of participants' technology-literacy . . . . .	54

## List of Tables

1. Preferences of frequency of notifications (where 0 = 'Not often' and 5 = 'Very often') . . . . . 58

## List of Abbreviations

CC	Cloud Customer
CB	Cloud Broker
COAT	Cloud Offering Advisory Tool
CP	Cloud Provider
DS	Data Subject
DC	Data Controller
DP	Data Processor
DPA	Data Protection Authority
DPIAT	Data Protection Impact Assessment Tool
DPO	Data Protection Officer
DSART	Data Subject Access Request Tool
DT	Data Track
DTMT	Data Transfer Monitoring Tool
GDPR	General Data Protection Regulation
HCI	Human Computer Interaction
IRT	Incident Response Tool
PAPV	Plug-In for Assessment of Policy Violations
PETs	Privacy Enhancing Technologies
RRT	Remediation and Redress Tool
SME	Small and Medium-sized Enterprise
TETs	Transparency-Enhancing Technologies
UI	User Interface

## 1. Introduction

### 1.1. Project Scope

The A4Cloud project focuses on accountability for the cloud and other future Internet services. It conducts research with the objective of increasing trust in cloud computing by developing methods and tools for different stakeholders, through which cloud providers across the entire cloud service value chain can be made accountable for the privacy and confidentiality of information held in the cloud.

The A4Cloud project is creating solutions to support cloud subjects and customers in deciding and tracking how their data are used by cloud service providers [PTC<sup>+</sup>12], including tools that are developed combining risk analysis, policy enforcement, monitoring and compliance auditing with tailored IT mechanisms for security, assurance and redress.

The A4Cloud stakeholders, for which A4Cloud develops tools, include so called individual or organisation cloud subjects that are entities whose data is processed by a cloud provider, either directly or indirectly; individual or organisation cloud customers that are entities that maintain a business relationship with, and use services from a cloud provider; as well as cloud providers and cloud auditors including data protection officers (DPOs).

### 1.2. Aims and Scope of the Deliverable

A key factor for the successful exploitation of A4Cloud Tools will be their usability and trustworthiness. This means that it should be possible for the respective stakeholder group to use A4Cloud tools with effectiveness, efficiency, and satisfaction. Besides, A4Cloud tools should be perceived as trustworthy and help user to reassess their trust or distrust in cloud services.

The HCI (Human Computer Interaction) - related task of the A4Cloud work package on “*HCI concepts for usable transparency and accountability*” (WP:C-7) has the specific goal to analyse what factors and HCI concepts influence perceived trustworthiness and comprehension of privacy-enhanced transparency and accountability tools, with the objective that users are empowered to make well-informed decisions in regard to privacy, control and the trustworthiness of cloud services.

This report D:C-7.3 on “*End user perceptions of privacy-enhanced transparency and accountability*” presents the final research results on HCI concepts for making privacy-enhanced transparency and accountability comprehensible and perceived as useful. We will summarise HCI requirements and principles that we elicited during the first project year, and present refined and additional HCI requirements and principles and discuss how they they were elicited during the second project year.

For this, we will report about further usability tests and evaluations that we conducted for A4Cloud prototypes in the second project year. In particular, this deliverable reports on the usability evaluations of the A4Cloud Data Track tool, for which already advanced user interfaces had been developed after one and a half project years that could be subject for usability testing. Besides, end user perceptions and preferences of aspects related to incident notification and response, which are of relevance for the Incident Response Tool and plugin for policy violations that can be connected to the Data Track, were analysed in a focus group workshop with



individual cloud customers that we organised in cooperation with work package B-2.

A central HCI requirement that we elicited during the first project year (as reported in the Deliverable D-C-7.1 [AFHP<sup>+</sup>13]) was that privacy policies should make the consequences of data disclosures by data subjects transparent. In D:C-7.1, it was discussed that for achieving this, policies could be complemented by standard and meaningful icons representing data attributes, purposes and processing steps. In the second project year, we have therefore assessed policy icons that were recently proposed as part of the LIBE Committee's compromise proposal of the General EU Data Protection Regulation (GDPR) [Eur13], and we developed and tested policy icons in order to highlight challenges for the attempts to provide user interfaces with higher transparency as regards data processing in the cloud. This will be useful when illustrating and highlighting policy aspects in user interfaces of A4Cloud tools. The results in the form of proposed icons, test results and HCI requirements and principles derived from the tests are also reported in this deliverable.

### 1.3. Relation to other A4Cloud Work Packages and Deliverables

This Deliverable focuses on exploring HCI concepts and principles and the user's perception. It is therefore reporting about the early conceptual work that was conducted in A4Cloud as well as usability evaluations that we conducted during the second project year. The earlier Deliverable D:C-7.1 on "*General HCI principles and guidelines for accountability and transparency in the cloud*" provided guidance for the design of usable and trustworthy user interfaces for transparency and accountability tools that will be summarised and further amended in this deliverable.

HCI research and development work is also conducted by A4Cloud work package D5 and reported in the Deliverable D:D-5.1 [ABFH<sup>+</sup>14], which however focuses on the development of user interface (UI) mockups and prototypes for A4Cloud tools and stakeholder-specific tool sets, while work package C-7 does not develop user interfaces, but rather focuses on the conceptual work and the users' perception of A4Cloud tools. The results of this Deliverable in the form of HCI requirements and principles should however guide the further development of UIs for A4Cloud tools and stakeholder-specific tool sets within work package D-5.

### 1.4. Methodology

In A4Cloud's Work Package C7, we follow a human-centred design approach for eliciting and testing HCI requirements and guiding the development of user interface design principles. Human-centred design is defined by ISO 9241-210, 2010 as an approach to interactive systems development that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors/ergonomics, and usability knowledge and techniques (ISO 9241-210:2010(en), [ISO10]). User requirements are considered right from the start and included in the whole design and development cycle. In A4Cloud, we have elicited and refined such user requirements and related HCI principles through methods including stakeholder workshops, focus groups, controlled usability testing, literature and law reviews, as discussed in A4Cloud deliverable D:C-7.1 (see also section 2.1).

For the choice of methods, we have taken into consideration that general concepts, which are of importance for the comprehension of transparency and related risks, such as what information is stored and where it is processed, are usually difficult to understand for the lay users, while other end user groups, such as regulators or security administrators, usually have a clearer understanding. Therefore, different user-groups require different interfaces and interaction paradigms. This also means that the different user groups have to be involved using different approaches to human-centred design. For eliciting HCI requirements and principles during the first project year, we have used controlled experiments and mock-up-based evaluations in addition to focus groups with ordinary users for exploring the needs of lay users, while the needs of professional stakeholder groups were mainly investigated by means of stakeholder workshops and focus groups with expert users. Furthermore, we used controlled experiments and mock-up-based evaluations with the objective to analyse the user's mental models of A4Cloud related technical concepts, since our earlier work had shown that many HCI issues are mental model issues which are difficult to solve for novel PET concepts [GHW<sup>+</sup>11], [WAFH11]. The results of this elicitation work in the form of HCI requirements and principles is summarised in chapter 2, and is further refined in the subsequent chapters.

For analysing the users' perception of accountability and transparency concepts and tools and for further refining our HCI requirements and principles during the second project year, we have in particular used the following research methods:

- **Iterations of usability tests for the Data Track and for policy icons:**

Usability testing is a technique that can measure the actual performance of users when trying to achieve a task with a given user interface. Usability testing of UI prototypes of the Data Track tool was considered a suitable method for our purposes since it has the advantage of letting lay users communicate their needs, opinions and expectations about new technologies. This is because lay users might not be very familiar with the terminologies and technologies related to cloud computing, and might not have a clear understanding of how Internet technologies and data handling works either. During a usability test session test participants are typically presented with a graphical user interface and are given a set of instructions or tasks that they are asked to complete. A test moderator usually guides the participant through the tasks, while at the same time observing and annotating the interactions of the participants with the interface. The moderator also encourages participants to express aloud their opinions, actions and reactions to the prototype, in an approach commonly referred to as the think aloud protocol [JSBG04]. The results of the Data Track usability tests will be presented in chapter 4. We also used usability tests with the help of questionnaires for testing the lay user's understanding of policy icons. The tests and their results are described in chapter 3.

- **Focus Group workshop:**

Focus groups are appropriate for bringing together a cross-section of users so that they can collaboratively share and unveil their opinions and needs regarding particular challenges foreseen in the design of a system. Moderators of a focus group can stimulate participants to discuss these opinions with the other group members by using different

approaches, such as asking direct questions to participants, encouraging brainstorming, instructing them to work with various probes, etc. In cooperation with work package B2, we organised a focus group workshop with individual cloud subjects to analyse their perceptions of the Data Track and their preferences in regard to incidence reports to be delivered by the Incident Reporting Tool (IRT). The workshop results are presented in chapter 4, section 4.3.

### 1.5. Outline

The remainder of this Deliverable is structured as follows:

- Chapter 2 “Preliminary HCI Requirements and Principles” summarises the HCI requirements and principles that we have elicited during the first project year. While these HCI requirements and principles were already presented in D:C-7.1, we will in this chapter provide a more concise overview of the HCI requirements, how they were derived, as well as related HCI principles and HCI design suggestions for meeting these requirements and principles.
- Chapter 3 “Users’ Perceptions of Policy Icons” presents our results in regard to the evaluation of policy icons, in particular our illumination of the challenges in the development and evaluation of cloud-specific policy icons for illustrating and highlighting policy aspects.
- Chapter 4 “Users’ Perceptions of A4Cloud Tools” reports on the results of evaluations of user interfaces for A4Cloud tools for cloud subjects by the means of a usability test iteration and a focus group workshop.
- Finally, chapter 5 “Concluding Remarks” rounds up this deliverable with final conclusions drawn from the usability evaluations reported in chapters 3 and 4 in regard to an amendment of the HCI requirements and principles and guidelines presented in chapter 2 and discusses how they relate to future HCI development in A4Cloud to be conducted within the work package D-5.

## 2. Preliminary HCI Requirements and Principles

### 2.1. Introduction and background

This chapter summarises HCI requirements, principles, design proposals and design suggestions implementing these principles for accountability and transparency tools that were derived in the first project year for the following reasons. First of all, even though they were already presented in larger detail in the Deliverable D:C-7.1 [AFHP<sup>+</sup> 13], this chapter has the objective to provide a more concise overview that clearly motivates the HCI requirements by the different research activities that we conducted in the first project year, and clearly relates them to the HCI principles and proposed design solutions for meeting these requirements and principles. Moreover, as this project deliverable has the objective to present the final research results on HCI concepts for making privacy-enhanced transparency and accountability comprehensible and perceived as trustworthy, this chapter will summarise research results on HCI concepts in the form of HCI requirements, principles and design solutions that we elaborated and elicited in the first project year. The subsequent chapters will then report about research results on HCI concepts and elicited additional and refined HCI requirements and principles from the second project year.

In order to propose a concise set of HCI principles and guidelines for cloud service chain transparency tools, we group the HCI requirements and related HCI principles obtained from the different research activities into general categories related to required functionality of possible accountability and transparency tools. This categorisation is at a high functional level and is of general applicability for tools developed to make cloud service chains transparent and service providers accountable.

From the analysis provided in A4Cloud and other projects, we suggest a categorisation into the following functionalities:

1. Ex ante transparency (i.e. transparency which enables the anticipation of consequences before data is actually disclosed, e.g. via policy display incl. policy mismatches, mediating of trustworthiness or risks to individual end users);
2. Exercising data subject rights;
3. Obtaining consent;
4. Privacy preference management (helping individual end users to manage their privacy preferences)
5. Privacy policy management (for business end users)
6. Ex post transparency (i.e. transparency which informs about consequences if data already has been revealed. We also include under this functionality the display of policy violations and help with risk mitigation)
7. Audit configuration (help with settings in regard to collection of evidences)
8. Access control management

## 9. Privacy risk assessment (for business end users).

In the following subsections, we map the obtained HCI requirements and related HCI principles and design suggestions onto these functional categories. This mapping has the objective to show for each type of functionality what HCI requirements need to be met and what HCI principles should be followed during the UI design. For each requirement, we list one or several observations noted in our studies that we conducted in the first year. As shown in Figure 1, these studies comprised one stakeholder workshop (with participation of lawyers from the Swedish Consumer Agency, Swedish Data Protection Commissioner, Government and industrial cloud consumers), focus group meetings with expert and non-expert users, experiments on the users' mental models in regard to personal data handling by cloud services, usability tests for Data Track tool as well as law reviews and literature reviews on human trust factors (see also [AFHP<sup>+</sup>13] for a detailed presentation and discussion of these methods). In the following subsections, we refer to results of these studies as *Workshop notes*, *Focus group observations*, *Experiment results*, *Usability test observations*, *Legal considerations*, and *Trust reviews*. For each observation, we attempt to formulate an HCI principle as well as one or several suggestions for UI design solutions.

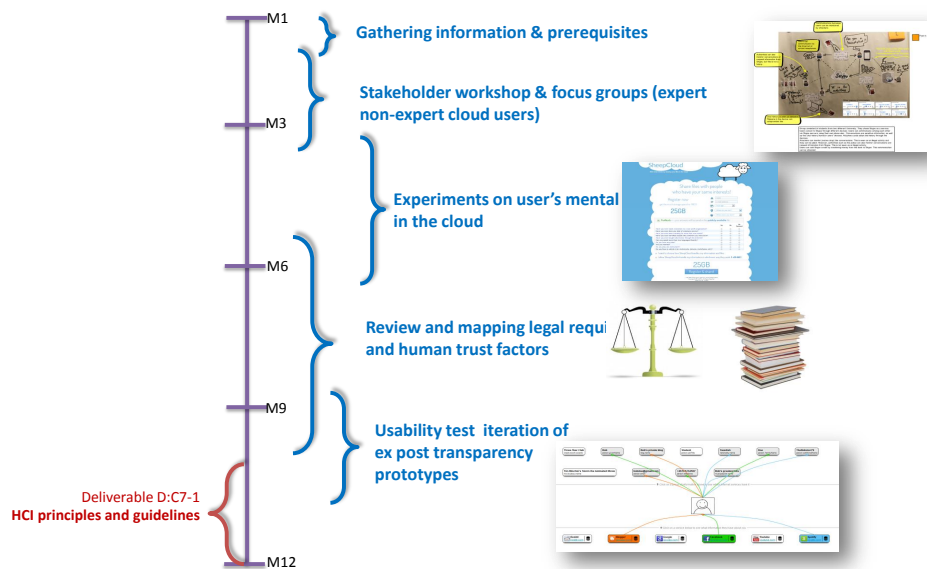


Figure 1: Methods used during project year one for eliciting HCI requirements and principles

## 2.2. Ex ante transparency

### 2.2.1. Make explicit data disclosures and implicit data collections transparent

This requirement is based on four observations made in our focus groups and in the usability test.

- **Focus group observation:** Non-expert users believe that different service providers are more related to each other than they might be in reality. Tendency to believe that personal information is distributed among many of the entities represented: All internet companies can share information about me.

**HCI Principle:** The interface should clearly show the different entities that could access which kind of personal information.

**Design suggestion:** Create a network visualisation that clearly shows the entities (nodes) getting users information and the pieces of information that each entity has (as the links).

- **Focus group observation:** Both non-experts and advanced users are aware that service providers can do analysis of their data to find out more information about them. However, non-expert users are less aware of the consequences of the possible misuse of their data.

**HCI Principle:** Users could be informed about some of the possible inferences that a service provider (or a group of service providers) can make based on their previous and current data disclosures.

**Design suggestion:** Show how different data items can be linked together to form new information or deduce information about them which they might not like to disclose. A series of small network visualisation can be done showing common examples of combinations of data that can reveal more than people tend to imagine.

- **Focus group observation:** Both groups are aware that it is not only the explicit release of personally identifiable information that is important, but also what can be deduced from the data (like behaviours, attitudes, etc.). Information about such inferred data is even less transparent than explicitly disclosed data.

**HCI Principle:** Show people the data that they have disclosed explicitly, and show some of the possible inferences that a service can do based on that data.

**Design suggestion:** Show a form where people enter data. Then a tool will present a list that shows the possible inferences about their behaviour and personal data based on simple searches that can be conducted.

- **Usability test observation:** There is a difference in the understanding of explicit and implicit collection of data.

**HCI Principle:** Users should be made aware of implicit collection of data and inferences done by the service provider.

**Design suggestion:** When informing about explicit, implicit and inferred personal data, make the look of the explicitly sent (i.e. information that user sent explicitly, for example

during registration to a service) information different from the look of implicitly collected information or inferred information (i.e. information that the service provider collects without the user being fully aware of it, such as location, browser version, whether the customer is reliable, etc.).

### 2.2.2. Make data sharing and data processing along the cloud chain transparent, and provide the means to verify it

This requirement is based on four observations from different studies.

- **Workshop note:** There is a lack of transparency along the chain of (cloud) service providers in regard to their location and applicable laws. The main services providers that are contacted may be located in Sweden, while back-end (cloud) service providers are located in another country (Cf. also [Art12])

**HCI Principle:** Users have to be informed about the country and legal regime of the data controller and data processors and/or the contract's explicit choice of law along the cloud chain.

**Design suggestion:** Policy icons illustrating the storage location (e.g., inside or outside EEA) and/or applicable laws.

- **Workshop note:** It is difficult for individual and business end users as well as auditors to track data in the cloud and to find out who has or has had access to the data for what purposes.

**HCI Principle:** There should be usable and selective audit and transparency tools which even make the handling of explicitly and implicitly collected data (e.g. via the Facebook Like button) transparent (incl. information about data processing purposes).

**Design suggestion:** Different visualisations of the users' previous implicit and explicit data disclosures and of the data flows to different service providers could be applied, using, for instance, a timeline view or a trace view. Information about agreed-upon policies can be provided by clicking on service provider representations in a trace view visualisation.

- **Focus group observation:** Both non-experts and advanced users have an idea that data are being forwarded to third parties by service providers. However, non-expert users seem to have a less clear idea of who these third parties may be.

**HCI Principle:** i) The interface should put emphasis on explaining the distribution of information to third parties in a clear way. ii) Present the purposes for which these third parties are allowed to use the data. iii) The interface should also explain that sometimes the third parties are not specified or identified by service providers in their policies. (No specific design solution suggested.)

- **Trust review:** Well-placed trust grows out of active enquiry ([O'n02]; [Wam10]; Trust-guide TG2 in [LCP06]).



**HCI Principle:** Users should be able to pursue experimentation and enquiring. Users should be guided beyond enquiring only of friends and relatives.

**Design suggestion:** (i) Safe environments for experimentations and enquiries (the environments must not oversimplify the complex cloud service ecology). (ii) Make it possible to enquire “good sources”.

### 2.2.3. Provide indicators for the liability, security and/or trustworthiness of nodes along the cloud chain

- **Workshop note:** Services (such as hotels.com, resia.se) operate only as a mediator/broker, but take no responsibility if something goes wrong. Service brokers have to inform the users about who is the responsible data controller/service provider, with whom the agreement/service contract is actually made.

**HCI Principle:** User interfaces of service brokers have to clearly inform the users about the identity of responsible data controller/service provider with whom the contract is made. (No specific principle suggested.)

- **Focus group observation:** Expert users have a clearer idea of where attacks can happen and of possible counter measures. Non-expert users had an idea that information can be at risk, but it is very unclear for them what can be attacked, why the information is vulnerable, and the approaches to mitigate the problems.

**HCI Principle:** Lay users need help creating correct mental models of what is vulnerable/risky and what is safe. They should be able to understand when they are performing risky actions and feel comfortable or confident when their risks are minimal. Risks should be communicate to users by showing consequences of behaviours in a minimalistic way.

**Design suggestion:** Indicate different risk levels with colours and clear explanations. Use adequate language that would communicate the right message to the right user group. Provide layered explanations in an understandable way that can be read in more detail if users are interested, thus catering for the different experience of users.

### 2.2.4. Policies need to make transparent the possible consequences of data disclosures in different (and especially in recurrent) situations

- **Experiment result:** Perceived sensitivity of data can influence people's behaviours in regard to exercising control. However, data that might be perceived as non-sensitive (or harmless) can become sensitive with changes in time and/or context.

**HCI Principles:** i) Users should be informed about possible scenarios in which data items could become sensitive. ii) Users should also be aware about the different purposes for which their information might be used, as well as the possible recipients of their data, since this can affect their behaviour. The perceived sensitivity of data can be dependent on the context in which it is used.

**Design suggestions:** i) In the user interface, provide inline examples of data aggregation or misuse of seemingly harmless data. ii) Provide a visual indication of how their data



might be transferred across the cloud chain or shared with third party services. Icons for data processing purposes could indicate context information in regard to the potential use of the data by these services.

- **Experiment result:** Users are willing to disclose personal data that are perceived as non-sensitive in exchange for a reward that seems valuable.

**HCI Principle:** Users should be made aware of the risk and benefits of disclosing their data to a service.

**Design suggestion:** Make users conscious about the value of the data they are releasing comparable to something they can relate to, like the estimated monetary value (that the data has for the service providers).

#### **2.2.5. Make explicit that a service is a cloud-based service and what this implies in terms of privacy/security for the intended user**

- **Experiment result:** Users are unaware or not well informed about the types of online services they subscribe to in regards to the handling of their data and personal privacy.

**HCI Principles:** i) Cloud providers should inform individual end users about the services' privacy policies and make the implications of data disclosures transparent to these users. ii) Ex ante transparency awareness should be promoted, in order for users to know what type of service they are subscribing to.

**Design suggestion:** Make it explicit through the wording and the use of standard icons the consequences in terms of benefits and risks of having personal data in the cloud.

- **Trust review:** Transfer of trust: trust in the company itself is often transferred to trust in the security of company's cloud services [MT12].

**HCI Principle:** Users should be clear about the difference between service performance and privacy performance.

**Design suggestion:** Make evaluation results concerning trustworthiness prominent.

#### **2.2.6. Provide easily comprehensible policies informing data subjects at least about the identity of the controller, other responsible parties, for what purposes the data will be used plus other details needed, so that they can understand the implications**

Four observations motivate this requirement:

- **Workshop note:** It is unclear for individual users how they can get redress or compensation if something goes wrong, and whom they should contact in this case, especially if sub cloud providers are used (for instance, a user signs up with the service Box providing a cloud service, and Box uses Amazon as a sub cloud provider).

**HCI Principle:** It has to be clear and understandable for the user who the responsible parties are and how they can be contacted in case of disputes.

**Design suggestions:** i) Clearly display the contact address of responsible parties on the top layer of multi-layered policies. ii) Redress tools have to support end users in contacting the data controller or responsible party.

- To this problem comes the workshop note mentioned under section 2.2.2 (lack of transparency along the chain of services as regards applicable laws).

**Experiment result:** Knowing and controlling who is able to view/access and see users' data stored in the cloud as well as how the data are used are appealing features.

**HCI Principle:** It should be easy for users to find and adjust functionality related to the visibility and usage of their data for specific purposes.

**Design suggestion:** Provide privacy-friendly default settings for data access controls and usage that can be easily adapted "on the fly" (as for instance suggested in [AFHPW12]).

- **Legal considerations:** Data subjects have the right to be informed at least about the controller's identity, purposes and other details as required under Art.10 EU Data Protection Directive 95/46/EC and should also be informed about any further information needed for making data processing in the cloud transparent and compliant with data protection laws.

**HCI Principle:** The data subjects know at least who is the controller of their data, for what purposes the data are obtained plus other details (e.g., contacts and geographic locations of data centres along the cloud chain, applicable laws, how requests by law enforcement are handled, etc.), so that they can understand the implications.

**Design suggestion:** Policy information is (1) provided in a way that accounts for the users mental models; (2) structured in multiple layers following the Art.25 WP recommendations [Art04]; and (3) complemented with suitable policy icons.

#### 2.2.7. Make trust-enhancing indicators intuitive, consistent and believable, as well as appealing for the appropriate user group

- **Workshop note:** i) There are no commonly used seal/labels for security and trustworthiness for cloud services (apart from the more recent CSA and Cloud Industry Forum certifications). If there were, how would the users know what labels to trust? ii) Individuals are often not interested in understanding all details of trust seals, but would rather like to know in general whether their data are secure.

**HCI Principle:** Information about trust seals should be displayed in an understandable manner. Further information about the meaning of the seal should be easily accessible.

**Design suggestions:** i) Information about trust-related aspects of seals can be hierarchically structured in different layers (similarly as multi-layered privacy policies as suggested by [Art04]). ii) Standardized and broadly used seals can be more easily recognized and understood. iii) In-place information about what a seal means can be provided, e.g. via tooltips or information dialogs and/or links to official information regarding the seals.

- **Experiment result:** People may become skeptical towards unknown services that promise to guard their privacy.

**HCI Principle:** The cloud provider should explain not only the benefits for users, but also the benefits for the cloud provider itself when offering accountable and privacy-friendly features to its customers. (No specific principle suggested.)

- **Experiment result:** Trust regarding unknown cloud services might have a cultural component to it. Users from different cultures exhibit different levels of trust.

**HCI Principle:** Cloud provider should consider their customers in terms of the culture, location of service, and legislative regimes and cater for their collective mental models and attitudes towards data in the cloud.

**Design suggestions:** i) When users are about to subscribe to a cloud service, appeal to their cultural background by emphasizing features of security, access policies and the like. ii) Accountability and transparency features might balance the level of trust across different cultures.

- **Trust review:** Internet is regarded as intrinsically insecure [ACC<sup>+</sup>05]; cf. the cloud study by [ISKČ11]; cf. also [TKD<sup>+</sup>09]; [The13]).

**HCI Principle:** Users needed more accurate and robust models to be able to discover and trust cloud computing services. [MT12]

**Design suggestion:** In the user interface: users should be directed to sources they would normally rely on. Trustguide TG1 speaks of the necessity of taking measures also outside the user interface; this does not directly translate into HCI requirements, but the UI should relate to it [LCP06].

- **Trust review:** perceived availability, access, security, and reliability would be key variables of cloud computing acceptance in public sectors since they were found to be influential in predicting the behavioural intention to use cloud technologies ([Shi13], p. 200).

- **Trust review:** A business first attitude in cloud adoption where economic considerations far outweigh privacy concerns.

**HCI Principle:** Business end users need to be correctly informed about cloud security, privacy, performance, and availability for individual cloud services they consider. This requirement holds for private sector [Pea13] and public sector [Shi13] alike. For private sector this requirement also meets the problem of the business first attitude if accountability measurements are included in the information so that such aspects can easily be included in the decision process.

**Design suggestion:** If available, display trustworthiness by evaluation results in regard to security, privacy, performance, and availability. Use visualisation of an accountability model and match with visualisation of current chain.

#### 2.2.8. Users should be able to know the approach and consequences when deciding to end the service

- **Workshop note:** At the time of service registration, end users do not think about how to end the service in the future. While the registration for a service is usually made easy, it is often (made) difficult for end users/organizations to unregister/terminate a service contract, delete data or transfer data to other service providers. It is not always clear to end users whether they “own” their data (or are still in control of their data), as they do not check the terms and conditions carefully.

**HCI Principle:** Information about service termination, any continued use of the data by the provider or others even after the termination, data deletion and portability should be easily accessible and comprehensible for end users.

**Design suggestion:** Clearly present information about the option and rights of deletion and data portability in the context when it is relevant (e.g., when a service is terminated).

- **Trust review:** Perceived lack of longevity of identifiers makes users blur partial identities: preference for long-lasting identifiers (such as personal email addresses rather than appropriate work-related email addresses [VOO13]).

**HCI Principle:** Users must trust that they can manage in a life-long way the information associated with different identities (implications for transparency and restitution controls).

*Design suggestion:* (No obvious way to bridge the trust gap or where to bridge it.)

#### 2.2.9. Users should be aware of the extent to which they can act under pseudonyms

- **Trust review:** Anonymity option unknown: unawareness of options for identity management has negative effects on trust in privacy-enhancing technology [ACC<sup>+</sup>05]).

**HCI Principle:** Users must be able to understand the extent to which they can act under pseudonyms and that they could also access to transparency information when acting under a pseudonym.

**Design suggestion:** Within the user interface demonstrate how pseudonymity and anonymity options work, and how users could access their data under a pseudonym.

#### 2.2.10. Inform users about the termination of their contract in a clear and straight-forward manner

See the workshop note under 2.2.8.

#### 2.2.11. Make reasonable claims about the privacy and security policies and technical capabilities of the service to promote trust

- **Trust review:** Unsubstantiated claims do not build trust (Trustguide TG6, in [LCP06]: this issue concerns a long-term perspective; one company’s misconduct can affect a whole sector).

**HCI Principle:** Users must be able to put the right scope to their distrust.

**Design suggestion:** Make privacy and security statements short and very clear, and make the scope (i.e. to whom they apply) very explicit.

## 2.3. Exercising data subject rights

### 2.3.1. Make users aware of their data subject rights, and support them to exercise their rights; in particular, make control options that are relevant in certain situations more obvious at those particular situations

We refer to several observations here. As in 2.2.6, in addition to the rights to be informed but also the problem that the right to redress and compensations are unclear to users. Moreover, the following three observations motivate 2.3.1:

- **Focus group observation:** Expert users' concerns go beyond the use of personal data, but deal also with people's rights and democratic governments. Non-expert users are less aware of their rights concerning the protection of their data.

**HCI Principle:** Interested users should be able to audit the chain of cloud services. Who has accessed data, for what purpose, why did they access those data a particular occasion, with whom data were shared with, etc. It should be easy for people to exercise their rights regarding data protection and handling practices.

**Design suggestion:** Make users aware of their rights with links to information (in further policy layers), and help them exercise them by providing them with clear options for action and show a list of logged data that users can query with various questions related to their personal information. Queries can help to filter results that are of relevance for the users. Display a visualization of the chain of clouds and their potential vulnerabilities.

- **Legal considerations:** Data subjects have the right to access their data pursuant to Art.12 EU Data Protection Directive. Data subjects may have further rights in regard to the processing of their data according to that Directive and more specific laws, e.g. in Sweden a data subject has the right to information on who have accessed the data subject's data according to the Swedish Patient Act.

**HCI Principle:** Data subjects are conscious of their ex post transparency rights, understand and can exercise their rights.

**Design suggestion:** i) Ex ante Transparency functions are displayed prominently and obvious to operate. ii) Transparency functions are based on a suitable metaphor and/or account for the user's mental models. iii) Transparency functions are made available at the right time / in the right context, e.g. tracking logs should display online functions to exercise the right to access. A "right of access button" could be provided that if clicked allows to see list of what info can be accessed including tracking logs.

- **Legal considerations:** Data subjects have the right to correct, delete or block their data pursuant to Art.12 (b) EU Data Protection Directive. Further rights, such as the data erasure or the right to data portability, are currently proposed.

**HCI Principle:** Data subjects are conscious of those control rights, understand and can exercise their rights.

**Design suggestion:** i) Functions for exercising data subject rights are displayed prominently and obvious to operate. ii) Transparency functions are based on a suitable metaphor and/or account for the users mental models. iii) Transparency functions are made available at the right time/context, e.g. at the time when users are accessing their data locally or online.

### 2.3.2. Provide clear statements of what rights apply to individual users considering different factors, such as the users culture or location and applicable legal regime

Again, we refer as in 2.2.6 to the data subjects' rights. In addition, we would mention:

- **Workshop note:** Web services that target their business to Swedish customers (by having a Swedish website, a Swedish telephone support number, using SEK as a currency, etc.) fall under Swedish consumer and data protection laws, even if the business is located outside of Sweden and independent of what contracts say.

**HCI Principle:** User should be informed about the applicable consumer rights. Redress tools should (at least in these cases) allow users to contact the data controller in their native language. (No specific principle suggested.)

- **Trust review:** Users from different countries may have different privacy expectations and understanding of privacy guarantees offered by the cloud storage system [ISKČ11].

**HCI Principle:** Internationalisation involves going beyond just translating the service interface and privacy policy [ISKČ11].

**Design suggestion:** When seeking customers outside EEA, seek expertise to cover different populations' expectations.

- **Trust review:** Restitution measures have positive trust effects (Trustguide TG3-4 by [LCP06]).

**HCI Principle:** Clearly highlight the possibility and ways of redress.

**Design suggestion:** Users' interfaces for transparency tools, such as the Data Track, could mark restitution measures.

## 2.4. Obtaining consent

### 2.4.1. Make users aware of pros and cons of their possible choices in an unbiased manner

- **Experiment result:** Users willingness to release personal data is influenced by the description of alternatives (users tend to prefer short-term benefits).

**HCI Principle:** Make users aware of all pros and cons of their choice in an unbiased fashion.

**Design suggestion:** Tooltips and/or help texts to clarify consequences of actions.

- **Trust review:** Unsubstantiated claims may also build trust [JRBS10]: the problem here is that well-articulated privacy assurances make many individual end users trust a service's competence and intentions.

**HCI Principle:** As users do not scrutinise privacy statements etc., users must be made aware of trustworthy assessments of trustworthiness.

**Design suggestion:** Make evaluation results concerning trustworthiness as prominent as cloud providers' privacy and security claims.

#### 2.4.2. Obtain users' informed consent by helping and motivating them to understand policies and service agreements, so that they understand the implications

- *Workshop note:* Often individual end users do not make a really informed choice. It is easy to deceive people because they often neither read nor understand the agreements.

**HCI Principle:** Display privacy policies in a simple and understandable manner.

**Design suggestions:** i) Privacy policy statements could be explained in short videos clips (produced by consumer organizations), at the time when the user has to make choices. ii) Display a graph view of personal data flow, showing how the service provider that users are contacting is connected to other services and the possible distribution of users' data for different purposes. iii) Drag-and-drop data handling agreements can also help users to consciously understand what they are agreeing to.

- **Workshop note:** Individual users find it difficult to read and understand long and complicated contracts/terms and conditions that are posted online. Often data loss, i.e. unavailability of their data, is the greatest of the consumers' concerns, but limitations of availability (in terms of the amounts of time that data are accessible) mentioned in terms and conditions are not transparent to them.

**HCI Principle:** Users have to be aware of and understand important service limitations.

**Design suggestion:** Use of UI elements for making users aware, e.g. suitable icons.

- **Legal considerations:** Personal data processing in the cloud can be legitimised by the data subject's unambiguously given consent pursuant Art.7 (a) EU Data Protection Directive.

**HCI Principle:** Users give really well informed consent and are understanding the implications.

**Design suggestion:** Consent is obtained by click-through agreements associated to short privacy notices (top layer notices of multiple-layered policies), or via DaDAs (Drag and Drop Agreements) as discussed in [PFHD<sup>+</sup>05].



## 2.5. Privacy preference management

### 2.5.1. UIs for preference settings need to make consequences in different recurrent situations and risks and benefits of disclosure transparent

Two observations: Lay users need help creating correct mental models of what is vulnerable/risky as noted in 2.2.3 above, and users must be able to understand the extent to which they can act under pseudonyms and that such identification schemes can provide access to transparency information, as noted in 2.2.9.

### 2.5.2. Make users aware of pros and cons of choices in a comprehensible and unbiased manner

Same as 2.4.1 under Obtaining consent.

### 2.5.3. Offer appropriate default settings and choices that are privacy-friendly and reflect the users preferred options

- **Workshop note:** Users have the need to classify their data or groups of data (e.g., by marking personal data that is perceived as especially sensitive, confidential data). Data classification is needed in particular for risk analysis and by policy tools.

**HCI Principle:** Users should be guided when defining and editing labels to classify their data in an easy and meaningful way. Moreover, the user should be able to browse through these data by the defined categories.

**Design suggestion:** Provide a filter that allows users to select which categories (labels) are displayed. A tree view can be provided where users can check/uncheck the data to be shown. Alternatively, use tabs to divide the different categories.

- **Workshop note:** Security and privacy risks are not very clear and comprehensible to many individual end users. Even security incidents have no long lasting impacts on the user's risk awareness. On the other hand, they are not interested in policy details but just would like to know whether their data are safe.

**HCI Principle:** Users should be able to understand risk evaluation results, especially if these describe serious risks of non-compliance. They must be informed about privacy breaches/non-compliance in regard to data that they have already disclosed, in such a way that they are aware of and understand those risks.

**Design suggestion:** An overall risk evaluation results can be displayed in a prominent way, using a multi-layered structure [Art04]. The presentation should be based on suitable metaphors.

### 2.5.4. Let users do settings at the moment when it is relevant (“on-the-fly” management of privacy settings)

- **Experiment result:** Users are unmotivated to spend cognitive effort or time in setting up privacy controls.



**HCI Principles:** Users should be motivated to spend the necessary cognitive effort or time in adjusting their privacy preferences at a moment that is relevant to them and meaningful to their actions. Consequences are easier to grasp than technical features and terms. Inform users not only about how settings can be adjusted, but the consequences of adjusting such settings.

**Design suggestion:** i) Provide appropriate privacy-friendly defaults for a set of situations in order to ease the users' burden of setting privacy preferences. ii) Let users adjust their preferences "on the fly" as needed. Providing brief but meaningful explanations in terms of the privacy consequences might motivate users to care about adjusting. iii) In order to enhance users' comprehension and motivation, a cloud provider should present its privacy-enhancing features in a way that relates to users' everyday reality and strive to put technical explanations in secondary information layers.

#### **2.5.5. Explain consequences not in technical terms, but in practical terms ("speak the user's language")**

- **Workshop note:** It is often unclear for individual users what cloud providers really do with the data (e.g., if they are linking and merging different registers) and whether they are following negotiated or agreed-upon policies and contracts.

**HCI Principle:** Users should understand data processing purposes and consequences. And, as in 2.5.3, users must be informed about serious risks of non-compliance and what this may imply when they set preferences, and about privacy breaches/non-compliance in regard to data that they disclosed.

**Design suggestion:** Present consequences by "speaking the user's language".

### **2.6. Privacy policy management**

#### **2.6.1. Make it possible for business end users to negotiate what is negotiable, and make negotiation clear and simple**

- **Workshop note:** In contrast to traditional outsourcing, standard contracts are usually used for cloud computing, which are often less negotiable for business end users in terms of security and privacy and indeed most other matters.

**HCI Principle:** Make it possible for users to negotiate what is negotiable, make additional service offers clear, and the negotiation process clear and simple.

**Design suggestion:** Provide opt-in alternatives, e.g. in regard to the country/legal regime of the data storage location.

#### **2.6.2. Provide opt-in alternatives, e.g. in regard to the country/legal regime of the data storage location**

Same motivating observation as for the requirement immediately above but here we raise the suggested HCI design to a requirement.

## **2.7. Ex post transparency**

### **2.7.1. Make users conscious of their ex post transparency rights, so that they understand and can exercise their right of access**

The motivating fact behind this requirement is of course that data subjects have the right to access their data pursuant Art.12 EU Data Protection Directive, etc. etc. as mentioned in 2.3.1 above.

### **2.7.2. Make users aware of what information services providers have implicitly derived from disclosed data**

As in 2.2.1, we noted in focus groups that non-expert users are less aware of the possibility of further data about them being derived or inferred from their explicitly-disclosed data, and of the consequences of possible misuse of their data.

### **2.7.3. Make users aware of the data processing and sharing practices of the service provider**

One should observe that it is often unclear for individual users what cloud providers really do with the data as mentioned in 2.5.5; cf. also 2.2.1 on non-expert users' belief that acting entities are more related to each other than they might be in reality, and 2.2.2 on the issue that non-expert users do not appear to have a clear idea of what third parties may be involved.

### **2.7.4. Help users making data traces transparent, e.g. by providing interactive visualisations**

The general problem is the one quoted in 2.2.2 that it is difficult for individual end users, business end users as well as auditors to track data in the cloud and to find out who has or has had access to the data for what purposes. In addition to the obvious requirement deriving from this, we add the suggestion about interactive visualisations from the following experimental results:

- **Usability test observation:** Visualizing data releases through a trace view was found useful, intuitive and informative. It seems to be preferred over a timeline view.

**HCI Principle:** Users should have an intuitive and interactive way of visualising previous disclosures of personal data.

**Design suggestion:** Data releases could be visualised as a bipartite network, with one possibility having the user as a node in the centre and links branching on one side to the different services (and chain of services) with whom he has had a relationship, and on the other side linking to the data items that have been released.

## 2.8. Audit configuration

### 2.8.1. Provide a standard way to perform audits across the chain of services. In particular, provide audit functions that visualise differences of SLAs along the cloud chain

- **Workshop note:** Service Level Agreements (SLAs) of different cloud services along the chain may not match (in addition to the problem that SLAs aren't even defined in the same way).

**HCI Principle:** Tools for auditors and business users should visualize the differences between different SLAs.

**Design suggestion:** Display a visual chain of SLAs and indicate with colors or icons when there is a mismatch of SLAs. Let users click on a particular mismatching connection to see the details and support his decisions.

### 2.8.2. Provide audit functions that make also implicitly collected data transparent

As in 2.2.2 and 2.7.4, there is a notable difficulty for auditors (among others) to follow up data collection and processing.

## 2.9. Access control management

### 2.9.1. Allow users to classify their data items and easily provide access control rules for these data

See 2.5.3, the first workshop note.

### 2.9.2. Allow system administrators to verify the accuracy of access control rules in a straightforward and simple manner

- **Experiment result:** It is very difficult for system administrators to verify the accuracy of access control rule sets regarding the access control policy. Thus rule sets need to be understandable and manageable to assist system administrators in their task.

**HCI Principles:** i) Concise rule sets are better than large sets. ii) Redundant / contradicting rules are to be avoided. iii) Rule sets need to be designed to facilitate tasks for administrators.

**Design suggestion:** Tools, sets, and metrics that can support administrators to evaluate and compare the security and usability properties of different rule sets.

## **2.10. Privacy risk assessment**

### **2.10.1. Provide different types of user (business end users versus individual end users) with appropriate indicators obtained from risk assessment activities. Make risk awareness long lasting**

Cf. 2.5.3, second note, and 2.2.7 for the problem that many lay users regard Internet as intrinsically insecure.

### **2.10.2. Provide clear visualizations of vulnerability of private data depending on different situations**

As noted in the focus group observation quoted in 2.2.3, it is very unclear for non-expert users what can be attacked, why is the information vulnerable and the approaches to mitigate the problems.

### 3. Users' Perceptions of Policy Icons

#### 3.1. HCI Requirements, Principles and Icon Design Proposals

As pointed out in [PK03], legal privacy principles for transparency, consent and data subjects' rights "have HCI implications as they describe mental processes and behaviour that the data subjects must experience in order for a service to adhere to these principles". In particular, the principles require that data subjects comprehend the transparency and control options, are aware of when they can be used, are able to use them. As argued in [PK03], HCI requirements mapping legal privacy principles can therefore be grouped into the 4 categories (1) comprehension, (2) consciousness, (3) control and (4) consent. In this section, we are limiting the discussion to comprehension as the chapter deals with user perceptions of privacy icons.

**Comprehension:** The category comprehension comprises categories that allow a user to understand the transparency and control options discussed above. For supporting the user's understanding, HCI methods from cognitive psychology can be exploited that try to either evoke appropriate mental models or analyse whether already existing models can be accounted for. Hence, HCI principles that were elicited as described in deliverable D:C-7.1 by analysing the users' mental models of transparency and control functions can be helpful for making transparency and user control options well understandable.

Furthermore, user interfaces, which use real-world metaphors, e.g. in form of suitable icons, are easier to learn and understand (following Jakob Nielsen's usability heuristics of a "match between system and the real world" [Nie95]). Privacy policy icons have been researched and developed for visualising policy elements in stated privacy policies with the objective of making the content of legal policy statements easier to access and comprehend. Policy icons should preferably be standardised in future and usable across different cultures.

Within the scope of the PrimeLife EU project, a set of policy icons addressing the legal transparency requirements of the EU Data Protection Directive has been developed. These icons can be used to illustrate core privacy policy statements, namely statements about what types of data are collected/processed, for what purposes, and what the processing steps are [HNH11]. An intercultural comparison test of the policy icons conducted at Karlstad University with Swedish and Chinese students as test participants gave insights into which icons seem to be well understood by both cultures and which were understood differently by persons with different cultural backgrounds [Pri10]. Icons easily understood by both Swedish and Chinese students were, for instance, the ones shown in Figure 2, displaying types of data (personal data, medical data, payment data), the purpose "shipping," and the processing steps (storage, retention/deletion).



Figure 2: Example of well understood PrimeLife policy icons

Other Creative Common-like privacy icons have for instance been initiated by Aza Raskin

in 2010 [Ras10] and further developed by a Mozilla-led working group (who however stopped their work a few years ago). Interestingly, it includes special icons informing end users about how easily services sides are cooperating with requests by law enforcement (see Figure 3 for examples of the alpha release of icons). This is an important aspect that is often not transparent to cloud users.



Figure 3: Icon proposals (alpha version) by Aza Raskin informing about how disclosure requests by law enforcement are handled [Ras10].

For meeting the demand of higher transparency for data processing in the cloud, further policy icons can be helpful for informing about geographic locations of all data centres along the cloud chain, and in particular whether they are placed in the EEA (the European Economic Area), and, in case that they are located outside the EEA, some sort of information about their data protection levels if there are standardised ways of gauging this.

Complex privacy notices are usually neither read and nor easily understood. This is also due to limited cognitive capacity that people usually have, such as limited attention spans, memory, as well as a restricted ability to process a large amount of complex information at one time, as pointed out by Patrick and Kenny [PK03]. Comprehension of policy information can also be facilitated by a multi-layered structure of policy notices, as it was recommended by the Art. 29 Data Protection Working Party in their opinion on “More Harmonised Information Provisions” [Art12]. This recommendation takes the approach to structure complex policies into different layers, where the top layer is only providing a short privacy notice with the policy information that is at least required by Art. 10 EU Data Protection Directive (i.e., at least the identity of the controller and data processing purposes) and further detailed policy information can be obtained from the condensed and full privacy notices on other layers. Each layer should offer to the data subjects the information needed to understand their position and make decisions whether to plunge into deeper layers, or simply accept or reject the policy (and the service).

However, as discussed in the A4Cloud project, if data are processed in the cloud, it may be argued that more policy information beyond what is required by Art. 10 should be displayed to the data subjects for providing transparency depending on the circumstances. Such information as listed here may also have to be displayed in the top layer for allowing users to comprehend the implications:

- Contacts & obligations of all data processors along the cloud chain (as far as data processors can be determined ex ante);

- Geographic locations of all data centres along the cloud chain and, in case that they are located outside the EEA, information about their data protection levels;
- How disclosure requests by law enforcement agencies are handled;
- Consumer rights and applicable laws.

### **3.2. Privacy Icons in the LIBE Committee's compromise proposal**

In March 12, 2014, the European Union Parliament adopted a resolution on the proposal for new EU regulations on the processing of personal data [Par14] (see also [Par13]). In this resolution, as an annex to its Article 13a, icons as well as short texts are defined for the first level of such a multi-layered structure as mentioned above.

The set of icons presented in the Annex should raise some questions whether they are as suggestive of the content as intended. The proposal states that icons, texts (= verbal statements of the "essential information"), and a brief evaluation of whether the statements are met or not shall all be presented in a table. However, as experienced in several experiments, indications of deviations of desired conditions should be marked close to the corresponding data entering fields or close to any OK or ACCEPT button rather than in a separate window or as a text that the user is likely to scroll away from in order to find the OK button. It is therefore of interest to see how a user would understand the icons in themselves, especially if understood as implied by Annex 1 so that they can be used in notifications and not only in the table (otherwise a user inter-face designer might end up having two sets of icons with similar meanings).

Furthermore, as the table presents evaluations which are made according to a desired policy, the composition of statements and evaluation symbols is of interest to investigate. (The statements of the desired policy are called "essential information" in Annex 1.)

The following subsections first presents the bulk of Annex 1, then explains the rationale of a minor survey made with Media and Communication undergraduates to see how they apprehend the icons, and, finally, summarizes the survey and also presents some further thoughts on the composition of icons for information and alerts.

#### **3.2.1. Article 13a and its Annex 1**







The first page of Annex 1 is reproduced in Figure 4 together with Figure 5 showing two symbols a) and b) which are to be inserted in the right-hand column of the table. *Nota Bene*, the table in Figure 4 is not included in the official amendment text from 2014. This is probably just a mistake and accordingly we have to refer to the 2013 document. The Annex thus presents a table which matches icons to "essential information" and then continues by explaining that the symbols a) and b) shall be used in the third column if the conditions in the second column is met or not met, respectively. It is also stated specifically that the words in bold shall be in bold.

#### **3.2.2. Design of the questionnaire**

In order to have some idea of whether people would have a fairly consistent comprehension of the table in Annex 1, especially its iconographic parts, a survey aimed at a university class was

*Annex 1 - Presentation of the particulars referred to in Article 13a (new)*

*1) Having regard to the proportions referred to in point 6, particulars shall be provided as follows:*

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are <b>collected</b> beyond the minimum necessary for each specific purpose of the processing	
	No personal data are <b>retained</b> beyond the minimum necessary for each specific purpose of the processing	
	No personal data are <b>processed</b> for purposes other than the purposes for which they were collected	
	No personal data are <b>disseminated</b> to commercial third parties	
	No personal data are <b>sold or rented out</b>	
	No personal data are retained in <b>unencrypted form</b>	

COMPLIANCE WITH ROWS 1-3 IS REQUIRED BY EU LAW

Figure 4: The first page of Annex 1





Figure 5: a) and b) are symbols presented on the second page of Annex 1

designed. More diverse respondent groups can of course be considered, but if the students of a university class have very divergent notions of the iconography presented, there is no reason to assume that a larger survey would suddenly reveal a coherent conceptualization of it.

The presumption of the suggested reformulation of Article 13a is that a table can easily (meaningfully) be presented to a data subject “Where personal data relating to a data subject are collected”. Probably, a table with icons, legends, and evaluation indicators (the two icons in Fig. 5) may give a good explanation because different parts can be related to each other: “We seek and use visual structure” as one user interface expert and psychologist puts it ([Joh14], Chapter 3). The icons, for instance, can be quite arbitrary symbols as they will occur next to what is called the “essential information”. However, always presenting a whole table may be problematic if the icons and texts are to be used in recurring or varied UI situations.

Thus, the first question in the questionnaire simply read: “Describe what you think the icons below are about. You can write one single word or 1-2 sentences.” It was followed by the six symbols encircled by red in the same order as they have in the Annex 1 table.

The second question requested the respondents to match icons with the “essential information” as defined in Annex 1. The order of the icons remained the same while the texts were put in alphabetical order of the main word (the bold face words). Naturally, as only six alternatives were available, a fairly high score on this question could be expected if respondents used a strategy of mutual exclusion. However, as the goal of this questionnaire was not primarily to see if a user can understand the full table, the instruction included an invitation to the respondent that, “If you think several icons match a text or that one icon would fit several of the texts, you just mark that.” It would be interesting to see if there were alternative interpretations of one and the same symbol (and vice versa).

Finally, a noteworthy circumstance of the “essential information” is that the sentences are negatively phrased (“No...”). It might not be a problem in itself, but it means that the icons are intended to signal a negative statement. Thus the icons have the red circle found in traffic signs. However, a red circle with a diagonal bar is presumably clearer for a negative statement. This is the first problem one can envisage: the proposed icons try to make a compositional statement with an unwanted condition in the middle and a red circle to signal, “It is not the case that...”. The case is further complicated by the table’s third column, where an indicator is to be put to signal whether or not the composite statement is fulfilled or not. The symbol a) in Figure 2 is presumably understood as affirmative, but the symbol b) should mean that “It is not the case that the statement in the left and middle column is fulfilled.” Thus, for each row with a red cross, the interpretation should run, “It’s not the case that it’s not the case that...”.

To see if people were prone to generate such interpretations, the third question was placed above a depicted sample row, and ran as follows: “When you are about to enter some personal data at a site, you notice the row below. What do you think the site is trying to say?”

Admittedly, there are points where the design of the study can be questioned. For instance, situating the icons (or the whole table) on actual web pages would have been fairer to the proposal. On the other hand, research projects such as PRIME, PrimeLife, and the on-going A4Cloud have made clear that there are functions which would provide similar information to data subjects but without the purpose of consent-giving (cf. in particular the Data Track in the following chapter and earlier references: [JSP07], and Deliverable D:C-7.1, section 5.3.1). Thus, there are reasons to explore how generally understandable the icons are as well as the doubling of negations.

Pilot questionnaire: Before the questionnaire was handed out to the class, four people were asked to read the introductions and answer the questions. These were one administrator, two academic psychologists, and finally one student union representative. The intro was slightly rephrased after the first pilot tester. Moreover it was obvious that the “necessary information” texts had to be given in Swedish (e.g., a word like *dissemination* was not understood by all pilot testers). The order of the texts was not rearranged when Swedish translations were inserted. The questionnaire can be found in Appendix A.1 together with English translations.

### 3.2.3. Summary of the answers and some implications for UI design

The questionnaire was handed out to an undergraduate class in “Visual communication and design”. Everyone was willing to participate which provided 21 responses. The answers (translated into English) are given in a working paper [Pet14].

In question 1, only one respondent, #21, understood the red circle as some kind of negation. The question (in translation to English) was: *Describe what you think the icons below are about. You can write one single word or 1-2 sentences.*

We present one example here. It is the 21 comments to the first icon in Figure 4. Notably, it is only respondent number #21 who starts his/her answers by, “not. . .”. In the list, alternative translations are given within round brackets. Multiple answers are separated by semicolon.



#### # Description(s) given

1. search for people (people search); more info about the person
2. Detailed information
3. Examination (check, inspection)
4. Search information about a person
5. Examination of an individual
6. Alert (warning) about surveillance
7. Find a person
8. Personal data
9. Identification of person
10. Inspection area
11. This icon means that the page looks up personal data about you, the user

12. Save data [personal data]
13. In order to search person . . . ?
14. Background information; personal data
15. ?
16. Person check
17. Investigate
18. Investigate deeper (closer)
19. Check (examination) of personal data
20. Searching for people (People search)
21. not search on persons (not searching for people/individuals)

All in all, the interpretation deviated quite often from the concepts intended in Annex 1 of the proposal. Considering how many times the phrase “personal data” is used in the introduction to the questionnaire, it is disappointing to see how few references to privacy policy issues that are found in the answers. The actual word in Swedish for personal data, *personuppgifter*, seems however to have influenced the wording in some answers as some respondents have used the Swedish non-technical term *uppgifter* rather than *data* or *information* which in this case would be completely synonymous with *uppgifter*.

Question 2 “Try to match”: Only one respondent made multiple matchings so a simple evaluation of the result is reached by counting the total number of correct matches for each respondent. On average, it was not very high:

<b>Matches</b>	<b>6</b>	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>0</b>	
Number	4	1	3	6	5	1	1	= 21

A more thorough inspection of the answers, however, reveals that the translation of “are retained” to *bevaras* while the standard Swedish term for saving files in computer programs is *Spara* and this is often associated with the floppy disk symbol. Choosing *Sparas* instead of *bevaras* in the questionnaire might have raised the number of all-corrects with some 30-50 per cents.

The lesson to be drawn from this is that if icons are used that distinctly resemble well-known icons from other user interfaces, the wording in each language must match the standard “textual” translation of the icon. Thus, the intended message must be conveyed in that word and also be close in meaning to the standard use of the icon + word.

In question 3, icon number three gets a definitive interpretation because the icon and the “essential information” is put together just as in the table in the Annex of the amendments. This of course influenced the respondents and it explains why the answers actually deviate from the explanations provided by the respondents to the same icon in question 1. What is interesting is instead that in spite of the “essential information” provided in the table row, many respondents extended the meaning to cover also the forwarding of data. Four examples are included here:

#### # Description(s) given

1. Personal info is not shared with third party
2. Info will not be furthered to other parties, will not be used

3. The information is not shared with others
4. One will not share the [personal] data

Moreover, as the icon and the textual statement were combined with the red cross-out icon (Fig. 2b), the meaning should be that “It is not the case that this statement holds.” However from the four samples just quoted, and all other answers, it is obvious that the system of negation of negation presupposed by the table semantics does not work. (Respondent #21 and two others left no comments to this question.)

#### **3.2.4. Functional design of icons**

For the future, the different needs of different user interface designs should be considered. For instance, icons do not have to make statements but rather only indicate area; this is appropriate when an icon is only used to open a table or dialog box with the evaluation of what pertains to the particular data request made by that particular service provider. The icon then has a classifying function (a headline function). In order to call the data subject’s attention to a specific and problematic issue, a classifying icon can get a warning triangle superscript. Such a composition of icons can still function as a place to click or hover over when one wants to read more.

There might be other alerts a user wants to have than the ones motivated by an EU directive. Therefore, customer tailored integration of alerts must be considered.

Additionally, the information texts do not cover all the information that could be conceived as pertinent for cloud processing. The “essential information” may need to be extended and then icons or parts of icons may need to be reused.

### **3.3. Professional designers’ suggestions**

Within the A4Cloud project we engaged two professional designers<sup>1</sup> to suggest designs for five concepts which could be argued to fit on a top layer, that is before a user has investigated further what it means for her or him. These were:

1. Data processing inside or outside the European Economic Area.
2. Jurisdiction. Consumer rights and applicable laws as these may vary also within EEA.
3. Responsibility for data handling. In a cloud chain the responsibility towards the data subject might vary with the roles of the service providers.
4. Level of security. (Of course, it must be clear if it is self-asserted or independently certified.)
5. Service contract termination. What happens with data: deleted or filed; can the data subject get the data collected about him/her?

---

<sup>1</sup>Jessica Edlom and Mia Toresson Runemark, who also work part-time at Kau as graphic design teachers.

In the earlier list with four items (last in section 3.1), there was also the item “How disclosure requests by law enforcement agencies are handled.” It is a bit hard to test it in ordinary usability tests or simple questionnaires and it was left out from the work assignment for the two designers. Contractual arrangements were also neglected except for what happens with data on “service contract termination.” However, the latter is important both as regards information kept at service side and for the possibility for the terminating customer to receive his/her data which might have been built up during several years, whether it is friends’ contacts or detailed bank account statements. A term often used for the latter function, also when it comes to ordinary computer programs, is *export* (but other terms can be considered, such as *data portability*).

The designers were not introduced to previous work or the brief evaluation mentioned in the previous section. The interesting point was how people without this legacy would interpret these five fields. However, one consideration from the evaluation discussed in the previous section was included in the commission: each icon should scale down well. The HCI group and the designers had three meetings where first the five concepts were explained and then two drafts from the designers were discussed. Issues raised were: (i) coherence of appearance, if internet users would understand these icons as belonging to the same group; (ii) colouring as differentiation of concepts vs. colouring as signaling a valuation; (iii) an icon as selected (among a series of alternatives); (iv) text inclusion in the sense of having icon legends as permanent parts of the icons; and, of course, (v) graphic form (shape rather than colouring).

For (i), the designers had proposed unframed icons to contrast ‘filled’ icons where a background colour make up the square which the icons (without subscripts) roughly occupied. The reason why a colour scheme was not proposed was that colour was used for differentiating purposes within each group. The alternatives with filled background appeared as the more coherent ones, but it is possible that the unframed ones would work just as well in the context of a specific tool (notably, they look less like app buttons in a smartphone).

For (ii), several colours were proposed and discussed. While it may seem natural for the three ‘Level of security’ icons to have red for low security, some orange (amber, yellow) for medium security, and green for high security, it is less easy to assign such value-laden colours in other cases. The ‘Responsibility’ in point 3 above is really merely a statement of the role of a service provider, not an evaluation or assurance of whether the cloud service is *behaving* responsibly or not. Amber/orange for the non-responsible part is therefore a questionable colour, especially if the data controller is dressed in green, as our designers suggested. When later trying to set up a usage scenario (see below), we actually had to ask for both icons in the same colour, namely grey. To continue with (ii), for the DELETE criterion of the ‘Service contract termination’ series, the designers originally suggested red, to warn the users that their data would be deleted when they terminate their relationship with the service. The A4Cloud HCI group, on the other hand, had to explain the data protection perspective where ‘privacy’ is to be protected. In this case it means that a service should delete all personal data when a person exits the relationship. We argued for the colour green. But there was the argument that if someone only later understands that she had a lot of useful data at that service (e.g. contacts or pictures), she would not at all benefit from having the service deleting everything by the time of termination. The compromise was blue.


For (iii), the designers delivered series where one icon is clear and the other 1-2 icons are faded (40% of normal). With varying symbols and colours, this might not be the best way as

it might be hard to determine if a shade is a distinct colour for that icon shape or if it is indeed a faded (or highlighted) variant. The filled square icons seemed to be clearer than the icons without explicit borders (Figure 6 gives one example of icons without visible borders). Fading even more might be a workable solution as the assumption is that such non-selected icons appear among a short series of icons (three or just two), to position a selected sibling icon, which makes the identification easier of all icons involved.



Figure 6: Two of three Contract Termination icons are dimmed

For (iv), i.e. icon legends as part of the icon, it was easy to agree that when icons were sufficiently big, they would include some text. An icon in its standard size should include a brief text such as *Jurisdiction* from point 2 above. The designers carefully selected fonts and spacing to make the icons legends readable or recognisable even in rather small sizes. It was harder to find the right wording. For contract termination, the designers had suggested FILE where we argued ARCHIVE to make it more clear that data was not supposed to be used. (For the icons to remain clear in small format when the legend is not present, we did not argue for a sidescript indication of “deletion within x hours” as in Figure 2.)

For (v), flags instead of abbreviations for countries were discussed but dropped to minimise the colour plethora. The symbol for processing within the European Economic Area, , was explained by the designers as not confusing EU with EEA and further by not violating the rights around the use of the EU symbols. The legend of the icon (in full size) was “DATA PROCESSED INSIDE EUROPEAN ECONOMIC AREA”. The HCI group felt the legal argument was not necessarily the right perspectives for a research project. It might not be feasible within the A4Cloud project to finally solve the question how to refer iconically in this case, but EEA is definitively not on every EU citizen’s lips while all the EEA countries follow the EU regulations. This was an argument to evaluate more familiar symbols as *pars-pro-toto* signifiers. Two new symbols were suggested to the designers which they delivered, namely: one ordinary EU logo with a circle of yellow stars on dark-blue background surrounding the letters ‘EU’, but the icon legend still speaking about EEA as this text correctly describes the geographical area; the other icon again derived from the ordinary EU symbol but the letters ‘EU’ replaced by ‘EEA’ and, again, the text beneath the EU logo still speaking about EEA.

Furthermore, for (v) one can of course note that the icons in most cases are enough to explain the idea intended. On the other hand, what these designers aimed for was icons that could stand a miniaturization when the icons are just indicators or placeholder. What is more, these icons do not appear to be as falsely suggestive as the ones in the previous section. This fact, however, makes it harder to evaluate them by themselves.

The next section will discuss precisely this, i.e. evaluation, but it can be noted already here that Appendix A.2 contains a questionnaire with many of the icons produced by the two profes-

sional designers.

### 3.4. Discussion of evaluation methods

As just indicated, the less suggestive or seductive a series of icons are, the more difficult it is to use a simple questionnaire to see how they work. Instead it would be demonstrations or tests in which the icons appear in relevant contexts that make clear if they can be appropriate. We did both to be able to give some guidance for the future. Below an account is given of the discussions made in Work Package C-7.

#### 3.4.1. A second short questionnaire

In a questionnaire with three questions, 49 students who attended their very first day at university volunteered to give their answers. We had chosen the icons with filled background as these corresponded to the EU-starred icons used in the demonstration-based questionnaire described in the next subsection. The first question asked the volunteers to describe six icons or short series of icons with the subscripts:

- LOW SECURITY, MEDIUM SECURITY, HIGH SECURITY
- RESPONSIBLE DATA CONTROLLER (grey icon was chosen)
- NO RESPONSIBILITY FOR DATA (grey icon was chosen)
- SERVICE CONTRACT TERMINATION: **DELETE**, SERVICE CONTRACT TERMINATION: **ARCHIVE**
- SERVICE CONTRACT TERMINATION: **EXPORT**
- JURISDICTIONS

Figure 7 shows (parts of) the three answer sheets of the questionnaire (for a full view, see Appendix A.2). There was also a front page informing about data regulations and related matters. This was also presented orally when the questionnaire was handed out.

The second question began with a text explaining the role of services and their subcontractors, and then explained the responsibilities of each towards the data subject. The respondent was then asked to choose a suitable colour for each of the icons (shown in grey in the explanatory text and shown in grey plus eight other colours in the answer area, namely yellow, amber/orange, red, light green, dark green, black, light blue, dark blue). The intention was of course to see whether the value-free definitions would prevent people from seeing the RESPONSIBLE DATA CONTROLLER and a subcontractor with NO RESPONSIBILITY FOR DATA as evaluated according to some trustworthiness parameter.<sup>2</sup>

---

<sup>2</sup>One could of course argue that data subjects only have to know about the data controllers, because these are the organisations to approach to exercise one's rights. However, some subcontractors would possibly like to make themselves visible which makes it necessary to include them in a cloud chain statement and in ex post tools such as the Data Track. Then it should also be clear what role they play. This could possibly be made in several ways, but here we tried to have the designers to mark roles of each individual service rather than having some sort of forwarding to the data controller(s) responsible to the data subject for each data processor.



## D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

D1. Beskriv vad du tycker att ikonerna nedan handlar om. Du kan  
meningar.

LOW SECURITY	MEDIUM SECURITY	HIGH SECURITY

D2. I framtiden, när allt fler internettjänster är  
sammankopplade (ibland talar man om  
"molnet"), så kanske det finns program som  
gör att du kan spåra vilka underleverantörer  
dina e-tjänsteleverantörer använder sig av i  
molnet.

Om du undrar över hur dina data har använts,  
kan det vara bra om du i ett  
"spårningsprogram" snabbt ser vilka  
molntjänster som:

1. är ansvariga för den information de  
har om dig,
2. inte har detta ansvar eftersom de bara  
utför tjänster på uppdrag av de  
personuppgiftsansvariga företagen.

Vi har två symboler för dessa två typer av  
databehandlare i molnet.

RESPONSIBLE DATA CONTROLLER	NO RESPONSIBILITY FOR DATA

Om du fick välja att färglägga dessa båda  
symboler, vilken/vilka färger skulle du välja  
då?  
Ringa in en av färgerna i varje kolumn!  
(Du kan välja grå.)


D3. Det finns en del stater utanför EU som också  
– The European Economic Area (EU + Island, Li  
Vilken ikon du skulle föredra att man använde

Icon	Please, indicate w/ You can also add :

Vänligen, vänd ej blad  
förrän du blir ombedd att gå vidare!

Figure 7: Outline of the three answer sheets on designers' icons.

Finally, this short questionnaire included the three EEA symbols (only the 'inside EEA' icons, not the 'outside EEA'), under the heading: "There are some states outside EU that also follow EU's regulations. Together with EU they form EEA The European Economic Area (EU + Iceland, Lichtenstein, and Norway). Which icon would you prefer that one uses to show that data processing takes place inside EEA?"

As for the results, the concepts revealed by the answers in the first table of six rows clearly showed that different respondents made different associations:

SECURITY icons: web site security, personal data processing, and passwords security.

RESPONSIBLE DATA CONTROLLER: no one really saw it as a role description; many though it indicated transmission (often secure) to the cloud.

NO RESPONSIBILITY FOR DATA: no role description but often negative value laden connotations; a few saw it as an indication of *no* cloud processing.



DELETE, ARCHIVE icons: a few read them as intended; other results are interpretations of the orange symbol as "a form to fill out" and "menu button" (cf. smart phone menu icons).

EXPORT icon: several gave no answer while the ones that did wrote about "data export" without specifying if it was to data subject or to third parties (some thought it was the latter).

JURISDICTIONS icon: as intended by most respondents. 3 of 49 misinterpreted the paragraph sign as 'currency' which made for two interpretations of the scales as 'exchange' or simply 'bal-



ance'. Other misinterpretations read it as a claim or even proof of secure and lawful data processing.




The icons including cloud outlines does not seem to have indicated their meaning by the symbol but only by the text (when interpreted as intended). There was no cloud priming in the introduction to the questionnaire, i.e., there was no introduction to cloud computing or cloud service chains, and answers to the other icons did not use the term 'cloud' which suggests that the concept of the Cloud is not prominent among the respondents. Also some references to Apple's iCloud shows the danger to rely on any pre-understood meaning of cloud outlines or the term cloud. The few icon interpretations of the ARCHIVE symbol also suggest that some priming is needed. In the Data Track experiment described in the next chapter, the cloud icon  seems to be better understood than the server icon, . This result corroborates the conclusion that priming is necessary, even if the Data Track eye-tracking experiment revealed that people shun text which seems to argue for informing users by icons and also allowing users to perform functions by interacting with icons. To this should be added that the answers mentioning iCloud in the questionnaire show that any application will have to fight the appropriation by some vendors of common symbols. Also the now common use of three bars for menu icons (blue buttons with white ribbons; click to open a menu) makes the ARCHIVE symbol questionable, but in the same time the Data Track experiment shows the old, usual server symbol to be a cognitive burden. That is probably because many people have never had the reason to tell the difference behind a server icon and a folder icon.

The case is further complicated by the fact that the contractual condition referred by the icon legend is not spelled out in full in the legend. The part missing is "by the service", i.e., it is the service provider who will archive (or delete) the data subject's data when the service contract terminates. The same problem comes with the EXPORT symbol. The meaning must be made clearer (termination + "possible to export data to you"). Another class of students, who were working on these icons, suggested some sort of a swish to indicate movement (compare Figure 2's shipping icon) Still, there is nothing that says that the icons themselves should be amended, just that the context of the A4Cloud tool easily differentiate the meaning from any other icon or natural object with roughly the same shape.

Question 2 was preceded by the definitions of the two cloud actors' responsibilities. Despite this very explicit introduction, the interpretations was similar to the one originally displayed by our contracted designers: around 35 respondents marked green for the RESPONSIBLE DATA CONTROLLER and red or orange for the one subtitled NO RESPONSIBILITY FOR DATA (for the available colour alternatives, cf. Fig. 7). This suggests that any definition has to express more clearly that the intended responsibility is towards the data subject, but that subcontractors have their responsibilities towards the data controllers. In an A4Cloud tool, for any data processor marked as the second category it must be clear to the data subject or professional cloud customer to what cloud provider they should turn in the first instance. If icons are signifying 'Here you can find the relevant contact address', we might need only one icon. On the other hand, at least seven persons seem to understand the conditions: one marked both grey; another marked both light blue; a third both dark blue; four coloured left icon blue, right icon grey. Also the four people marking the right-hand icon black may have understood that no evaluation was involved. But in all, these 11 respondents constitute only 25% of these predominantly young

university students.



Votes in question 3:  13 (27%),  33 (67%),  3 (6%). As for the argument provided (by some) of the respondents, the advocates for a totally new design wanted to avoid confusion with EU, while the two-thirds voting for the hybrid icon (starred circle + 'EEA') saw it as an inspired combination of a well-known symbol and a new content. Thus, even if our professional designers for legal reasons feared using the starred circle, it seems indeed to be preferred. However, our argument that 'EEA' should be included should perhaps be re-evaluated. The scales or paragraph sign (or some symbol not mistaken for a '\$') inside the starred circle might be better than 'EEA', as the interesting question is whether EU regulations apply. That will not be obvious for all variants of the JURISDICTION icon (and may in the future not be confined to EEA).

As for the low support for the 'pure' EU logo (with the same EEA legend as the others), it is interesting to see the opposite preference by the subjects who were first presented an illustrated scenario (step-by-step screen shots) where the letters 'EU' were used in the starred circle.

### 3.4.2. Example of icons situated in a web service

The icons discussed in the previous subsection could be used in *ex post* tools to be put adjacent to information and as summaries of certain information. To get some sense of how data subjects may apprehend them in context, we did however an *ex ante* test so to speak, that is, we placed these icons with the brief texts in a context which most data subjects are familiar with, namely, on-line data disclosures rather than situating the icons in the A4Cloud tools. If a set of icons are used in the tools for transparency, the same icons should appear in situations of data disclosure (either by the services themselves, or by some tools data subjects may use to evaluate these services).

Hence, after a simple task of making an online registration at a booking service in order to make a hotel reservation outside EU (outside EEA), test subjects were asked to choose whether to give credit card information to the hotel or to pay immediately by giving credit card information to the booking service (inside EU, that is). When designing the case together with a Master student<sup>3</sup> who had not been involved in the project before, it became apparent that the two RESPONSIBILITY icons could not be coloured. The two roles should not be associated with any evaluations of reliability (trustworthiness) - that is not the essence of the question of who is the data controller. (Therefore grey icons were chosen for the questionnaire reported above.) Also, the conditions for 'Service contract termination' could not be DELETE, ARCHIVE, or EXPORT, as Figure 6 would have it. Rather, deletions and archiving are mutually exclusive alternatives, while the possibility to have the data about yourself belongs to another set of alternatives where the opposite is NO EXPORT, i.e. the service provider does not grant the data subject the right to receive the data collected or inferred.

<sup>3</sup>Thanks to Henrik Andersson for making the paper prototype and collecting data from the participants.

In our test case, we let the provider of the physical service, the hotel, be the one not providing the data upon termination. A drawback with using an *ex ante* scenario is that ‘Security’ is something that has to be stated by the web site itself. It is unclear why the icons for the two weaker levels should be used by any for-profit organisation. We could have replaced the security icon with an export icon, but we feared that test subjects might misinterpret EXPORT as ‘sent to third parties for whatever use’ which of course would have been the opposite value to the intended good value of ‘yes, this service promise to give you all your data when you terminate the contract’. Instead, we used a security icon and added a text for the EU company, that its MEDIUM LEVEL SECURITY did ‘fulfill the legal requirements found in EU data regulations’ (without specifying exactly what regulation this referred to) while the extra-EU/EEA hotel had a HIGH SECURITY icon to contrast the ‘safe’ EU booking company. On the other hand, the foreign hotel had an ARCHIVE icon in relation to termination. The popup at the booking service’s website is shown in ‘expanded view’ in Figure 8: all five icons are shown instead of only the ‘Inside EU’/‘Outside EU’ icons.

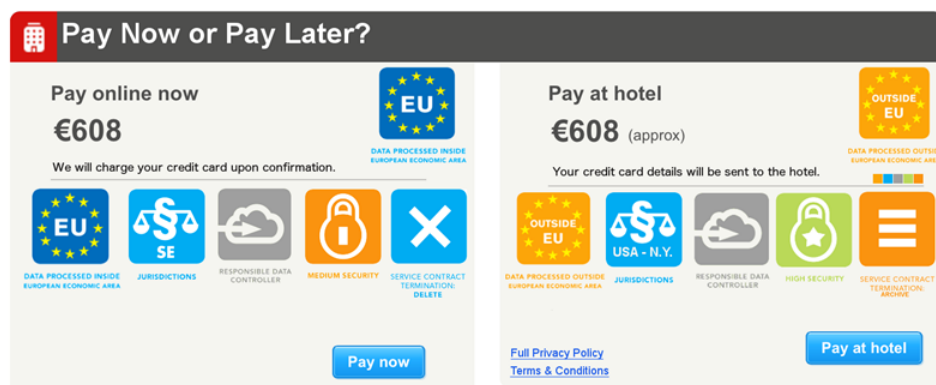


Figure 8: The popup to select pay within EU but in advance or later at the American hotel.

Participants of this evaluation followed the scenario and were then asked to fill out a questionnaire that asked about the reason behind their choice of payment method in a couple of questions, then asked them to comment on the four TERMINATION OF CONTRACT icons (i.e., including NO EXPORT), and also as in the other questionnaire reported above, about colour preferences for the responsibility icons and preferences as concerns EEA icons. After a pilot with five participants, which resulted in a final test design, 10 persons from a wide variety of backgrounds participated.

Several participants, both in the final test and in the pilot test, gave expression to the colours, specifically to the light green (and blue) coloured icons which gave them the feeling of a “secure and safe” icon. Besides that, the JURISDICTION SE and the EU icon also made the participants feel safe and secure.

Five out of ten participants argued it is better to “Pay later” as money is not paid in advance. But four of the five also gave privacy reasons, namely the higher level of security indicated. The other five chose the “Pay now” option, and justified it with their data being deleted upon termination of account, the Swedish jurisdiction and the information being processed inside the

EU. Thus, this ten people had a rather good understanding of what the conditions were.

The SERVICE CONTRACT TERMINATION icons made the participants feel very uncertain of the meaning of the icons, as shown by the answers. The icons for EXPORT / NO EXPORT caused the most problem for the participants with two not even being able to respond anything. Two other participants interpreted these icons as having something to do with travelling, e.g. “No help with the luggage” and “OK to bring luggage”. This may indicate that the context in which the icons is presented is very important. Initially, persons being presented to the icons may believe that the icons are event-specific more than general, which may lead to misunderstandings. (These responses also illuminates why general functional categories for icons, as for instance the ones recently presented by Jakob Nielsen [Nie14], do not offer any a priori help in design work: the correct applications of a category is not obvious until after user testing.)

Taking both the pilot test and the final test into account, eleven out of fifteen participants coloured the NO RESPONSIBILITY FOR DATA icon red. The RESPONSIBLE DATA CONTROLLER icon was coloured light green by eight out of a total of fifteen participants. Thus, it is again confirmed that a text about *responsibility* has to be explicit about *to whom* and for what.

All of the participants but one preferred the icons with the stars over the one with the arrows; eight chose EU over EEA, as it is “easier to understand” according to the participants. This is in striking contrast to the decontextualised questionnaire where the ‘pure’ EU icon got hardly any votes at all. This could be a consequence of the scenario participants having seen the EU icon at work in the scenario.

Because of some delays we were not able to test small versions of the icons in scenarios. However, despite some counter-intuitive icon texts, this scenario-based evaluation shows that big icons with legends can guide users in the right direction. Of course, it remains to be shown how easy it is to retain in memory the various symbols if they are used in a second scenario as indicators in small size without immediately visible text.

## 4. Users' Perceptions of A4Cloud Tools

### 4.1. Introduction and background

Previous studies carried out as part of other projects such as PRIME or PrimeLife have shown that users (individual cloud subjects) tend to have the wrong conception of the control that they have over their data stored at different service providers as well as on how these data is handled and shared among these services. Moreover, the concept of transparency is often hard for users to grasp, since they are not accustomed to have the possibility to see and control the data that is collected about them by different service providers.

As part of the A4Cloud project, we are developing a series of tools supporting the notions of accountability and transparency in the cloud. Therefore, one of our tasks within the project is to explore how the design of the user interfaces for such tools can evoke the right mental models of transparency and accountability for the cloud.

Within the scope of this Deliverable, we have focused on the evaluation of the user interfaces of the Data Track tool, as it is the one with the most advanced user interface development after project year two. Another reason for focusing on the Data Track usability evaluation is that the A4Cloud Data Track will probably serve as the basis for a privacy dashboard for cloud subjects, in which other tools, such as the plugin for policy violation, the Data Subject Access Request Tool (DSART), the Incident Response Tool (IRT) and the Redress and Remediation Tool (RRT) will be integrated. Therefore, the usability of the Data Track tool may play an important role for the success of the A4Cloud toolset for cloud subjects.

The Data Track tool is a user-side ex post transparency tool, which was first developed by us in the PRIME and PrimeLife EU projects [FHHW11], [PFHB07]. It is currently enhanced and extended in A4Cloud for providing transparency in regard to the processing of a user's personal data in the Cloud. Initially, the PRIME Data Track comprised of a history function for keeping a log of each transaction in which a user discloses personal data. The log contained a record for the user on which personal data were disclosed to whom, for which purposes, which credentials and/or pseudonyms have been used in this context as well as the details of the agreed-upon privacy policy. These transaction records were stored at the user side in a secure manner (protected by the PRIME core). In the PrimeLife project and in the follow-up A4Cloud project, the Data Track was extended with online access functions allowing users to exercise their data subjects rights to access their data at the remote services online and to correct or delete their data (as far as this is permitted by the services).

Usability tests of early design iterations of the PrimeLifes Data Track revealed that many test users had problems to understand whether data records were stored in the Data Track client on the users side (under the users control) or on the remote service providers side. Therefore, in the A4Cloud project, we have developed and tested alternative HCI concepts consisting of graphical UI illustrations of where data is stored and to which entities data has been distributed. One motivation for this new UI concept is that graphical illustrations of data storage and data flows have a potential to display data traces more naturally, like in real world networks.

In the next section 4.2, we will report on the results of the usability evaluations of two iterations of the graphical A4Cloud Data Track user interfaces.

Then, in section 4.3, we will summarise the results of a focus group workshop that was held in

cooperation with work package B-2 with individual cloud subjects to analyse their perceptions of the Data Track and their preferences in regard to incident reports to be delivered by the Incident Response Tool (IRT).

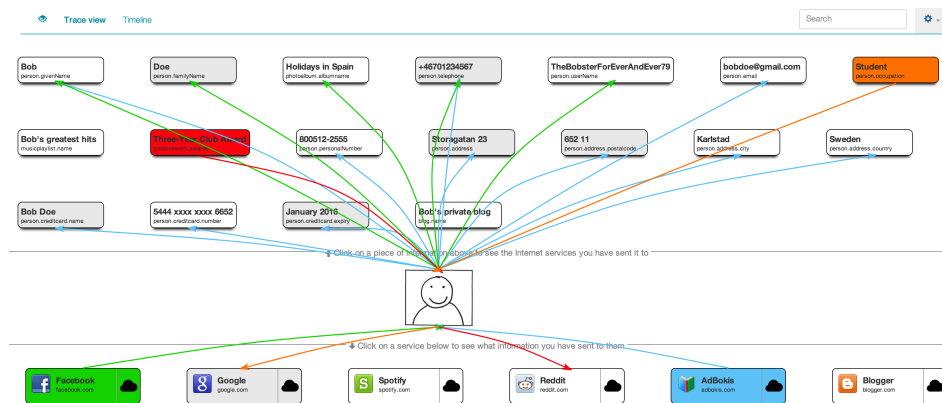


Figure 9: The trace view interface of the Data Track tool

## 4.2. Data Track usability evaluation

In order to understand the users' mental models with regards to the concept of transparency and the control of their data as described above, a series of usability evaluations were carried out for the A4Cloud Data Track tool in various iterations of the design process.

The evaluation of the first design iteration of the A4Cloud Data Track user interfaces implementing the initial graphical design ideas for this tool was conducted in the first project year and discussed in the deliverable D:C.-7.1 [AFHP<sup>+</sup>13] and in [FHAP14]. It is also summarised below for motivating the second design iteration, which was evaluated during the second project year. Afterwards, the usability evaluation of the second design iteration of the A4Cloud Data Track's interface is presented and discussed in more detail.

In order to perform the evaluations in a way that reflect a real life situation, we set up a scenario consisting of a fictitious online book store, where participants were supposed to buy a book and submit some personal data in order to complete the transaction.

During a test session, participants were asked to read instructions about the test, sign a consent form, and then pretend that they were purchasing a given book online. In order to complete the transaction they were required to submit some personal information (none of the information submitted was stored in reality and participants were given a fake credit card number). After buying the book, participants were shown the Data Track trace view interface (see Figure 9) and a test moderator asked them to complete a predefined series of tasks and answer some questions using the prototype, which are included in Appendix B.

The tasks and questions given to test participants had the purpose of answering general research questions regarding the level of intuitiveness of the interface, as well as users' understanding of the possibility to control their data disclosures and of the difference between the view showing the Data Track logs stored under their control (Figure 9) and the view showing

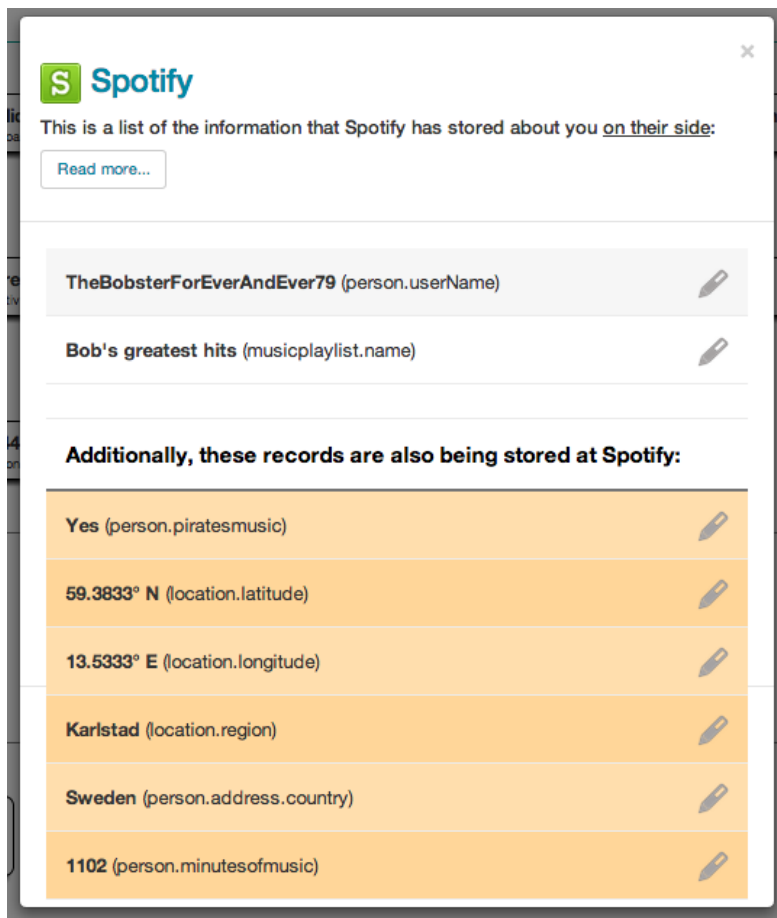


Figure 10: Personal data about a user stored at the services' side (collected explicitly or collected/derived implicitly about the user).



the data stored at the service providers' side (Figure 10). The order of many of these tasks was randomly altered in order to decrease the risk for latter tasks being answered more successfully, due to increased familiarity with the interface. A set of successful criteria for each task was set a priori and participants were asked to think aloud about their steps to solve those tasks. When they had gone through all tasks, they were also asked to answer a post-questionnaire with the intention of capturing their subjective opinions.

The objective of the usability evaluation was to research the following questions that are mostly related to usability issues experienced in earlier tests of the Data Track:

Q1 : Do users find the Data Track's trace view intuitive and comprehensible?

Q2 : Do users understand what data they have sent to whom?

Q3 : Do users understand the difference between the view showing the Data Track logs stored under their control (Figure 9) and the view showing the data stored at the service providers' side (Figure 10) and how to switch views for accessing their data electronically?

Q4 : Does the interface convey the idea that the services have collected information implicitly, and that it is more than the information explicitly sent by users?

Q5 : What are the expectations of users when removing an information attribute from the Data Track's interface?

**First design iteration.** In the first design iteration (described in more detail in the earlier deliverable D:C-7.1 from WP:C-7 [AFHP<sup>+</sup>13]), 14 people between 19 and 40 years old were recruited in different parts of the city of Karlstad, Sweden. 7 of them were working professionals and 6 were undergraduate students (1 preferred not to state occupation). All of the tests were performed using a laptop or tablet computer at the participants' locations at the moment that they were asked to participate in the test. For this first iteration, participants were asked to carry out through a series of semi-randomized tasks. For every task there was a set of successful completion criteria, and the test moderator annotated whether the participant completed the tasks successfully, partially or not successfully.

Evaluations on the first round of testing confirmed that users understood graphical illustrations of the flows of their data represented as traces connecting nodes. Results obtained from the moderator's objective observations while participants interacted with the tool as well as the participant's subjective answers to the post-questionnaire, showed good levels of intuitiveness of the trace view interface. The chart in Figure 11 depicts the participant's responses to statements related to the benefits of the tool.

On the other hand, the controls to access their data remotely on the services side did not provide enough *affordance*, and it was still hard for them to grasp the distinction between data logged locally by the Data Track program and data about them stored remotely in the services' databases (a challenge also identified in [AKLS13]). In this version, a pop-up dialog that displayed data located at the service providers appeared beside the service and showed data structured by the date (i.e., a timestamp) in which a disclosure was made to the selected provider. This forced users to drill down into each disclosure to see the actual attributes that



were disclosed at that instance. The details of the results of the evaluation of the first design iteration can be found in [AFHP<sup>+</sup>13].

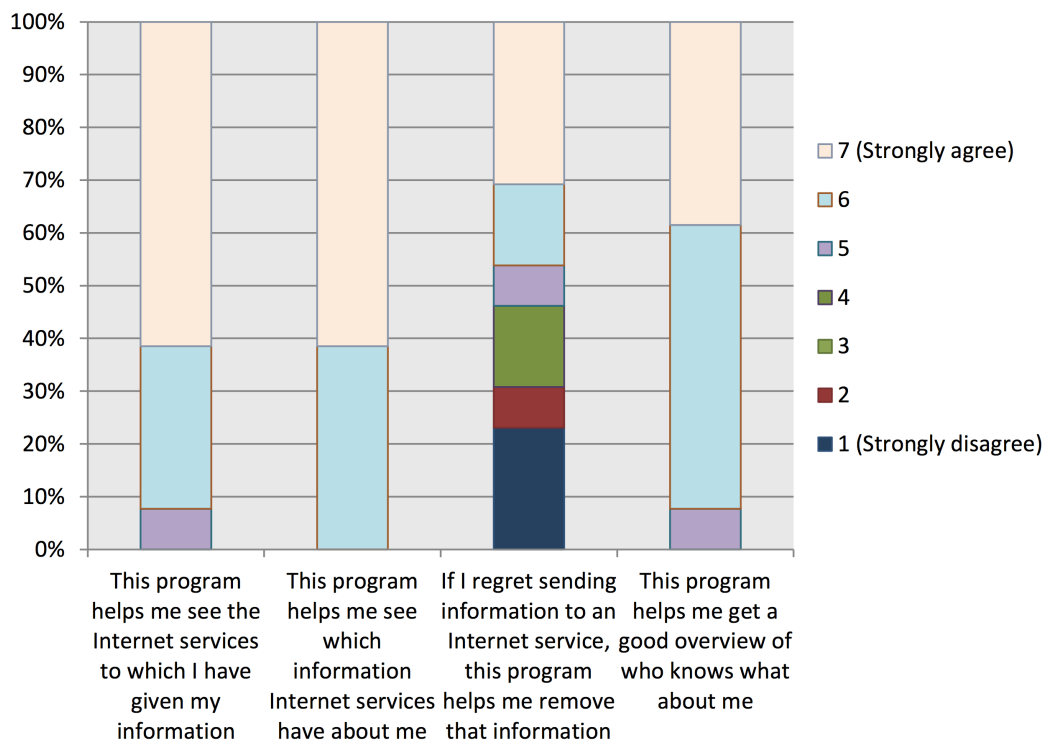


Figure 11: Some results from the first round of testing.

**Second design iteration.** For the second design iteration, we mocked up and implemented some improved functionalities in the interface based on the feedback and test results obtained from the first iteration. For one, an introduction tour was included that illustrated the different aspects of the interface and explained the distinction of the view showing data stored by the Data Track under the users' control and the dialog that showed data stored remotely at the service provider. The tour not only explain the difference between these views, but also how to access them. We also included timely tooltips to explain interface elements that were deemed important when users moved the mouse over them [Nie99]. Figure 12 shows an example of one of the tour's steps and a tooltip that appears when hovering over an element.

The dialog showing data on the service's side (Figure 10) was redesigned to be more aesthetically pleasing, conforming to standards of current designs (using the oostrap UI framework) capturing better the attention of the user, minimizing its learnability, and showing the service provider's icon more prominently at the top. More importantly, a clearer division between data disclosed explicitly and data collected implicitly was made by introducing prominent colours, a clearer heading and wider spacing.

This second design iteration was tested with 17 participants between the ages of 19 and 40

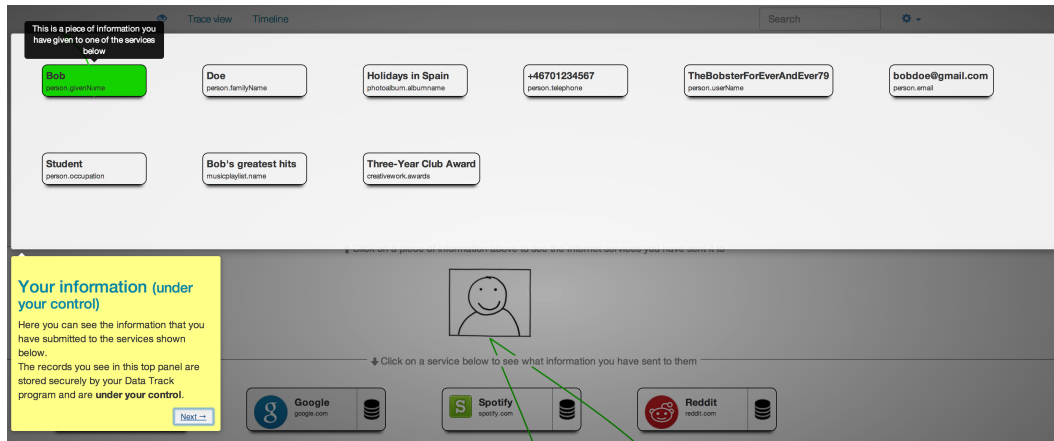


Figure 12: Example step of the introduction tour and of a tooltip in a data item.

located in the city of Karlstad, Sweden. Participants came from different cultural backgrounds and had different levels of computer proficiency. 9 of them were students at the University and the remaining 8 were either working or in between jobs. With 9 of the participants the tests were conducted at the University's usability lab (not necessarily the nine participants who were students) and eye-tracking equipment was used, whereas the rest of the test were carried in different locations around the city.

For this iteration, the tasks that participants were asked to complete were slightly revised in order to evaluate the changes made to the interface (as describe above) and to rework the tasks that were found to be confusing for participants of the first round (see tasks in Appendix B). For instance, instead of posing the question "In your opinion, can others access your data that Adbokis.com has stored on their servers?", we phrased the question in a more open-ended form, like "In your opinion, who can access your data that AdBokis.com has stored on their servers?" As for the first iteration a set of successful completion criteria were laid down for each of the tasks before the test sessions took place. Participants responses were categorized into these criteria, for instance one of the tasks asked participants to name out-loud "what do you think do the elements on the top represent?" and the moderator would record the participant's answer into the choices of "All of my own information", "My own information that I have sent to online services", "Other people's information", "No idea", or "Other". If the participant's answer didn't fit any of the four first choices, the moderator would mark it as "Other" and write down the actual answer. Additional comments were also annotated for each of the tasks in case relevant observations or interesting remarks were made by the participant.

Similarly to the first test iteration, participants were first introduced to the scenario of purchasing a book with the fictitious online bookstore Adbokis.com. In order to complete the transaction they had to submit some personal information such as their name, their home address, their email, their phone number, their credit card for payment (participants were given a fake credit card number that they used to purchase the book with). For reasons of consistency between test sessions and for privacy reasons, participants were asked to pretend that they were the character *Bob Johansson* as they carried through the transaction.

Once the transaction was completed, participants were asked to open the Data Track tool. Then they had to go through the introductory tour which explained the different aspects of the tool and how to access the services side view. After the introductory tour, participants were asked the tasks listed in Appendix B.

**Results of second design iteration.** In general, results from the usability evaluations of the second round of iterations confirmed that participants easily understood and appreciated having an overview of the data that they have sent to different service providers using coloured tracing lines. These results are consistent with the first iterative round. All 17 participants could correctly identify the services to which they had sent a particular attribute (e.g., their email address), and all the attributes that were sent to a particular service provider. Only one participant was initially unsure about what the elements in the bottom panel represented, stating that the squares portrayed “activities I have done on the Internet.” Another participant suggested that “if there would be a lot of things on the top, it would be good if there would be a *zoom* when I select something. For me some times is difficult to distinguish the different colours, it would be nice if what I select also becomes bigger.”

Most participants ( $n = 13$ ) believed that the Data Track log entries were either stored in some kind of servers belonging the Data Track ‘service’ or inside their computer, one participant was assured, for instance, that the data “is not stored in my computer. It is in my [Data Track] account”, while another participant had doubts if the entries were “on my computer... or maybe in a Data Track server?” In general the interface evoked the right mental model in 13 out of 17 participants, who understood that the records shown in the trace view were under their control. When asked to identify where would they click to access the information that the bookstore had about them in their servers, only 4 participants did not complete the task successfully, but they understood the idea after getting assistance from the moderator.

Once the modal dialog opened, all participants correctly identified that more data than they have explicitly submitted was collected and stored on the service’s servers. Eye-tracking analysis of the results revealed that participants paid a lot of attention to the section of the dialog on the right side on the bottom displaying the implicitly collected data, as shown in Figure 13. The uttered comments from participants also showed that realizing that a service collected data about them implicitly, without them being fully aware, created some kind of emotional reaction.

As a matter of fact, participants were asked to best describe their feelings when they were presented with the information displayed by the Data Track tool, and results indicated that the majority of participants experienced an activated emotional state (according to the circumplex of emotions suggested in [Rus80]). Taking into account participants from the previous evaluation iteration ( $n = 31$ ), 11 were astonished/surprised, 7 were scared/distressed, 3 were excited/enthusiastic and 4 were happy/pleased, the remaining 6 were in a deactivation state of being either relaxed or not caring.

When asked to choose all the possible entities who they believed would be able to access their data logged by the Data Track program, 7 participants out of the 17 (44% of the cases) indicated that “no one else, only me” would have access, which was the right mental model we wanted to create, since the data records displayed by the Data Track are stored securely under the users’ control, as described earlier. Participants also imagined others as being capable to

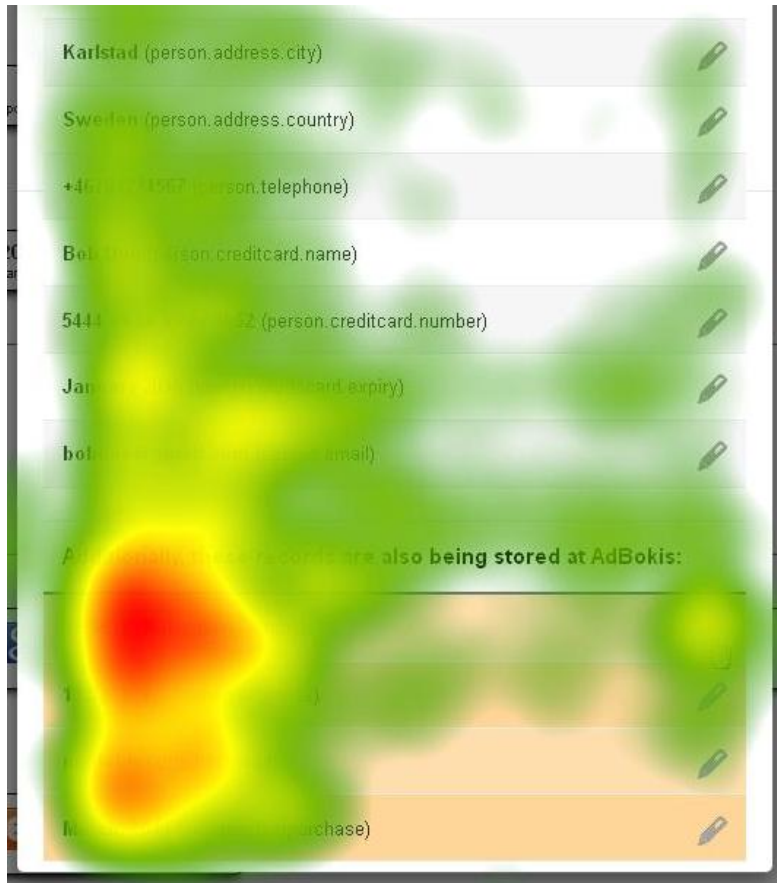




Figure 13: Heat map of participants' average eye gaze on the dialog showing data at the service's side.

access their Data Track entries, for instance, 5 (31%) cases referred to “employees of the Data Track services”, 3 (19%) mentioned “the government”, and 4 said they had no idea (43.8%). Interestingly, 2 participants referred to Google as being able to know the data logged by the Data Track, even when no remarks about the company were made (during the test one of these participants used the Firefox browser and the other used Google Chrome). These results indicate that users are still unsure about the breadth of third party access to their data, and that the interface should convey the notion that privacy-enhancing mechanisms are in place to protect these data.

On the other hand, comments from participants showed that they have a good understanding that their data is being shared with third parties and that, once released, services can do almost whatever they want with their data. This indicates that while users would like to have more control over their data, they lack a clear actionable approach to enforce this control and do something practical about it.

One of the challenges for the design was to find appropriate visual indicators, or standard icons, that users would intuitively recognize as buttons that, when clicked, will display infor-

mation about them that is located at the services' sides and outside their direct control. In the second round of experiments we did a comparative test of two common icons that tried to represent this, a database icon , and a cloud icon . Although not much difference was observed, the results from the eye-tracking analysis showed that the database icon had longer fixation duration mean than the cloud icon (11.08 sec vs. 17.38 sec), was looked at more times (29 vs 39 times in average) and was clicked more than double (1.75 vs 4.40 times in average). This shows the influence that visual elements can have in the users' interaction with the tool, suggesting that the database icon was less intuitive for lay users who required more cognitive effort to understand it. Eye-tracking also revealed that most participants skipped reading many of the texts embedded in the interface, which emphasizes the need for intuitive and easily spotted graphical elements. Regarding the erasure or correction of disclosed data, all participants easily identified what to click to request this manipulation.

More interestingly are the users' expectations on how to remove a data entry from the trace view and what ought to happen internally when this is done. When asked "how would you remove your email address from the Data Track?", 13 participants mentioned that they would right-click or double-click on that data item, where they would get a menu with a *delete* option. Participants also shared their mental models of what would happen when removing a data item, where one participant, for example, commented that "I would like that it will be deleted in all the services that have it, so that I don't have to go in to each [service] to take it away. But of course, I would also like it to have it manually on each, because maybe it's needed. For example, the email in Spotify might be good to have because otherwise they cannot send information on new music..."

When asked about how often do they believe that they would use the Data Track program to control their data and see their data disclosures, 88.2% of the participants indicated that they would use the tool at least a few times per month. However, this proportion might not be realistic and cannot be confirmed until studies are done with users who interact with an actual working product. Worth noting is that one technology-savvy professional commented in a later seminar, that he would use the Data Track a few times per month, mostly to detect discrepancies or things that fall out of the ordinary in the distribution and usage of his data. This comment is useful to understand the users' motivations for using such a transparency tool.

### **4.3. Workshop with individual cloud customers**

A workshop was organized at Karlstad University on April 28, 2014, as part of the collaborative activities between WP:C-7 and WP:B-2, where a total of 19 students and faculty members were different levels of technology-literacy were invited to participate in a three hour workshop.

#### **4.3.1. Participants**

From the 19 participants, seven are from 18 to 23 years old, and 9 from 24 to 30 years, 1 from 31 to 40, and 2 participants were over forty years old.

In the following subsections, we briefly summarise the workshop, demographics of the participants and some of the results. More details about the workshop and the results are published in A4Cloud deliverable D:B-2.3

Figure 14 provides an overview of the level of technology-literacy the participants considered themselves.

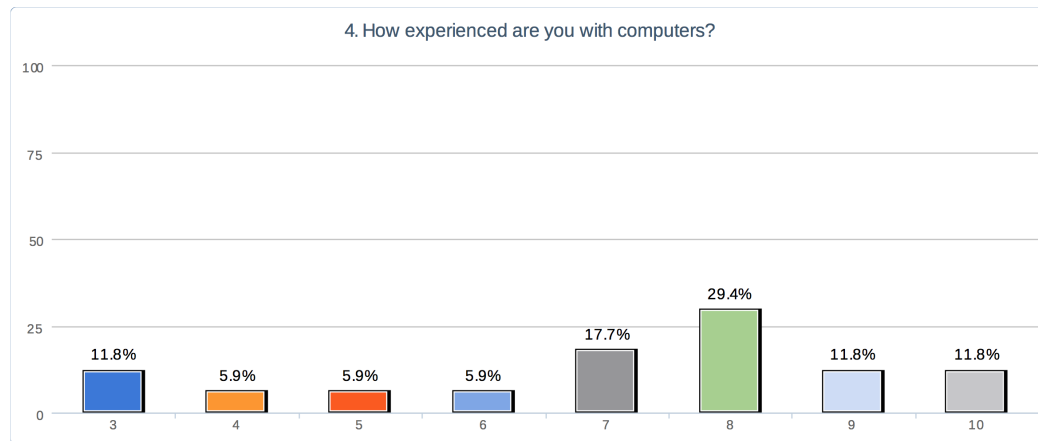


Figure 14: Frequency distribution of participants' technology-literacy

#### 4.3.2. Sessions

The workshop was divided into two sessions. During the initial session participants were introduced to the purpose and user interface of the Data Track tool. First, they were shown an interactive prototype of the initial iterations of the Data Track's trace view, as displayed in Figure 9, and they were also presented with a video explaining an specific use case where this tool can be useful. The moderator then gave the opportunity to ask questions and generate discussions. After the presentation, participants were divided into two main groups with 10 and 9 participants in each group and also a moderator who tried to keep the discussion inline with the topics. During the group discussions the moderator incited discussions based on predefined questions:

- Do you think you will use this tool?
- When do you think you would make use of this tool?
- In which context do you think this tool will be interesting?
- What did you like the most about this tool?
- What did you like the least about this tool?

After the group sessions, participants were asked to answer a questionnaire about different aspects of the Data Track tool. The questionnaire can be found in the Appendix C.1.

After a small break participants were then shown a newer version of the Data Track tool, which emphasize the tool's scalability, allowing it to handle large amounts of personal attributes

at the top and many different service providers at the bottom. Discussions were then created with the whole group of participants about the newer version of the Data Track, where participants were encouraged to express their opinions regarding the usability of its interface, its usefulness, its purpose and promotion of ideas that would fit the concept of visualizing large sets of data disclosures.

After the discussions, participants were then asked to answer a second questionnaire with their individual opinions about the Data Track tool. This allowed participants who felt uncomfortable to express their opinion in front of the whole group to have a say in writing. In the questionnaire a printed illustration of the tool was provided so that participants could draw new ideas, suggestion for improvement or comments. The questionnaire can be seen in Appendix C.2.

Besides, we asked participants about their preferences in regard to security and privacy incidents notifications in order to analyse the users' perceptions of incident reports that the IRT tool, which can be implemented as an extension of the Data Track, will deliver.

Participants were rewarded at the end of the workshop with incentives for their time and contributions, equivalent of two tickets for the movies.

#### **4.3.3. Results**

The following workshop results list some of the findings reported in D:B-2.3:

In regard to the question on how much the participants agreed with the level of usability of the tool, the participants in principle agree that:

1. The tool will probably be used frequently in the future.
2. The tool is not complex.
3. The tool is easy to use.
4. The tool is easy to learn quickly.
5. The tools functionalities are clear and understandable
6. The tool integrates well with current practices.
7. The tool integrates well various functionalities.

However, the participants had different views in regard to some other questions concerning usability:

8. Some believe that the tool requires user training and others thought not. Thus, there was a big variation in the opinions.
9. The participants in general believed on average that the tool does not require users to learn a lot of new concepts, but there was still some variation in the results.



10. The participants indicated to neither agreed nor disagreed with the statement that: the tool lacks many useful functionalities.

In regard to the question on how participants agree that the objectives of A4Cloud are accomplished by the Data Track tool, participants agree that the Data Track tool:

11. gives users more control and transparency over how the data is used in the cloud

In general, participants mostly agreed that the Data Track tool:

12. enables cloud service providers to give their users appropriate control and transparency over how their data is used.
13. enables users to make choices about how cloud service providers may use and will protect data in the cloud.
14. will make the relationship between users and providers substantially more transparent, because it will be easier to see who is liable for the problems.

The participants were neutral or disagreed to that the Data Track tool:

15. will substantially increase users' trust in cloud services.
16. will substantially reduce the number of serious security problems.

In regard to the question on how the participants rated the importance of the listed functional requirements of the tool, all functionalities were rated as important, without much variation on the opinions. Controversial were however requirements 29 and 30, which were not rated by everybody as important. The list of requirements is as follows:

17. The Tool should let me see which of my data was sent by me and which data was collected automatically by the service.
18. The Tool should let me know which data is collected by which services and for what purposes are they going to use my data.
19. The Tool should inform me whether the Cloud service stores my data in an encrypted form or if they can see the contents of my data.
20. The Tool should let me check how my data has been processed by the Cloud service and what conclusions they can draw about me based on this.
21. The Tool should allow me to find out whether my data has been used in a way that was not specified in the privacy policy when I sent my data.



22. The Tool should allow me to see how my data has been passed on to other Cloud services.
23. The Tool should allow me to correct (edit) or to delete the data that the Cloud services have about me.
24. The Tool should let me know the country in which my data is stored and the laws that apply.
25. The tool should inform me when other people send data about me to a Cloud service.
26. The Tool should provide a report that tells me how risky or secure is to have my data in a Cloud service.
27. The Tool should inform me about the risks and threats associated with Cloud services.
28. The Tool should enable assessing the security level of the service providers.
29. When the Cloud service doesnt do what they promised me at the time of registration, the Tool should let me do something about it.
30. The Tool should send me many notifications per week to inform me how the Cloud service is handling my data.

In Appendix C.3, we summarise the aspects that participants rated as positive and those that the participants thought could be further improved.

In regard to the preferences of how frequently participants would like to be notified about different types of incidents, participants expressed that they would prefer to be notified about violations to their private data only if they were able to do something about it. Participants mentioned that obtaining information about something bad that happened without being able to take action, might just cause stress and anxiety, and that they might not even want to know what happened in that case.

Table 1 shows that cloud subjects mainly would like to be notified when hackers obtained their data or when a services side that hosts their data was attacked by a hacker, while they were less interested to be informed about data transfers to other countries or other kind of negative news about the services that host their data. Admittedly, these are average values, and it should be possible for users to set with what priority different kinds of incidents should be reported to them.

I would like this tool to notify me	avg.
when a hacker has obtained my data from the service that has it	4.78
when a service that has my data has been attacked by a hacker	4.53
when a service that has my data has used my data for purposes that I do not agree with (e.g. for sending me advertisements, or for tracking my activities, etc.)	4.21
when my data has been shared with other companies or people	3.63
if a service that has my data was recently mentioned in the news or if a scandal is reported about this service	3.47
when my data has been moved to a different country (which might have different laws to handle my data)	2.89

Table 1: Preferences of frequency of notifications (where 0 = 'Not often' and 5 = 'Very often')

## 5. Concluding Remarks

This deliverable has refined HCI discussions and highlighted UI issues which were raised in previous A4Cloud work. A previous deliverable, D:C-7.1, gave a very comprehensive thematic account of problems and HCI solutions. It listed a huge number of HCI requirements derived from various ways of elicitation. Then functional categories such as “Exercising data subject rights” were mapped to general HCI requirements derived from all the specific requirements collected. In addition, a collection of guidelines with examples from existing services were provided. The present deliverable has only summarized the previous comprehensive and high-level presentation rather than repeated it. The summary of “Preliminary HCI Requirements and Principles” is to be found in chapter 3. The remainder of the present deliverable has highlighted specific UI issues that have been much discussed within the project.

This concluding chapter is divided into one section with additional HCI requirements and principles, and one with suggestions for the future development work on user interfaces in A4Cloud.

### 5.1. Additional HCI Requirements and Principles

#### 5.1.1. HCI Requirements and Principles concluded from the Privacy Icons Evaluation

- If icons are used that distinctly resemble well-known icons from other user interfaces, the wording in each language must match the standard “textual” translation of the icon. The intended message must consequently be conveyed in that word and also be close in meaning to the standard use of the icon + word;
- Contextual framing provided by the tool is important to impose meaning on a symbol;
- Include text (subscripts/legends) to explain icons’ meaning even when the icon is easily recognised as a picture because the specific cloud privacy implication is not well-known to users;
- Icon legends need to be further supported with more comprehensive means for new users;
- The framing parts of an icon should not be relied on for the icon semantics but only used to show that the icon belongs to a certain series of icons;
- There might be other alerts a user wants to have than the ones motivated by an EU directive. Therefore, customer tailored integration of alerts must be considered;
- Make sure that colour used for differentiation is not misinterpreted as evaluation.

In general it is worth to consider the following for icons: icons do not have to make statements but rather only indicate general subject matter, in particular:

- when an icon is only used to open an evaluation in a table or dialog box;
- when an icon has a classifying function (a headline function);

– when alerting the user, a superscript warning triangle can suffice on a classifying icon. For the latter, it was noticed in section 4.2.4 that such a composition of icons can still function as a place to click or hover over when one wants to read more.

Finally, five concepts which pertain in particular to cloud processing, i.e. that services rely on chains of services, was considered in the icon evaluation. This resulted in some further requirements / principles to be considered in addition to the ones above:

1. Location inside/outside EEA: for experimental purposes, consider using icons derived from EU symbols.
2. Jurisdiction: simple law symbol plus standard country abbreviation will do for most users;
3. Responsibility: in any service chain display, signal clearly which actors are accountable to the data subject and for what (if the distinction *controller* vs. *processor* is communicated, make sure users understand the implications);
4. Level of security: when designing security icons for more than *insufficient* vs. *sufficient*, make sure all levels have a reasonable meaning in the situations where the icons will appear;
5. Termination: be aware of the different dimensions of the concepts to be communicated (more than one icon may be needed if icons state conditions rather than only indicate general subject matter).

#### 5.1.2. HCI Requirements and Principles concluded from the Data Track Evaluation

An overall conclusion of the findings reported in chapter 5 is that while users would like to have more control over their data, they lack a clear actionable approach to enforce this control and do something practical about it.

The following list summarises the findings in the most recent usability evaluations of Data Track and the workshop with individual cloud customers (partly overlapping those listed in chapter 3).

- Cloud subject A4Cloud tools should provide transparency not only in regard to data that was explicitly disclosed by the cloud subject but also personal data that was implicitly obtained or derived by the cloud service providers;
- Provide users with help (e.g., via tooltips or introductory tutorials) for understanding how control functions can be activated;
- Choose icons for activating control functions with care and test them (see previous section);
- Prioritise notifications to users of incidents for which remediation and redress actions can be offered;
- Provide users with options to set priority / frequency of each kind of incident notifications.

## 5.2. Pertinent takeaways for the future HCI development work in A4Cloud

As this deliverable is finalised important decisions are to be made within the project, namely to decide whether all tools in the A4Cloud collection should be developed into final running prototypes to be integrated in the A4Cloud solution. The Data Track maintains a key role as pointed out in this deliverable. As a host for plugin versions of several of the other tools, it can host also mockups of tools not implemented but for which the project needs to show at least an indicative user interface.

For the more detailed work that will be pursued in the project's last year, some conclusions from the WP C-7 work should be considered:

- While a UI object such as an icon may work well in A4Cloud prototypes it might not be generally applicable for the same function in other systems. The cloud icon clearly benefited from being tested with introductions about *cloud* computing. 'EEA' might need a similar backing. Naturally, such contextual features should be reported so that what are workable UI solutions are presented with information on the contextual background.
- Wording of icon legends, tooltips, etc. should be given more attention as should also other means of quick introductions about specific A4Cloud topics such as data processors responsibilities, data logs and services side data, comprehension on and actionability of incident notifications.

## References

- [ABFH<sup>+</sup>14] Julio Angulo, Karin Bernsmed, Simone Fischer-Hübner, Christian Frøystad, Erlend Gjære, and Erik Wästlund. D:D-5.1 User Interface Prototypes V1. Project deliverable D:D-5.1, A4Cloud Project, August 2014.
- [ACC<sup>+</sup>05] Christer Andersson, Jan Camenisch, Stephen Crane, Simone Fischer-Hübner, Ronald Leenes, Siani Pearson, John Sören Pettersson, and Dieter Sommer. Trust in prime. In *Signal Processing and Information Technology, 2005. Proceedings of the Fifth IEEE International Symposium on*, pages 552–559. IEEE, 2005.
- [AFHP<sup>+</sup>13] Julio Angulo, Simone Fischer-Hübner, John Sören Pettersson, Erik Wästlund, and Leonardo Martucci. D:C-7.1 General HCI principles and guidelines for accountability and transparency in the cloud. Project deliverable D:C-7.1, A4Cloud Project, September 2013.
- [AFHPW12] Julio Angulo, Simone Fischer-Hübner, Tobias Pulls, and Erik Wästlund. Towards usable privacy policy display & management. *Information Management & Computer Security*, 20(1):4–17, 2012.
- [AKLS13] Alessandro Acquisti, Ioannis Krontiris, Marc Langheinrich, and Martina Angela Sasse. 'My Life, Shared' - Trust and Privacy in the Age of Ubiquitous Experience Sharing (Dagstuhl Seminar 13312). *Dagstuhl Reports*, 3(7):74–107, 2013.
- [Art04] Art. 29 Data Protection Working Party – European Commission. Opinion 10/2004 on More Harmonised Information Provisions , 25.11.2004.
- [Art12] Art. 29 Data Protection Working Party – European Commission. Opinion 5/2012 on Cloud Computing , 1.07.2012.
- [Eur13] European Commission. Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 C7 0025/2012 2012/0011(COD)) Compromise amendments on Articles 1-29. Available at [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/dv/comp\\_am\\_art\\_01-29/comp\\_am\\_art\\_01-29en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf), 21.10.2013.
- [FHAP14] Simone Fischer-Hübner, Julio Angulo, and Tobias Pulls. How can cloud users be supported in deciding on, tracking and controlling how their data are used? In *Privacy and Identity Management for Emerging Services and Technologies*, pages 77–92. Springer, 2014.
- [FHHW11] Simone Fischer-Hübner, Hans Hedbom, and Erik Wästlund. Trust and assurance hci. In *Privacy and Identity Management for Life*, pages 245–260. Springer, 2011.

- [GHW<sup>+</sup>11] Cornelia Graf, Christina Hochleitner, Peter Wolkerstorfer, Julio Angulo, Simone Fischer-Hübner, Erik Wästlund, Marit Hansen, and Leif-Erik Holtz. Towards usable privacy enhancing technologies: Lessons learned from the primelife project. In *PrimeLife Deliverable D4.1.6*. PrimeLife, February 2011.
- [HNH11] L. Holtz, K. Nocun, and M. Hansen. Displaying privacy information with icons. In *PrimeLife/IFIP Summer School Proceedings 2010. Helsingborg, August 2-6, 2010*. Springer, 2011.
- [ISKČ11] Iulia Ion, Niharika Sachdeva, Ponnurangam Kumaraguru, and Srdjan Čapkun. Home is safer than the cloud!: privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, page 13. ACM, 2011.
- [ISO10] ISO. International organization for standardization, iso 9241-210:2010 ergonomics of human-system interaction – part 210: Human-centred design for interactive systems. Directly by the International Organization for Standardization, 2010.
- [Joh14] Jeff Johnson. Designing with the mind in mind, 2014.
- [JRBS10] Adam N Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B Paine Schofield. Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, 25(1):1–24, 2010.
- [JSBG04] Monique WM Jaspers, Thiemo Steen, Cor van den Bos, and Maud Geenen. The think aloud method: a guide to user interface design. *International journal of medical informatics*, 73(11):781–795, 2004.
- [JSP07] Mike Bergmann John Sören Pettersson, Simone Fischer-Hübner. Outlining data track: Privacy-friendly data maintenance for end-users. In *Proceedings of the 15th International Conference on Information Systems Development (ISD 2006)*, pages 215–226. Springer, 2007.
- [LCP06] Hazel Lachée, Stephen Crane, and Andy Phippen. Trustguide: final report. *Trustguide*. October, 2006.
- [MT12] Cathy Marshall and John C Tang. That syncing feeling: early user experiences with the cloud. In *Proceedings of the Designing Interactive Systems Conference*, pages 544–553. ACM, 2012.
- [Nie95] Jakob Nielsen. Usability inspection methods, 1995.
- [Nie99] Jakob Nielsen. Tooltips on webpages, August 10 1999. US Patent 5,937,417.
- [Nie14] Jakob Nielsen. Icon classification: Resemblance, reference, and arbitrary icons, 2014.

- [O'n02] Onora O'Neill. *A question of trust: The BBC Reith Lectures 2002*. Cambridge University Press, 2002.
- [Par13] European Parliament. Compromise amendments on articles 1-29. comp article 1., 2013.
- [Par14] European Parliament. European parliament legislative resolution of 12 march 2014 on the proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(general data protection regulation)(com(2012)0011), 2014.
- [Pea13] Siani Pearson. Privacy, security and trust in cloud computing. In *Privacy and Security for Cloud Computing*, pages 3–42. Springer, 2013.
- [Pet14] John Sören Pettersson. A brief evaluation of icons suggested for use in standardised information policies. a brief evaluation of icons suggested for use in standardised information policies: Referring to the annex in the first reading of the european parliament on com (2012) 0011, 2014.
- [PFHB07] John Sören Pettersson, Simone Fischer-Hübner, and Mike Bergmann. Outlining “Data Track”: Privacy-friendly data maintenance for end-users. In *Advances in Information Systems Development*, pages 215–226. Springer, 2007.
- [PFHD<sup>+</sup>05] John Sören Pettersson, Simone Fischer-Hübner, Ninni Danielsson, Jenny Nilsson, Mike Bergmann, Sebastian Clauss, Thomas Krieglstein, and Henry Krasemann. Making prime usable. In *Proceedings of the 2005 symposium on Usable privacy and security*, pages 53–64. ACM, 2005.
- [PK03] Andrew S. Patrick and Steve Kenny. From privacy legislation to interface design: Implementing information privacy in human-computer interactions, 2003.
- [Pri10] PrimeLifeWP4.3.2. Ui prototypes: Policy administration and presentation - version 2. In *PrimeLife Deliverable D4.3.2*, 2010.
- [PTC<sup>+</sup>12] Siani Pearson, Vasilis Tountopoulos, Daniele Catteddu, Mario Südholt, Refik Molva, Christoph Reich, Simone Fischer-Hübner, Christopher Millard, Volkmar Lotz, Martin Gilje Jaatun, et al. Accountability for cloud and other future internet services. In *CloudCom*, pages 629–632, 2012.
- [Ras10] A. Raskin. Privacy icons making your online privacy rights understandable. <http://www.drumbeat.org/project/privacy\icons>, 2010.
- [Rus80] James A Russell. A circumplex model of affect. *Journal of personality and social psychology*, 39(6):1161, 1980.
- [Shi13] Dong-Hee Shin. User centric cloud service model in public sectors: policy implications of cloud services. *Government Information Quarterly*, 30(2):194–203, 2013.



- [The13] The European Consumer Centres Network. Trust marks report 2013: “Can I trust the trust mark?”, 2013.
- [TKD<sup>+</sup>09] Janice Y Tsai, Patrick Kelley, Paul Drielsma, Lorrie Faith Cranor, Jason Hong, and Norman Sadeh. Who’s viewed you?: the impact of feedback in a mobile location-sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2003–2012. ACM, 2009.
- [VOO13] Amy Volda, Judith S Olson, and Gary M Olson. Turbulence in the clouds: challenges of cloud-based information work. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2273–2282. ACM, 2013.
- [WAFH11] Erik Wästlund, Julio Angulo, and Simone Fischer-Hübner. Evoking comprehensive mental models of anonymous credentials. In Jan Camenisch and Dogan Kesdogan, editors, *iNetSeC*, volume 7039 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 2011.
- [Wam10] Caroline Wamala. Does it count?: complexities between access to and use of information technologies among uganda’s farmers. *Sort*, 20(50):100, 2010.

## A. Icon questionnaires

### A.1. First Icon Questionnaire (EU Parliament Icons)

*The following five pages show with translations to English the 4-page questionnaire used in a class where 21 people responded. 2014-03-24*

#### INTRODUCTION TO QUESTIONNAIRE ABOUT WEB ICONS FOR PERSONAL DATA PROCESSING

When shopping online, signing up for a service, contacting authorities, associations and businesses via the Web or through apps on the phone and in tablet, these sites are required by the Personal Data Act to explain what they are going to have one's personal data to. The Swedish law follows the EU directives.

It's not always easy to find that information. And even if it is easy to find information about the sites' personal data processing, the information text can be lengthy with many qualifications.

It has been suggested that users would be able to get short summaries, perhaps in the form of icons, which show the main features of the site's handling of personal information. If one uses the icons they should be simple images that say something about the processing of personal data.

This survey contains a few icons that came with a recent EU proposal for an EU directive on personal data processing. On the following pages, we ask you to comment the icons and texts to the icons.

**Please, do not turn page until you have been requested to do so!**

#### INTRODUKTION TILL ENKÄT OM WEBB-IKONER OM PERSONDATAHANTERING

När man handlar på nätet, registrerar sig för någon tjänst, kontaktar myndigheter, föreningar och företag via webben eller via appar i telefon och surfplatta, så är dessa sajter skyldiga enligt Personuppgiftslagen att förklara vad de ska ha ens persondata till. Den svenska lagen följer direktiv från EU.

Det är inte alltid så lätt att hitta den information. Och även om det är enkelt att hitta information om sajternas personuppgiftshantering, så kan informationstexten vara långgrandig med många förbehåll.

Det har föreslagits att man som användare skulle kunna få korta sammanfattningar, kanske i form av ikoner, som visar huvuddragen i sajtens hantering av personuppgifter. Om man använder ikoner så bör de vara enkla bilder som säger något om hanteringen av personuppgifter.

Den här enkäten innehåller några ikoner som kom med senaste EU-förslaget till EU-direktiv om personuppgiftshantering. På de följande sidorna ber vi dig att kommentera ikonerna och texter till ikonerna.







**Vänligen, vänd ej blad förrän du blir ombedd att gå vidare!**

### D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

---

1. Describe what you think the icons below are about. You can write one single word or 1-2 sentences.

1. Beskriv vad du tycker att ikonerna nedan handlar om. Du kan skriva ett enda ord eller 1-2 meningar.

Please, do not turn page until you have been requested to do so!  
Vänligen, vänd ej blad förrän du blir ombedd att gå vidare!

## D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

---

2. Try to match the texts on the right-hand side to the icons to the left side. Draw a line between icon and text.

If you think several icons match a text or that one icon would fit several of the texts, you just marked that.

*[The matching texts were given both in their original English wording and in Swedish translation.*

*As show on the next page, English texts were in green while the Swedish texts were printed in blue.*

*The instruction (in Swedish) appeared in the original questionnaire on the same page as the icons and texts.]*

2. Försök matcha texterna till höger mot ikonerna till vänster. Drag streck mellan ikon och text.

Om du tycker att flera ikoner matchar en text eller att en ikon passar till flera av texterna, så markerar du det.

### D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

---



No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing

Inga personuppgifter **samlas in** utöver de som är nödvändiga för varje specifikt syfte med databehandlingen

No personal data are **disseminated** to commercial third parties

Inga personuppgifter **sprids** till kommersiella tredjeparter

No personal data are **processed** for purposes other than the purposes for which they were collected

Inga personuppgifter **behandlas** för andra syften än för vilka de samlades in

No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing

Inga personuppgifter **bevaras** utom de som är nödvändiga för varje specifikt syfte

No personal data are **sold or rented out**

Inga personuppgifter **säljs eller hyrs ut**



No personal data are retained in **unencrypted** form

Inga personuppgifter sparas i **okrypterad** form

**Please, do not turn page  
until you have been requested to do so!**

### D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

3. When you are about to enter some personal data at a site, you notice the row below. What do you think the site is trying to say?



	No personal data are processed for purposes other than the purposes for which they were collected	
---	---	---

---

---

---

3. När du ska lämna några personuppgifter på en sajt, så får du se nedanstående rad. Vad tror du sajten försöker säga med den?

	Inga personuppgifter <b>behandlas</b> för andra syften än för vilka de samlades in	
---	--	---

---

---

---

## A.2. Second Icon Questionnaire (Designers' Icons)

*This questionnaire (in Swedish) was handed out to a class of c:a 50 students in August 2014.*

*The structure follows to some extent the structure of the first questionnaire. The three questions are in this questionnaire numbered "D1" – "D3" as it is the Designers' icons that are shown.*

### INTRODUKTION TILL ENKÄT OM WEBB-IKONER OM HANTERING AV PERSONDATA

När man handlar på nätet, registrerar sig för någon tjänst, kontaktar myndigheter, föreningar och företag via webben eller via appar i telefon och surfplatta, så är dessa skyldiga enligt Personuppgiftslagen att förklara vad de ska ha ens persondata till. Den svenska lagen följer direktiv från EU.

Det är inte alltid så lätt att hitta sådan information. Och även om det är enkelt att hitta information om sajternas personuppgiftshantering, så kan informationstexten vara långgrandig med många förbehåll.

Det har föreslagits att man som användare skulle kunna få korta sammanfattningar, kanske i form av ikoner, som visar huvuddragen i sajtens hantering av personuppgifter. Om man använder ikoner så bör de vara enkla bilder som säger något om hanteringen av personuppgifter.

Vidare skulle man kunna kontrollera vilka data man släppt ifrån sig, och det forskas om olika sådana verktyg för både vanliga medborgare och företag som använder molntjänster för att kunna leverera sina egna tjänster.

Den här enkäten innehåller några ikoner som skulle kunna användas på webbsidor som frågar efter persondata eller i program som du i framtiden använder för att kolla upp sajter som har fått personuppgifter antingen direkt från dig eller från andra internetjänster som du har använt. I enkäten ombeds du kommentera ikonerna som visas.

**Vänligen, vänd ej blad förrän du blir ombedd att gå vidare!**

## D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

D1. Beskriv vad du tycker att ikonerna nedan handlar om. Du kan skriva ett enda ord eller 1-2 meningar.

 <b>LOW SECURITY</b>	 <b>MEDIUM SECURITY</b>	 <b>HIGH SECURITY</b>	
 <b>RESPONSIBLE DATA CONTROLLER</b>			
 <b>NO RESPONSIBILITY FOR DATA</b>			
 <b>SERVICE CONTRACT TERMINATION: DELETE</b>	 <b>SERVICE CONTRACT TERMINATION: ARCHIVE</b>		
 <b>SERVICE CONTRACT TERMINATION: EXPORT</b>			
 <b>JURISDICTIONS</b>			

Vänligen, vänd ej blad förrän du blir ombedd att gå vidare!



## D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

D2. I framtiden, när allt fler internetjänster är sammankopplade (ibland talar man om "molnet"), så kanske det finns program som gör att du kan spåra vilka underleverantörer dina e-tjänsteleverantörer använder sig av i molnet.

Om du undrar över hur dina data har använts, kan det vara bra om du i ett "spårningsprogram" snabbt ser vilka molntjänster som:




1. är ansvariga för den information de har om dig,
2. inte har detta ansvar eftersom de bara utför tjänster på uppdrag av de personuppgiftsansvariga företagen.

Vi har två symboler för dessa två typer av databehandlare i molnet.



Om du fick välja att färglägga dessa båda symboler, vilken/vilka färger skulle du välja då?

Ringa in en av färgerna i varje kolumn!  
(Du kan välja grå.)

 RESPONSIBLE DATA CONTROLLER	 NO RESPONSIBILITY FOR DATA
	
	
	
	
	
	
	
	

Vänligen, vänd ej blad  
förrän du blir ombedd att gå vidare!

## D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

D3. Det finns en del stater utanför EU som också följer EUs regler. De ingår tillsammans med EU i EEA  
– The European Economic Area (EU + Island, Lichtenstein och Norge).

Vilken ikon du skulle föredra att man använder för att visa att databehandling sker inom EEA?

Icon	Please, indicate which icon you would prefer You can also add a comment on why.
	
	
	

## B. Usability evaluations material - Tasks and questions

- What do you think the elements on the top represent?
  - All of my own information
  - My own information that I have sent to online services
  - Other people's information
  - I have no idea
  - Other
- What do you think the elements at the bottom represent?
  - Services on the Internet in general
  - Services on the Internet that have collected information about me
  - Services on the Internet that I have send information to
  - Other
- Using the Data Track's traceview, how can you see the information that you have sent to *AdBokis.com*?
  - Success (clicked on the AdBokis.com service on the bottom panel)
  - Partial success (succeeded after 45 seconds)
  - Failed
- How can you see to which Internet services you have given your email address?
  - Success (click on the email address on the top panel)
  - Partial success (succeeded after 45 seconds)
  - Failed
- Where would you click to see the information that AdBokis.com has stored on their servers when you purchased the book?
  - Success (clicks on the "server" icon on the AdBokis.com service on the bottom panel)
  - Partial success (succeeded after 45 seconds)
  - Failed (if failed, moderator should show correct way)
- In your opinion, who can access your data that AdBokis.com has stored on their servers?
  - Only me and AdBokis.com
  - The Data Track employees and AdBokis.com
  - Other services shown by the Data Track (including AdBokis.com)
  - Everybody using the Data Track program (including AdBokis.com)

- Everybody on the Internet
  - Other
- What information about you does AdBokis.com have on their servers?
  - Success (correct information given)
  - Partial success (succeeded after 45 seconds or partial information given)
  - Almost failure (very incomplete idea, or mentions the information sent by participant, but not information in AdBokis.com)
  - Failed
- Did AdBokis.com store the location you were at when you bought the book?
  - Success (Answers yes)
  - Partial success (Answers yes because I gave it to them)
  - Failed (Answers no or "i don't know")
- Is the information that AdBokis.com have about you more or less than what you gave to them? Why do you think this is?
  - Success (Answers more, because they can store more information or collect more when I make a transaction)
  - Partial success (Answers more, but is not sure why)
  - Partial failure (Answers less and gives a reasonable explanation for it)
  - Failed (Answers "less" but it is not sure why)
- The Data Track gives you an overview of the information you have given to different Internet services. Where do you think the records shown in the top panel of the Data Track are stored?
  - On the Data Track program (on a cloud/Internet storage)
  - On the Data Track program (locally in computer)
  - On the Internet somewhere (not mention Data Track)
  - On the services that I have given information to
  - I have no idea
  - Other
- In your opinion, who has access to the records being shown in the top panel of the Data Track?
  - No one else, only me
  - The Data Track employees
  - Everybody with a Data Track 'account' or program

- Everybody on the Internet
  - The government
  - I have no idea
- What would you do to request to delete or correct the information that AdBokis.com has stored on their servers?
  - Success (goes to the services side and deletes the attributes or disclosures)
  - Partial success (goes to the services' side, but is not sure what to do )
  - Failed (if failed, moderator should show correct way)
- How would you remove a piece of information from the Data Track?
  - Clicks on a piece of information and drags to trashcan
  - Right-clicks or double clicks somewhere
  - Goes to the settings
  - Tries other things and can't remove
- What view shows the Data Track records stored on your system and what view allows you to check what data a services side has stored about you?
  - Success (Indicates that the information on the top panel are stored on the system and that the information that appears in the dialog is remotely located)
  - Partial success
  - Failed

## C. Workshop with individual cloud customers

### C.1. Questionnaire - Part 1

TP#: \_\_\_\_\_

#### Stakeholder Workshop: Cloud Actor Feedback for Data Track

**Instructions:** For each of the following statements, mark one box that best describes your reactions to the accountability tools demonstrated *today*.

The tool:	Strongly Disagree	Disagree	Neither	Agree	Strongly Agree
1. The tool will probably be used frequently in the future.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. The tool is unnecessarily complex.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. The tool is easy to use.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. The tool requires user training.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. The tool integrates well various functionalities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. The tool is easy to learn quickly.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. The tool requires users to learn a lot of new concepts.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. The tool's functionalities are clear and understandable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9. The tool integrates well with current practices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10. The tool lacks many useful functionalities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The usage of this tool will:	Strongly Disagree	Disagree	Neither	Agree	Strongly Agree
11. enable cloud service providers to give their users appropriate control and transparency over how their data is used.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12. enable users to make choices about how cloud service providers may use and will protect data in the cloud.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13. substantially increase users trust in cloud services.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14. give users more control and transparency over how the data is used in the cloud	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15. will substantially reduce the number of serious security problems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16. will make it substantially easier the relationship between users and providers because it will be easier to see who is responsible for the problems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Data Track Functional Requirements

**Instructions:** For each of the following statements, please rate the importance of each functionality the tool should provide.

	Not important 0	1	2	3	4	Very important 5
17. The Tool should let me see which of my data was sent by me (for example, my email address, my credit card number, etc.) and which data was collected automatically by the service (for example, my location, my IP address, the device I'm using, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18. The Tool should let me know which data is collected by which services and for what purposes are they going to use my data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19. The Tool should inform me whether the Cloud service stores my data in an encrypted form or if they can see the contents of my data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20. The Tool should let me check how my data has been processed by the Cloud service and what conclusions they can draw about me based on this processing of my data (e.g., whether I fall within their profile of a "reliable" or "risky" or "not trusted" customer)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21. The Tool should allow me to find out whether my data has been used in a way that was not specified in the privacy policy when I sent my data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22. The Tool should allow me to see how my data has been passed on to other Cloud services.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23. The Tool should allow me to correct (edit) or to delete the data that the Cloud services have about me.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
24. The Tool should let me know the country in which my data is stored and the laws that apply in that country.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
25. The tool should inform me when other people send data about me to a Cloud service.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
26. The Tool should provide a report that tells me how risky or secure it is to have my data in a Cloud service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27. The Tool should inform me about the risks and threats associated with each Cloud services.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
28. The Tool should enable assessing the security level of the service providers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
29. When the Cloud service doesn't do what they promised me at the time of registration, the Tool should let me do something about it, like complain or get compensation from the Cloud service.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
30. The Tool should send me many notifications per week to inform me how each Cloud service is handling my data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## **C.2. Questionnaire - Part 2**

### **Data Track Functional Requirements**

Please provide any comments (extra requirements, improvements, suggestions, recommendations, justification of your answers ) about this tool.

If you would be ok to be contacted for extra clarification please provide:

Name:

Email:



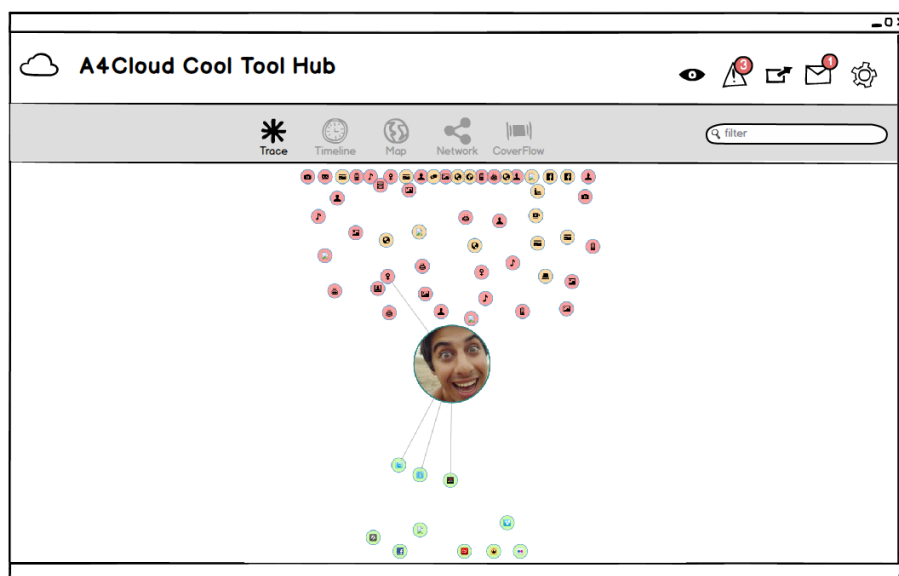
TP#: \_\_\_\_\_

### Data Track – Next version

Mention at least two things that are good about this new interface in your opinion:

Mention at least two things that can be improved in your opinion:

Feel free to draw notes on the figure to illustrate your suggestions and opinions



### Data Track - Notifications

**Instructions:** For each of the following statements, please rate how often you would like to be notified about the following

	Not often <b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	Very often <b>5</b>
31. I would like this tool to notify me when my data has been shared with other companies or people	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
32. I would like this tool to tell me when a hacker has obtain my data from the service that has it	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
33. I would like this tool to notify me when my data has been moved to a different country (which might have different laws to handle my data)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
34. I would like this tool to notify me when a service that has my data has used my data for purposes that I do not agree with (e.g. for sending me advertisement, or for tracking my activities, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
35. I would like this tool to notify me when a service that has my data has been attacked by a hacker	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
36. I would like this tool to let me know if a service that has my data was recently mentioned in the news or if a scandal is reported about this service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

---

### C.3. Feedback by Workshop participants

TP	Positive thing	Improvement
TP01	Moving icons; More User friendly; Easier to visualize in the way of future web interfaces	Show most important information bigger; Categories of data are missing; Possibility to select what's important for you; Use colours to group by topic
TP02	More friendly than the other one; Modern; Graph shown more clearly	The black icons representing the data are too many and small. They are also repeated and that's confusing and increases the searching-for-an-icon time. Instead the searching box would be used and the functionality of the icons would decrease; What's the difference of colours in the circles?
TP03	It looks nice and inviting but I think that the function is more important than how it looks so I liked the first one better; I think this kind of service should be and look serious and like a new game.	Make it look serious; Make it possible to choose what kind of information of the data you have sent that you want to be able to see.
TP04	It keep me informed; It holds the big company in line	It should give me time to react
TP05	The interface is attractive and looks clean	I reckon it will be a lot of information if you have a lot of disclosures, maybe a filter would fix this
TP06	Looks more tidy; Easy to find out what I'm looking for	Categorize the service. Make social networks into one category, make entertainment into another category. Show the time and date when I left my data in the website
TP07	Enjoyable; Easy to understand	Sub-icon for certain icons (e.g. Photos can be various, like party, work, etc.) could have sound when people click the icon.
TP08	Design of the tool; Icons that leads to more space and enables to have for info on one page	What to do if too much icons?; Focus on websites that are the most use everyday
TP09	- Easy to see everything; Easy to reach what you want	Order; Save
TP10	- The presentation (design) is not huge like on the first prototype; The dynamic collection by clicking a service is nice in placing the important data into the middle of the screen.	Search engine is mandatory; Preventive mechanisms should be taken; Putting more focus on the activated information; Separate links from all other icons, gray out the others and make space in between

### D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability

TP	Positive thing	Improvement
TP11	The structure and categorisation; More clear	Emphasise the most sensitive or important data; Highlight the most used data.
TP12	More playful; Easier	To make it more easy to work with, by making "main-group", it is too much information at the moment, I would like the program to find information that I find important
TP13	It makes you more aware what information you put on the Internet, you will probably be more careful; It's good to find out where your data will go and if it has connections to other links on the Internet	It should not be so many icons and be easier to use; You should be able to personalize your account so you don't have to look through everything to find out the exact data that you want to find out.
TP14	The structure seems easier to work with when there are more files; There are more tools, like notifications, settings, etc.	The categorization of the files; The importance of notifications
TP15	It is more comprehensible for me to understand the different links without being too confused by other things around; As you said, its playful, so if people take their time they can easily understand and track their data streams and inform themselves better; However, so far it is only tracking, so a reactive device which means it will probably be time consuming for me as a user to check/track down all my movements and to decide what to do.	Classification of importance of data (within sub-categories) and based on that notifications on what happens to the important things; Too much information is at worse as no information; In my opinion, it still shouldn't be too playful, as in the end this is a serious topic, and its not about playing around, but more about serious help to secure myself.
TP16	Simple; Easy to use; Good to have a search bar	Customization like icon selection, interface, pop-ups, folders, information about consequences
TP17	Easy to get a good overview of where is my data; Possibility to evaluate different websites and what they store and why	Categorize information in order to reduce the number of icons; Filters to only show certain icons
TP18	Information divided into categories; Easier to see the information with the icons	Put a search toolbar; could be faster to find a type of information; Define the number of icons that you want to show. Lot of icons could be a mess; Avoid repeating icons; It is important to improve how to interact with the tool ("edit, remove information, etc."). You will most likely just check the tool once, and then close or uninstall the tool.
TP19	The tool is going to give the possibility of removing some data I gave to some services; I can see the connection between different services in regard to my data	To have less icons; To categorize the information I am sensitive about; The same with services. To select the ones I use or care more about the info they have.