

## D:D-5.4 User Interface Prototypes V2

**Deliverable Number:** D45.4

**Work Package:** WP 45

**Version:** Final Version

**Deliverable Lead Organisation:** Karlstad University (KAU) and SINTEF

**Dissemination Level:** PU

**Contractual Date of Delivery (release):** 30/09/2015

**Date of Delivery:** 30/09/2015

### Editor

Karin Bernsmed (SINTEF), Simone Fischer-Hübner (KAU)

### Contributors

Henrik Andersson (KAU), Julio Angulo (KAU), Karin Bernsmed (SINTEF), Simone Fischer-Hübner (KAU), Christian Frøystad (SINTEF), Erlend Andreas Gjære (SINTEF), Farzaneh Karegar (KAU), Daniel Lindegren (KAU), John Sören Pettersson (KAU)

### Reviewers

Massimo Felici (HP Labs), Carmen Fernandez Gago (UMA)

## Executive Summary

This deliverable “User Interface Prototypes V2” presents the results from user centered analyses, designs and evaluations of the A4Cloud tools. Our main objective has been to develop usable user interface (UI) prototypes for various combinations of tools assembled to address stakeholder specific needs by following user-centered design processes. In this deliverable we present subsequent iterations of the user interface prototype developments and tests for A4Cloud tools and stakeholder-specific toolsets that to a large extent build directly on the initial prototypes presented in our previous deliverable “User Interface Prototypes V1” [2]. Our main focus has been on the discussions of the UI designs and evaluations of UIs for the following A4Cloud tools and toolsets for different A4Cloud stakeholders:

- A toolset for cloud subjects in the form of the privacy dashboard *GenomSynlig*, which comprises the *Data Track (DT)* and *Remediation and Redress Tool (RRT)*;
- Tools for Cloud customers including the *Data Protection Impact Assessment Tool (DPIAT)* and the *Cloud Offering Advisory Tool (COAT)*;
- Tools for Cloud providers and auditors including the *Accountability Lab (AccLab)*, the *Audit Agent System (AAS)* as well the *Incident Management Tool (IMT)*.

To facilitate a consistent look and feel of the A4Cloud tools and toolsets, we have provided a bootstrap template and a conceptual analysis of the terminology that is being applied in the existing versions of the UI prototypes and mock-ups.

As A4Cloud tools for the different stakeholders require different interaction paradigms targeting stakeholders with different levels of expertise, different user-centered evaluation methodologies and types of test participants were used for the different stakeholder-specific tools and toolsets.

For the Data Track functions of the cloud consumer toolset *GenomSynlig*, which allows cloud subject to track their data disclosures and exercise their data subject rights, we have suggested two main designs for the visualizations of personal data disclosures called trace view and timeline view. The evaluations of *GenomSynlig* with lay test users revealed that they appreciate the transparency properties offered by *GenomSynlig* with a preference for the trace view visualization over the timeline. The test users understood the purpose of the tool very well and mostly managed to track their data disclosures well. Nonetheless, the way how users can access their data on the services' side for exercising their rights was still unclear for many test persons. This deliverable therefore also suggests alternatives for future improvements of the user interface of *GenomSynlig* which can allow users to exercise control over the data that they have disclosed in a more intuitive way.

For the evaluation of the cloud customer tools *DPIAT* and *COAT* heuristic expert evaluations were conducted. They showed that while the tools and their interfaces are already rather mature, some of the wordings and use of UI concepts could be improved to make the UIs even more intuitive and to avoid any misunderstandings especially by lay individual cloud customers.

Cloud provider specific tools were evaluated mainly by expert evaluations, heuristic evaluations and focus interviews with security experts and system administrators. The final tests of

the AAS UIs, which were tested and improved in three iterations, showed that while some of the tasks were still difficult to perform at the start, the expert test users then quickly learned how to use of the tool. Therefore, we still recommend to add tooltips and other support functionalities to make the use of the tools more easily understood for first time use.

For UI of *AccLab*, which was improved by the tool developers in several iterations in discussion with us, we still recommend to implement a wizard to guide the user through the policy creation process. Furthermore, based on the evaluation of early UI prototypes of *IMT*, we came up with a few recommended improvements that are presented in this deliverable. In particular, the difference between local incidents and incidents that have been derived and received from 3rd party providers should be made more clear by the user interface.

In addition to the discussions of UI designs and usability evaluations, we provide a number of scenarios that can be used in future evaluation workshops where the tools are used by specific stakeholders groups in the context of the “wearable use case” (the A4Cloud demonstrator).

## Contents

<b>1. Introduction</b>	<b>10</b>
1.1. Deliverable aims and scope . . . . .	10
1.2. User-Centered Methodologies . . . . .	11
1.3. Structure of this deliverable . . . . .	13
<b>2. Background</b>	<b>14</b>
2.1. The A4Cloud accountability model . . . . .	14
2.2. The A4Cloud toolset . . . . .	14
2.3. The A4Cloud demonstrator . . . . .	16
<b>3. Foundations</b>	<b>18</b>
3.1. Consistent conceptual designs . . . . .	18
3.2. Bootstrap UI template for A4Cloud tools . . . . .	20
<b>4. User Interface development for cloud subject tools and tool set</b>	<b>22</b>
4.1. GenomSynlig – A dashboard for end-user transparency . . . . .	22
4.2. Interplay of GenomSynlig with Cloud Provider-specific A4Cloud Tools . . . . .	23
4.2.1. Data Track – Data disclosure visualizations . . . . .	23
4.2.2. PAPV – Plugin for Assessment of Policy Violations . . . . .	33
4.2.3. RRT – Remediation & Redress Tool . . . . .	34
4.3. User evaluations . . . . .	37
4.3.1. Purpose . . . . .	37
4.3.2. Research questions . . . . .	38
4.3.3. Method . . . . .	39
4.3.4. Results . . . . .	43
4.3.5. Results from post-questionnaire . . . . .	48
4.3.6. Findings and suggestions for UI improvements . . . . .	49
<b>5. User Interface Development for Cloud Customer Tools</b>	<b>55</b>
5.1. Data Protection Impact Assessment Tool (DPIAT) . . . . .	55
5.2. Cloud Offers Advisory Tool . . . . .	59
<b>6. User Interface Development for Cloud Provider Tools</b>	<b>63</b>
6.1. Audit Agent System (AAS) . . . . .	63
6.2. Accountability Lab (AccLab) . . . . .	69
6.3. Incident Management Tool (IMT) . . . . .	74
<b>7. Suggestion for Scenarios in Workshop Evaluations of the A4Cloud Demonstrator</b>	<b>83</b>
7.1. Short description of the A4Cloud Demonstrator . . . . .	83
7.2. Targeted scenarios for hands-on demos . . . . .	84
7.3. Scenario 1. Cloud Customers' business and security experts (E) . . . . .	85
7.4. Scenario 2. Individuals (I) . . . . .	86
7.5. Scenario 3. Cloud Providers (P) . . . . .	86



7.6. Scenario 4. Auditors and Supervisory Authorities (A) . . . . .	88
<b>8. Conclusions</b>	<b>89</b>
<b>Appendices</b>	<b>94</b>
<b>A. Appendix</b>	<b>94</b>
A.1. Concepts in prototypes: A table for comparison of UI contents . . . . .	94
A.2. GenomSynlig usability study: Tasks and Questions . . . . .	102
A.3. GenomSynlig usability study: Procedure . . . . .	106

## List of Figures

1.	The A4Cloud toolset . . . . .	15
2.	The Wearable use case . . . . .	17
3.	The suggested A4Cloud tool UI template. . . . .	21
4.	GenomSynlig landing page (as of August 2015) . . . . .	22
5.	The interplay of GenomSynlig with other A4Cloud Tools at the Cloud Provider Side	24
6.	The user interface of PrimeLife's Data Track. . . . .	25
7.	The user interface of the trace view visualization in GenomSynlig (Section 4.2.1), part of the A4Cloud project. . . . .	26
8.	Box showing details about the selected online service provider. The cloud button opens a modal dialog (Figure 14) that shows data on the services' side. . . . .	27
9.	Selecting many service providers can give users an idea of the magnitude of their data disclosures. . . . .	28
10.	Users can see the attributes in common that have been sent to different online services. . . . .	29
11.	The timeline view of the GenomSynlig program, showing each disclosure event in chronological order. . . . .	30
12.	A disclosure event with a time stamp, showing four personal data attributes . . .	31
13.	Sketch showing the responsive properties of the timeline view. . . . .	31
14.	The modal dialog showing the explicitly sent and derived data stored at the ser- vice's side . . . . .	32
15.	Some filtering and searching controls . . . . .	33
16.	When the RRT is triggered by the IRT, users can review and complete the reme- diations request. . . . .	36
17.	Fictitious bookstore, AdBokis.com . . . . .	40
18.	Information that is requested from participants to complete the purchase with AdBokis.com . . . . .	41
19.	Participants answers to the tasks: " <i>Rate how much you agree or disagree with each of the following statements concerning the Synlig program</i> " . . . . .	48
20.	Conveying to the user that newly imported data is stored securely in their device and under their control. . . . .	50
21.	Suggested dialogs for importing external data disclosures into GenomSynlig. . .	51
	(a). Login with user credentials. . . . .	51
	(b). Uploading a data archive. . . . .	51
22.	A redesign proposal of GenomSynlig in which users have the choice from the start to access data stored locally or control their data stored in a remote service. .	52
23.	Connecting services to GenomSynlig – suggestions for the synchronization status. .	53
24.	Font-Awesome icons which participants pointed out as unclear in the context of data disclosures. Taken from [23] . . . . .	54
25.	The starting point when using DPIAT. The user selects pre-screening or screen- ing questions . . . . .	55
26.	The user must answer questions about the service . . . . .	57

27. Upon completing the questionnaire, the user is presented with a report of the risks associated with his answers . . . . .	58
28. The user is asked to select services categorised by deployment type . . . . .	59
29. The user can view offers and add further requirements . . . . .	60
30. The user can view details of the offer . . . . .	61
31. An example of the initial sketched of the UI for AAS. . . . .	63
32. Screenshot of the original AAS UI used for the mockups in the first test session	64
33. Screenshot from one of the mockups used in the final test iteration . . . . .	65
34. The interface of AccLab as implemented . . . . .	69
35. Mockup demonstrating how to clean up the interface . . . . .	70
36. Updated UI for AccLab by students at Mines-Nantes . . . . .	70
37. The Web Application Menu for AccLab by students at Mines-Nantes . . . . .	71
38. Color options in AccLab . . . . .	72
39. Edit actions in AccLab. Move and Zoom buttons highlighted with red circles . . .	72
40. An example from the ArchiMate® 2.1 specification on how to label actors graphically – here, a location is displayed . . . . .	73
41. An example of the correct actor being highlighted in the editor when hovered or active in the outline . . . . .	73
42. List of Incidents . . . . .	75
43. Add Incident . . . . .	76
44. Incident Details . . . . .	77
45. Incident Notification Status Indicator . . . . .	78
(a). Incident notification not sent . . . . .	78
(b). Incident notification sent . . . . .	78
46. Incidents Type Details . . . . .	79
47. Subscription Details . . . . .	80

## List of Tables

1.	Design and evaluation methodologies used for the different A4Cloud tools and tool-sets . . . . .	11
2.	Participant overview, GenomSynlig evaluation (n=13) . . . . .	42
3.	Participants and the order and sequence of their respective test sessions. . . .	68

### List of Abbreviations

AAL	Abstract Accountability Language
AAS	Audit Agent System
AccLab	Accountability Lab
A-PPL	Accountability - PrimeLife Policy Language
CC	Cloud Customer
CB	Cloud Broker
COAT	Cloud Offering Advisory Tool
CP	Cloud Provider
CSP	Cloud Service 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
GUI	Graphical User Interface
HCI	Human Computer Interaction
IMT	Incident Management Tool
PAPV	Plug-In for Assessment of Policy Violations
PETs	Privacy Enhancing Technologies
PLAT	Privacy Level Agreement Tool
PO	Privacy Officer
RRT	Remediation and Redress Tool
SME	Small and Medium-sized Enterprise
TETs	Transparency-Enhancing Technologies
TL	Transparency Log
UCD	User Centred Design
UI	User Interface
UML	Unified Modelling Language

## 1. Introduction

The A4Cloud project deals with accountability for the cloud and other future Internet services. The project 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 chains can be made accountable for the privacy and confidentiality of information held in the cloud.

The A4Cloud stakeholders, for whom methods and tools are developed, include according to the A4Cloud Conceptual Framework deliverable D:C-2.1 [11]:

- *cloud subjects* that are entities whose data is processed by a cloud provider, either directly or indirectly. Individual cloud subjects are so called data subjects w.r.t the processing of their personal data and are often also acting as end users at the same time.
- *cloud customers* that are entities that maintain a business relationship with, and use services from a cloud provider; as well as
- *cloud providers* and affiliated cloud auditors and data protection officers (DPOs).

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 and for assessing privacy impacts [27] as well tools for cloud providers for providing transparency of data processing practices and handling security incidents based on risk analysis, policy enforcement, monitoring and compliance auditing with tailored IT mechanisms for security, assurance and redress.

### 1.1. Deliverable aims and scope

This report on “*User Interfaces Prototypes V2*” is delivered by task T:D-5.3 of work package “WP:D-5 User-centric tools for accountability”. The objective of the work package is to develop usable user interface (UI) prototypes for various combinations of tools assembled to address stakeholder-specific needs by following human-centered design processes.

The first deliverable D45.1 produced by task T:D-5.3, “*User Interface Prototypes V1*” [2], presented an initial user centred analysis of the A4Cloud tools for developing selected user interface prototypes, mostly in the form of mockups or lo-fi prototypes. All user interface prototypes in this first deliverable were developed by various user centred design methods, ranging from workshops with novice end users to expert evaluations by tool owners. The main intention of these prototypes were to serve as a starting point for further discussions, user testing and refinements.

This deliverable presents subsequent iterations of the user interface prototype developments and tests for A4Cloud tools and stakeholder-specific toolsets that to a large extent build directly on the initial prototypes presented in D45.1 [2]. The tools and toolsets, for which user interfaces are presented and discussed in this deliverable, are divided into cloud subject-, cloud customers- and cloud provider-specific tools and toolsets.

#### D:D-5.4 User Interface Prototypes V2

User Group	Tools	UCD Methodologies	Participants
Cloud subjects	“GenomSynlig” (Data Track & RRT)	Usability testing	13 participants for the Data Track.
		Survey	16 interview participants and 549 survey respondents for RRT.
		Semi-structured Interviews	
Cloud customers	DPIAT	Heuristic evaluations	1 expert user
Cloud providers & auditors	AAS	Expert evaluation	10 participants
		Wizard-of-Oz	
		Heuristic evaluation	
	AccLab	Heuristic evaluation	2 expert users
	IMT	Focus interviews	2 participants

Table 1: Design and evaluation methodologies used for the different A4Cloud tools and tool-sets

### 1.2. User-Centered Methodologies

User-Centred Design (UCD) is the approach of considering and involving users through the entire development process. The concept of User-Centred System Design was originally suggested as a method to promote the understanding of potential users in the different phases of a product’s design process [26]. Nowadays the term UCD is often used interchangeably with other similar approaches, such as Participatory Design [33], to refer to products being designed with the involvement of users at the different stages of the design process. This process is often iterative and can include different methods to consider end users’ goals and needs. The following sections describe some of the evaluation methods that have been used in our user interface development work for A4Cloud when following a UCD approach.

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. In particular, we have used usability testing of user interface prototypes for the tools and tool sets that are targeted to lay end users as cloud subjects, while expert evaluations were used for evaluating user interfaces for security administrators at the cloud provider’s side. The different approaches that we have been taken to do the usability evaluations are summarized in Table 1. Note that the UCD methodology for COAT is not included in the table since it has only been evaluated within the scope of WP:D-4.

**Usability testing** Usability testing is a technique that can measure the actual performance of users when trying to achieve a task with a given user interface. 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 [19]. Usability testing was considered a suitable method for testing of UI prototypes of the Data Track tool (see Section 4), since it has the advantage of letting lay users communicate their needs, opinions and expectations about new technologies.

**Semi-structured interviews** Semi-structured interviews are interviews where not all questions are designed or planned before the interview, allowing the interview to follow and explore new directions as they come up in the interview process [7]. In comparison to a structured interview, which has a fixed set of questions, this method allows the interviewer tailor the questions to the answers he receives and to further explore new ideas that may surface during the interview. In the context of WP:D-5, usability testing combined with semi-structured post-test interviews were used to evaluate the UI of the Data Track tool (see Section 4).

**Heuristic evaluation** Heuristic evaluation, as described by Jacob Nielsen [25], is a usability engineering method that helps finding problems related to usability in a user interface. The method includes letting a small group of evaluators examine the user interface and evaluate it w.r.t. its compliance with a set of usability principles; i.e. the “heuristics”. The heuristics are general rules that aim to describe common properties of usable interfaces. In a heuristic evaluation the evaluators usually inspect the interface individually, several times, before assessing its various elements in accordance to a pre-defined checklist based on the heuristics. The results are then used to produce a revised user interface design. Since the evaluators do not actually use the system to perform a real task, heuristic evaluation can be used early in the usability engineering lifecycle by using, for example, paper prototypes or mock-ups.

In the context of WP:D-5, heuristic evaluation has been used to evaluate the GUI of the Data Protection Impact Assessment Tool (DPIAT) and an early version of a GUI for AccLab (see Section 5.1 and 6.2). Heuristic evaluation was also used to find suitable tasks for the short usability test in the first iteration of the development of mockups for the UI of AAS (Section 6.1).

**Wizard-of-Oz** The Wizard-of-Oz method enables a UI to be evaluated technology that has not yet been implemented. A simulation is carried out by replacing a system’s functionality with a human experimenter (the “wizard”) who interprets the user’s actions and mimics the functionality, with or without the user’s knowledge. The technique can be used to “probe, discuss, demonstrate and evaluate ideas on how a device should respond to inputs (or actions) from users” [29]. In the context of WP:D-5, the Wizard-of-Oz technique has been used to evaluate the UI of the Audit Agent System (see Section 6.1). For a few test sessions, this was done over the Internet, aided by Skype for oral communication. The Wizard-of-Oz tool used (Ozlab; [29])



lets test participants connect to the (manipulated) mockup via ordinary web browsers. The presence of the web browser for the participant was not a distracting factor as this would be the normal way to access the A4Cloud tools.

**Expert evaluation** Besides usability testing done with lay users, expert evaluations are also considered valid usability studies which rely on the experience and knowledge of persons that specialize on their field of expertise. Their opinions and suggestions based on their experience can be a valuable input on the design and evaluation of technology. In the context of WP:D-5, expert evaluation has been used to evaluate the UI of the AccLab tool (see Section 6.2). For the iterative development of AAS UI mockups (see Section 6.1), walkthroughs of the mockups scenarios followed after the Wizard-of-Oz tests mentioned above.

**Focused interviews** Focused interview, as described by Merton and Kendall [24], is a method which can be used on both individuals and groups. The main goal is to test a hypothesis in a concrete situation which the participant is known to have been involved in before. Focused interviews could further be catalyzed by artifacts and encourages examination of the participants answers beyond the interview guide – making it semi-structured in nature. The method was chosen as an initial test method for tools not yet as mature as the rest of the A4Cloud toolkit; one such tool being the Incident Management Tool (IMT) (see Section 6.3).

### 1.3. Structure of this deliverable

The remaining part of this deliverable is organized as follows:

Section 2 introduces the A4Cloud reference architecture, the accompanying tools and the project demonstrator.

Section 3 then presents the foundation for our work in WP:D-5; an analysis of the concepts and terminologies that are currently being used in the existing versions of the A4Cloud tools as well as a bootstrap template that we created for the tools, in order to harmonize the look and feel of their graphical implementation.

In Section 4, user interfaces of cloud subject-specific tools and toolsets, namely of the GenomSynlig dashboard comprising the Data Track tool, PAPV (Plugin for Assessment of Policy Violations), and RRT (Remediation and Redress Tool), will be presented and the latest cycle of user evaluation of GenomSynlig will be discussed.

Section 5 discusses the user interfaces of tools for cloud customers, namely the Data Protection Impact Assessment Tool (DPIAT) and the Cloud Offering Advisory Tool (COAT).

In Section 6, the development and evaluation of user interfaces of tools for cloud providers; the Audit Agent System (AAS), the Accountability Lab (AccLab) and the Incident Management Tool (IMT) will be presented.

Section 7 presents an approach that can be used to plan and evaluate the user interfaces of A4Cloud project demonstrator.

Finally, Section 8 concludes our work with a summary of the main findings.

## 2. Background

This chapter explains some of the underlying concepts that the A4Cloud toolset rely upon, provides a brief overview over the different tools included in the toolset and outlines how the tools will be used in a project demonstrator. The purpose of the chapter is to make the reader familiar with the objectives of the tools and the context in which they are to be used before we present the results from the UI prototype work.

### 2.1. The A4Cloud accountability model

The A4Cloud project has developed a conceptual model for accountability (D32.1) [11], which defines a set of accountability attributes, practices and mechanisms. The accountability mechanisms have then been integrated into a framework that supports accountable cloud data governance, and that is based on a legal, regulatory, socio-economic and technical approach. The accountability mechanisms are functionally classified as being either preventive, detective and/or corrective and are intended to be used at different points in times, addressing the requirements that arise from a number of stakeholders in a cloud ecosystem.

To analyse the interactions that occur between the actors that are involved in the support of the accountability attributes, the project deliverable D33.1 (“Requirements for cloud interoperability”) [34] identifies four generic interactions paths between pairs of actors. These are:

- **Agreement**, which covers all interactions that lead to one actor taking responsibility for the handling of certain data provided by another party according to a certain policy (including a potential negotiation phase).
- **Reporting**, which covers all interactions related to the reporting by an actor about current data handling practices.
- **Demonstration**, which covers all interactions that lead to one actor demonstrating the correct implementation of some data handling policies.
- **Remediation**, which covers all interactions that lead one actor to seek and receive remediation for failures to follow data handling policies.

These phases have been used to outline the evaluation scenarios that we will present in Section 7 of this deliverable.

### 2.2. The A4Cloud toolset

To support the implementation of the accountability mechanisms, the A4Cloud project delivers a toolset, which has been described in the project deliverable D42.3 [8]. This toolset consists of in total 11 tools and a plug-in, which are illustrated in Figure 1. The tools that implement preventive mechanisms can be used to evaluate the potential risks in cloud data stewardship and to draft policies and decide on what security and privacy mechanisms that should be followed. The tools that implement detective mechanisms contains detection and traceability controls that monitor misbehaviours, for example policy violations or intrusions, during the normal operation

of cloud processes. Finally, the tools that implement corrective mechanisms can be used to provide notification and remediation to incidents in the cloud service delivery chains.

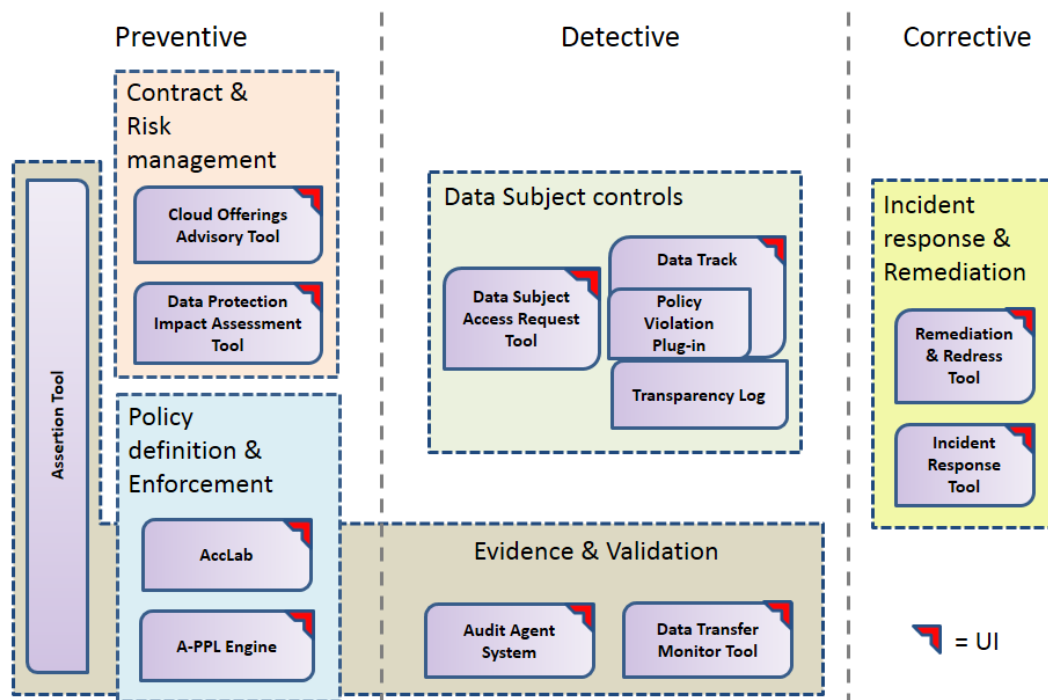


Figure 1: A high level view of the A4Cloud toolset [8]

As can be seen in Figure 1, seven of the tools in the A4Cloud toolset have graphical user interfaces (GUIs) and are hence in the scope of this deliverable. These seven tools are the following ones that are primarily developed for the following stakeholders:

- Tools for cloud subjects:
  - **Data Track (DT)**, which is used by data subjects to get a user-friendly visualization of all personal data they have disclosed to cloud services, with the additional capability to rectify data if necessary;
  - **Remediation and Redress Tool (RRT)**, which will assist cloud subjects (individuals or SMEs) in responding to real or perceived data handling incidents.
- Tools for cloud customers:
  - **Data Protection Impact Assessment Tool (DPIAT)**, which aims to help cloud customers to identify the risks in a given configuration and environment of carrying out

a certain business transaction, which involves the processing of personal or confidential data;

- **Cloud Offering Advisory Tool (COAT)**, which is designed to assist potential cloud customers (SME organizations and individuals) in assessing and selecting cloud offerings, with respect to certain security and privacy requirements.
- Tools for cloud providers:
  - **Accountability Lab (AccLab)**, which aims to help specifying human readable accountability obligations expressed in the Abstract Accountability Language (AAL) and to transfer them into a lower level machine-readable accountability policy language called Accountable Primelife Policy Language (A-PPL);
  - **Audit Agent System (AAS)**, which will enable the automated audit of multi-tenant and multi-layer cloud applications and cloud infrastructures for compliance with custom-defined policies, using software agents;
  - **Incident Management Tool (IMT)**, which will be used to manage anomalies and violations that occur in cloud services and should be notified to the cloud subjects, such as privacy violations or security breaches.

In addition to the seven tools presented above, the A4Cloud toolkit includes the following software: the Accountability PrimeLife Policy Engine (also referred to as the A-PPL Engine), the Assertion Tool, the Transparency Log (TL) and the Plug-in for Policy Violation Assessment (PAPV). These software are further described in the project deliverable D42.3 [8]. In the next version of the A4Cloud toolkit an additional tool will be introduced - the Privacy Level Agreement Tool (PLAT), which scope is to enable semi-automatic translation of Privacy Level Agreement statements to machine readable A-PPL rules.

### 2.3. The A4Cloud demonstrator

To demonstrate the applicability of the A4Cloud approach, the project has defined a *demonstrator*, which is an attempt to instantiate the A4Cloud accountability framework. The demonstrator describes how the A4Cloud tools are used by its intended stakeholders in the context of the so called “wearable use case”. The wearable use case constitutes a realistic scenario in which a cloud customer engages with cloud providers in order to deliver a web-based application for offering well-being data analytics to end users. A first implementation of the wearable use case has been done in the context of WP:D-7 and has been documented in the A4Cloud project deliverable D:D-7.1 (“First system and use case prototype”). An overview of the main concepts in this use case is displayed in Figure 2. A Cloud Subject (Wearable Customer) of the service provider, i.e. the Cloud Customer (Wearable Co), will get services that in fact are delivered by a network of cloud services, as demonstrated in the figure. However, the demonstrator can showcase the full accountability path from agreement to violation handling with the various kinds of stakeholders (including auditors, not shown in Figure 2).

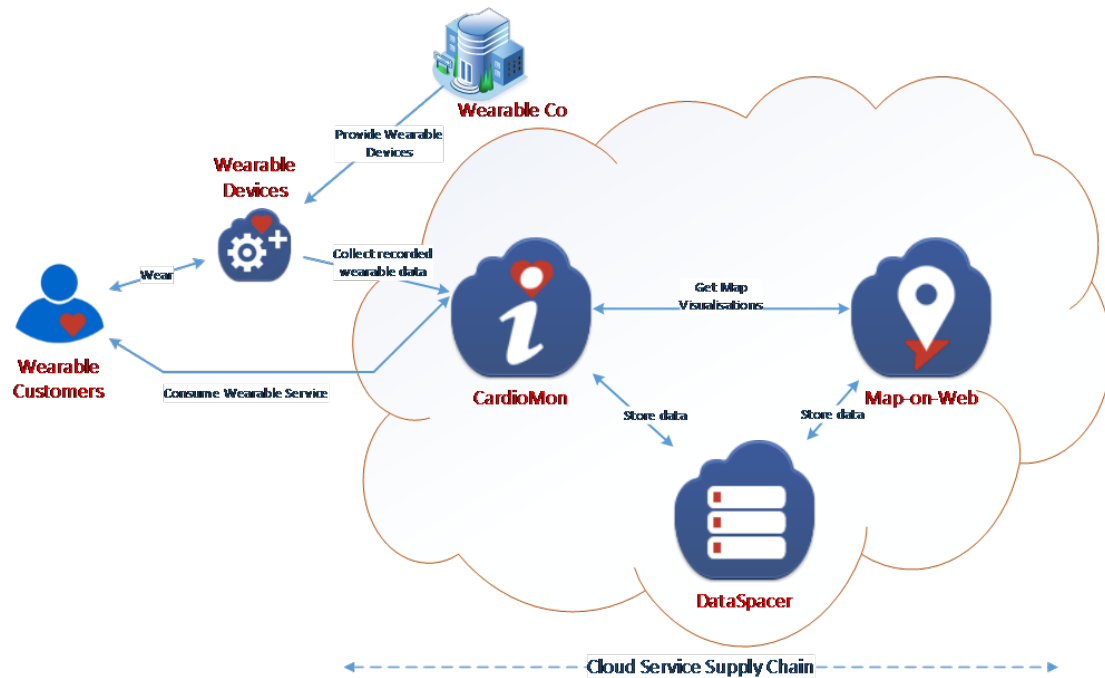


Figure 2: The conceptualisation of the Wearable Service. Picture taken from [8]

### 3. Foundations

The aim of Task T:D-5.1 is to develop stakeholder-specific UI prototypes for toolsets comprising different tools developed within the project with a **consistent** UI design.

In the following section 3.1, we will report on our efforts of providing consistency of terms and concepts across the different user interfaces considering at the same time also requirements of using terms and concepts that are suitable for their contexts and intuitively understood.

Moreover, for a unique “look and feel” of the UI designs of the A4Cloud tools and toolsets, a bootstrap template has been provided to all UI developers, which will be briefly outlined in the subsequent section 3.2.

#### 3.1. Consistent conceptual designs

This section provides a preliminary review of the tools and highlights their initial inconsistencies; this provides a motivation and rationale for having a common UI template and to a certain extent driving also the user-centred evaluations presented in the subsequent chapters of this deliverable.

A scanning of keywords and concepts, such as icons, appearing in different A4Cloud prototypes has been conducted during the spring 2015 as part of task T:D-5.1. The results have been collected in a table and can be found in Appendix A.1. The inspected user interfaces came from mockups in deliverables, videos, slide presentations, and prototypes. Naturally, concepts may start to be expressed differently when different teams develop prototypes in parallel. However, it should also be understood that depending on context, for instance intended user group or simply other texts in a certain user interface, differences may be allowed. What is presented in the table should serve as a starting point for further comparisons, discussions, and refinements rather than a hunt for superficial harmonisation.

Nevertheless, in addition to evaluations in the following chapter, this section lists things that might call for some sort of resolution. These are also marked in the table in Appendix A.1 with bold face “COMMENT:” as are also some other comments on wording and what appeared as unclear during the scanning.

Below is a list summarising some observations and comments that we have raised as feedback to the tool owners. This summary as well as the more detailed table with all comments in the appendix have the purpose to allow the A4Cloud UI prototype developers to put terminology and (early) icons in relation to the other prototypes.

- Should the Data Track 4.0 use both the terms *service* and *service provider*? These two concepts do not seem to be kept distinct. Possibly, one could elaborate on the difference between the service per se and the provider of the service.
- COAT (video) mentions “Acceptable Storage Location including Backup”. Note the assumption that “storage location” is about geographical location and what privacy laws apply. However, the end-user might mistake “storage location” to mean whether data are located on her hard drive, USB stick, or stored online at the service provider side. The icons in the mockup (earth globe and national flags) may help seeing people but possibly not all.

- COAT moreover mentions “Acceptable Data Processor Location” and the questionnaire pop-up says, “This refers to where the users personal data is processed and what laws apply to protect it. Processing data is very wide and it means carrying out any operation or set of operations on the information or data (for example organizing, retrieval, consultation, deletion or use of the information or data)”. This explanation is possibly not intuitive. Does it refer to where the data are being processed, where the data processor has its head quarter or what laws that apply? These can be three different locations.
- COAT on subcontracting: “Sub-contracting means that the Service Provider will use other companies or individuals (called third parties) to provide some of its services.” Can an SP really use “other individuals” (i.e. human beings) to provide some of its services?
- COAT on compliance: COAT mentions legal compliance but compliance could also refer to standards.
- COAT: “Should unlimited backup be included?” This phrase may spur further questions: Where is the backup located? In the same geographical location? On the same server?
- COAT’s security breach explanation mentions only a subset of all possible security breaches. Does this fact call for any additions?
- DPIAT (video): Is there a need for both “personal data” and “PII” to refer to the same concept?
- DPIAT (video): Is the word “establishment” good? The explanation says that territory does not matter but to whom the offer is made.
- AAS (web prototype), for Records window, In this window, is it possible to obtain old audit results? The term “Records” is also used in the Data Track. Do the term mean the same thing in both tools? (I.e., is there a risk that a AAS user sends a message about “records” that a Data Track user will read?)
- AAS label “Need review”: The verb in plural fit the headline as one can presume that more than one item can occur here. But does the verb also occur on individual items? (“Needing review” is longer and will not fit well in a tab label.)
- DTMT (D:D-5.1 mockup) “Location”: Again, what does location really mean?
- DTMT, “Take action” with a direct link to AccLab: does this mean that the user has to install AccLab in order to review a policy?
- RRT (D:D-5.1 mockup): Are incidents categorised by data types?
- RRT’s label “Contact service” appears inappropriate for a function to find incidents regarding a particular service (or service provider).
- DSART (D:D-5.1 mockup): The word “data” is used where it might be better to write “personal data”.

- PLAT: It might be unclear to users what some of the menus contain. (PLAT is now part of DPPT.)

AccLab is included in the table but no specific comments on the wordings in the UI is made there. Comments from different kinds of evaluations of AccLab and the other tools are found in Chapters 4-6, while the detailed table in the appendix have, as already mentioned, the purpose to allow the A4Cloud UI prototype owners to put terminology and (early) icons in relation to the other prototypes.

### 3.2. Bootstrap UI template for A4Cloud tools

In order to facilitate consistency in the look of the various tools developed within the A4Cloud project, we provided a template using the Bootstrap UI framework for web applications, which other tool owners in the project could take as the basis of the design of the user interface for their tool.

The template was based on Bootstrap 3<sup>1</sup> UI framework, which at the time of writing is a popular way of deploying the front end of web user interfaces. The advantage of Bootstrap is that it provides various layouts and predefined UI components that are easy to plug into the user interface as they are needed by the design. It also provides responsiveness, meaning that it can easily be adapted to work with various screen sizes.

The idea with providing this template was that the owners of the different A4Cloud tools being developed would be able to concentrate on the logic of the tool, and adapt this template to the visual and other UI needs of their tool. Tool owners were shown the template in a project meeting and were told to freely adapt this template to their own work, advising them to try to maintain the same colour schemes and to use the UI controls provided by Bootstrap as much as possible, instead of reinventing their own controls.

The template provides some examples on how to include some of the standard Bootstrap controls, such as showing alerts, opening pop-up dialogs, and using the icon library that comes with Bootstrap;Glyphicons. Instructions on how to use the font-awesome icon library was also provided. The colour scheme of the template was dictated by the initial prototypes of the COAT tool [1], which in turn resembled the colours of the A4Cloud project. An example screenshot of the template is given in Figure 3.

The template was created using Less CSS pre-processor<sup>2</sup>, which allows for quick changes in the styling of a web application by allowing more modularity, the creation of variables and the nesting of the DOM elements. When compiled, the resulting CSS is done to support multiple web browsers and to be more effective.

---

<sup>1</sup><http://getbootstrap.com/>

<sup>2</sup>More information on Less and how it works can be found in <http://lesscss.org/> (Accessed 2015-09-02)



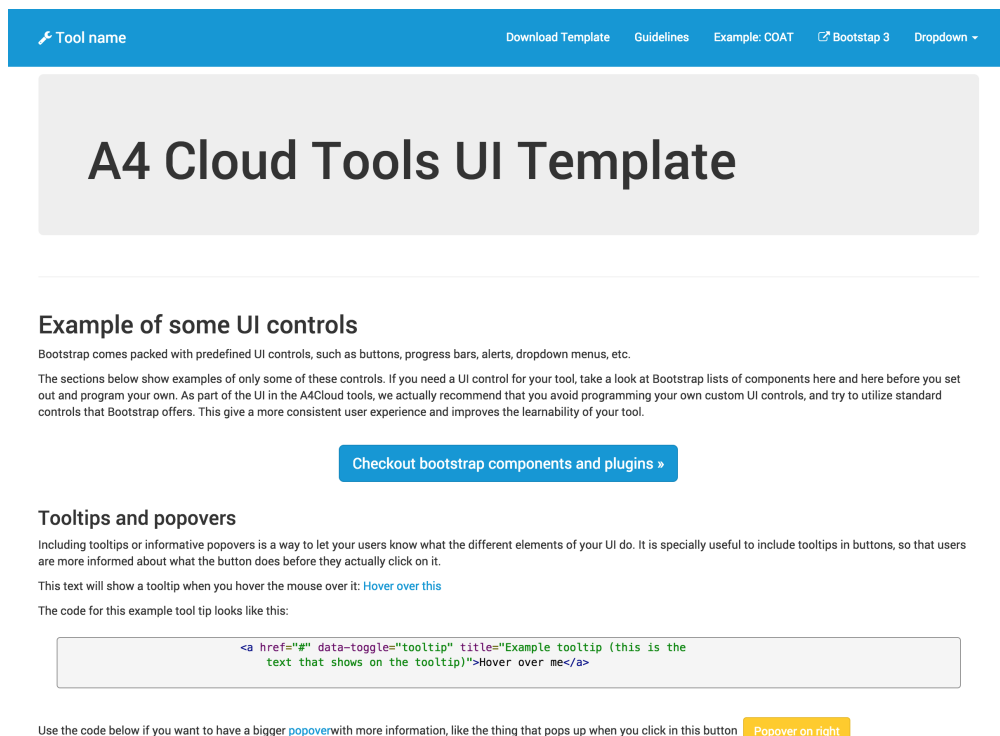


Figure 3: The suggested A4Cloud tool UI template.

## 4. User Interface development for cloud subject tools and tool set

Within A4Cloud, several tools have been developed for enhancing transparency over the flow and use of cloud subjects' personal data and for providing them with increased control over their data handled by service providers. This set of tools have been bundled into a privacy dashboard, which we have called GenomSynlig. In this section, the user interface development and evaluations of these tools and of the GenomSynlig dashboard will be presented and discussed.

### 4.1. GenomSynlig – A dashboard for end-user transparency

GenomSynlig<sup>3</sup> (or *Synlig* for short) is a proof-of-concept resembling an end-user dashboard which would allow cloud subjects to visualize and manage their data disclosed to different online cloud service providers, as well as become informed about possible incidents regarding their disclosed data to different online services and take appropriate action to remedy the incident or obtain redress for the possible damages caused. A screenshot of the GenomSynlig landing page is shown in Figure 4.

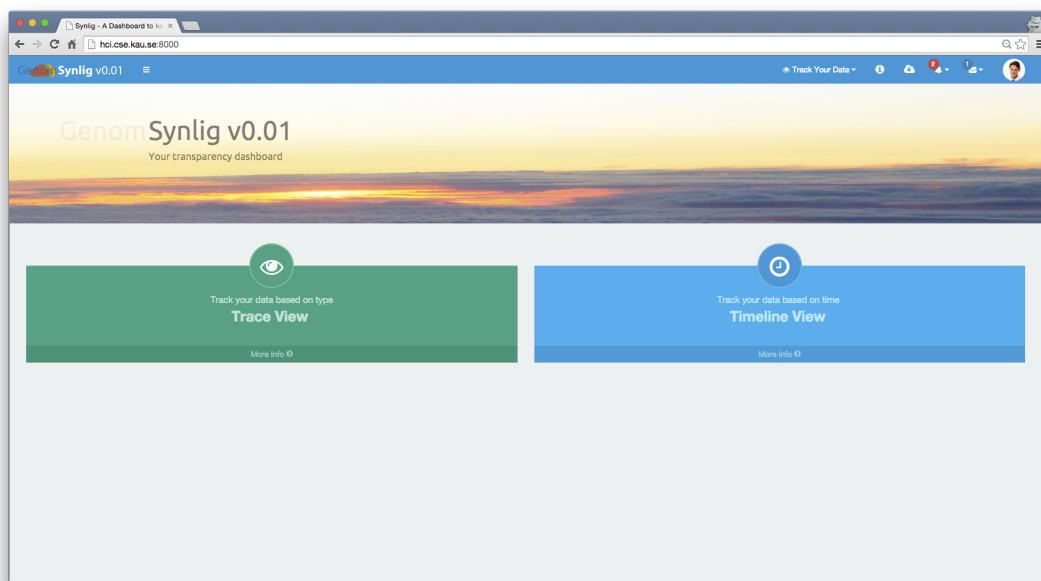


Figure 4: GenomSynlig landing page (as of August 2015)

The GenomSynlig dashboard comprises different tools for end-users that have been conceptualized and developed as part of the A4Cloud project. These tools include:

<sup>3</sup>GenomSynlig is a play of words in the Swedish language, where *genomskinlig* means transparent and *synlig* means visible.

**Data Track (DT):** presenting users with different visualizations of their personal data disclosed to different online services and allowing them to exercise their data subject rights online [4], [2], [3] (Section 4.2.1). The Data Track program is part of the GenomSynlig platform, and it has been referred to as a function of GenomSynlig under the user evaluations (see Section 4.3).

**Plugin for Assessment of Policy Violations (PAPV):** assessing privacy-related incidents in order to determine the appropriate channel and visual ways to notify the user about an incident [2] (Section 4.2.2).

**Redress and Remediation Tool (RRT):** allowing users to remedy a possible privacy-related incident and seek compensation when policy violations occur [2] (Section 4.2.3).

## 4.2. Interplay of GenomSynlig with Cloud Provider-specific A4Cloud Tools

This section will present the interplay of GenomSynlig with other A4Cloud tools at the cloud provider side for detecting and managing privacy incidents, which is also illustrated in Figure 5. The text below is an excerpt in slightly modified form from the project deliverable D45.3 [31].

The Data Transfer Monitoring Tool (DTMT) and the Audit Agent Systems (AAS) are tools at the cloud provider side for auditing the system for security and privacy incidents and informing the Incident Management Tool (IMT) about any detected potential incidents. A-PPLE (the Accountable PrimeLife Policy Engine) is a tool running at the cloud provider side that acts like a middleware between a database storing personal data at a service provider and the main application provided as a service (in the case of the A4Cloud demonstrator, the Wearable application provided by Kardio-Mon). A-PPLE will attempt to enforce the privacy policy associated with personal data stored in the database, such as purpose-binding rules and obligations like deleting data after a retention period. Since A-PPLE knows of all data subjects in the Wearable application, it is ideally suited to forward all human-readable incident descriptions from the IMT to the relevant data subjects. To do this, A-PPLE uses the Transparency Log (TL) as a secure channel.

On the cloud subject's computer, the cloud subject uses the Data Track (DT) to receive incidents reports from the service provider. DT uses its TL Recipient (the part of TL that receives messages) to do so. Once an incident description is received, DT uses the Plug-in for Assessing Policy Violations (PAPV) to access the severity of the incident, in case it is a policy violation. Based on the severity, DT displays the notification of an incident more or less prominently in the interface for the user. Once the cloud subject wishes to address the incident, he or she uses the Remediation and Redress Tool (RRT), which provides more information about the incident and offers, as the name suggests, remediation and redress options to the cloud subject.

### 4.2.1. Data Track – Data disclosure visualizations

The initial version of the Data Track prototype was designed and implemented during the PRIME<sup>4</sup> and PrimeLife<sup>5</sup> projects [28, 14]. Figure 6 shows a screenshot of a PrimeLife's ver-

---

<sup>4</sup>EU FP6 project PRIME, <https://www.prime-project.eu/>

<sup>5</sup>EU FP7 project PrimeLife <http://primelife.ercim.eu/>

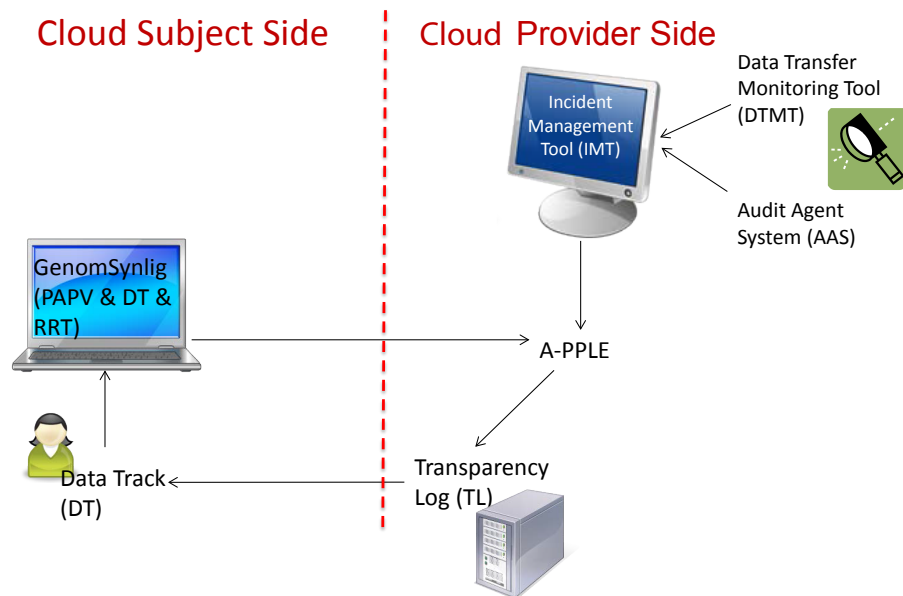


Figure 5: The interplay of GenomSynlig with other A4Cloud Tools at the Cloud Provider Side

sion of the Data Track's main user interface, which consisted of a two-dimensional table listing disclosure values of data sent to various service providers along with a time stamp and an overview of the remotely store data at the services' side. Moreover, the Data Track's UI allowed users to request corrections to or deletions of their remotely store data, and to check for possible policy violations by showing existing mismatches between the data that users have disclosed at some point in time and the data that was currently stored at the remote servers. A more detailed description of the PRIME and PrimeLife's versions of the Data Track along with the legal, security and UI considerations can be found in [28] and [14].

During the A4Cloud project, we have expanded the concept of the Data Track tool, adapting its UI to become part of a more comprehensive toolset for cloud subjects, as explained in the beginning of Section 4.1, and conforming with the A4Cloud architecture, as outlined in the project's deliverable D42.3 and D42.4. A description of the initial UI concepts of the Data Track within the A4Cloud project has been given in deliverable D45.1 [2], and results of the user evaluations of these early UI prototypes have been presented in deliverable D37.3 [3] and in [4]. An overview of the technologies used to design and develop the front-end of GenomSynlig's Data Track is presented in deliverable D45.3 [31].

The following paragraphs summarize the Data Track's approaches for the visualization of personal data disclosures presented in previous reports for earlier UI prototype iterations of the A4Cloud's Data Track. We expand those earlier descriptions with newer developments

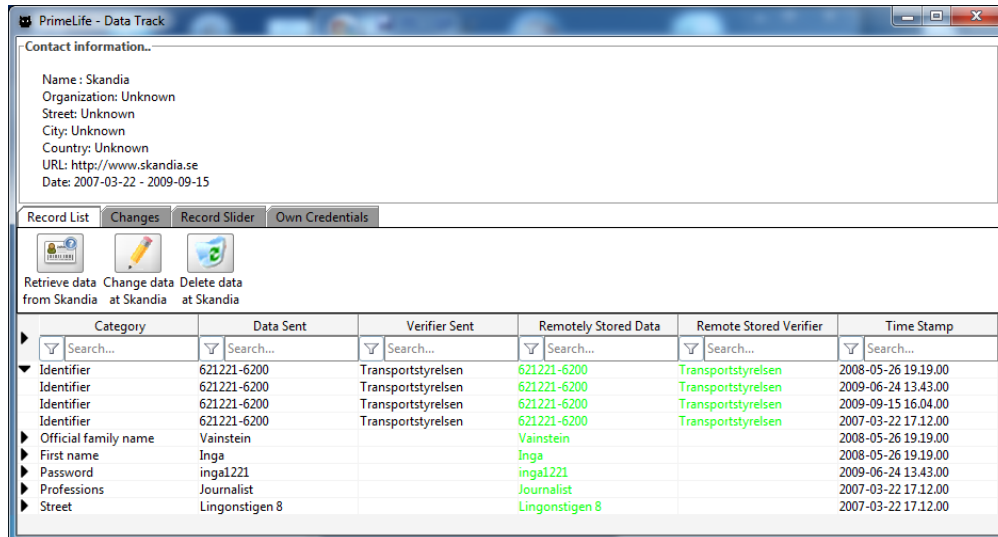


Figure 6: The user interface of PrimeLife's Data Track.

and improvements for the latest UI iteration. A report on the usability evaluations of these newer interface of the Data Track tool (referred to as “Synlig” integrated into the GenomSynlig dashboard are also presented in Section 4.3.

**The trace view.** Previous research studies suggest that network-like visualizations can provide a simple way to understand the meaning behind some types of data [6, 15, 20]. From a security perspective, it has been suggested that network visualizations have the potential for scalability and dimensionality often encountered in data related to security monitoring or mitigation [18]. Also, using traces between different online entities in order to visualize data flows and to promote transparency in online commerce has been suggested in [21] and [22]. In [16] diagrams displaying nodes and links have proved to be effective when analyzing paths, whereas matrix diagrams are better for identifying communities in the data. Earlier work related to visualizing an individual's history through LifeLines has also proposed the use of alternating colours, varying line sizes and icons to convey information about events on a person's life [30].

The concepts and ideas presented in these studies inspired us to suggest a visualization of a users' personal data disclosures, which we refer to as the “trace view”. A screenshot of the latest design of the trace view prototype is shown in Figure 7.

The main screen of the trace view is divided horizontally into three main panels. The middle panel (center of the screen) represents the user of the dashboard, with the intention to give the user the feeling that this is a dashboard where personal ‘things’ will be visualized (‘personal information about *me* and online services that *I* have contacted’). Personal data items that have been disclosed to an online service provider are displayed as icons on the top panel, and the logotypes of online service providers that have received the users' personal data items are presented on the bottom panel.

Showing small icons saves screen-real states, making the interface more scalable and allow-

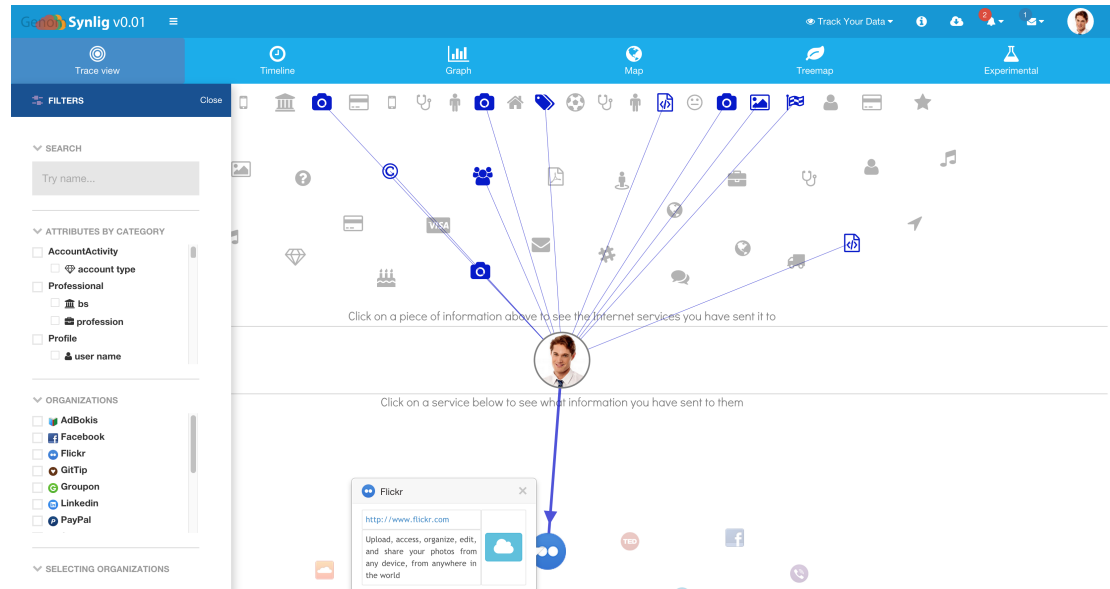


Figure 7: The user interface of the trace view visualization in GenomSynlig (Section 4.2.1), part of the A4Cloud project.

ing to display more items at the same time. When the user hovers over one of these items or icons, a box is displayed with more detailed information about the targeted item. For instance, hovering over a service provider's logotype opens up a tooltip<sup>6</sup> in the form of a box with the service's contact information, description of their business, etc. An example of such box is shown in Figure 8. Inside the box, a button in the shape of a cloud icon is shown. When this button is clicked a dialog is opened showing the data about the user stored remotely at with the selected service provider (as explained in the upcoming sections).

When the user clicks on one (or many) of the Internet service provider icons she will be shown traces connecting from the service provider icon to the profile picture in the middle panel and then to the icons for the information that those services have received about her. In other words, she can directly see the information that the selected service(s) have received about her (see Figure 7). Similarly, if she selects pieces of information on the top panel she will be shown tracing lines pointing to the service providers to which those pieces of information have been disclosed (see Figure 10). The intention with this interface is to let users see in a quick and interactive way all the data about them that they have disclosed at some point to different service providers. The tracing lines connecting the user's profile picture in the middle to the service providers at the bottom resemble arrows pointing towards those services, which indicate that personal attributes (from the top panel) have been sent or flowing to these services.

When users select many service providers, as shown in Figure 9, the tracing lines and personal attributes are colored, so that it becomes easier for users to identify which personal

<sup>6</sup>The open source library, qTip was used in our prototype to present information inside an enhanced tooltip.

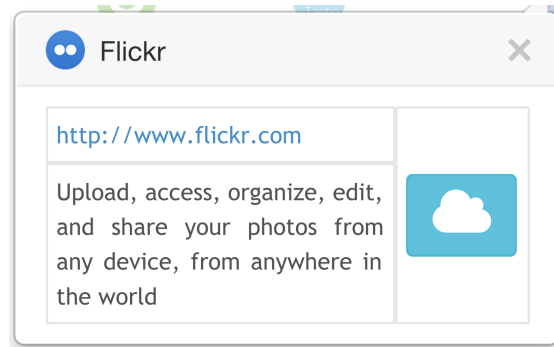


Figure 8: Box showing details about the selected online service provider. The cloud button opens a modal dialog (Figure 14) that shows data on the services' side.

attributes were disclosed to which selected services. Moreover, the thickness of the lines, which connect the service providers to the user's profile picture in the middle, increases or decreases depending on the amount of personal attributes that have been disclosed to those services. Since the tracing lines being displayed on the screen can grow substantially as users select many service providers or personal attributes, the trace view might help them realize the magnitude of the data that they have disclosed, potentially making them become more aware of consequences of online disclosure behaviors in future. The trace view also provides controls for filtering the number of items displayed on the screen by a certain property and for searching through the disclosures, as explain in the subsequent sections.

The trace view also offers users the option to see the common personal attributes that have been released to different service providers. For example, when this option is on, selecting three different services will show the trace from the service providers to the personal attributes that these services have in common, like the users' email address, as shown in Figure 10.

**The timeline view.** A second visualization approach of data disclosures that we have explored, presents each disclosure along a vertical line in chronological order. Thus, we call this visualization the *timeline view*, shown in Figure 11.

Every time a user discloses information to a service provider, it is logged in the Data Track's local database as a disclosure event (using the mechanisms provided by the Transparency Log tool described in [31]). Every disclosure event recorded in the user's Data Track contains a time stamp along with the users' personal attributes that were disclosed at that moment. The timeline UI retrieves ranges of disclosure events and displays them to the user in a vertical timeline, sorted initially from newest to oldest.

The logotypes of the service providers to which a disclosure was made are shown along the vertical line, the date and time when the disclosure was made is displayed on one side of the logotype, and a *disclosure box* appears to the opposite side. Inside this box, the personal attributes that were released on that disclosure event are listed, showing the type of attributes disclosed, their values and an image (i.e., an icon) representation of the attribute sent within the disclosure. The timeline implements the concept of infinite scrolling, meaning that it keeps

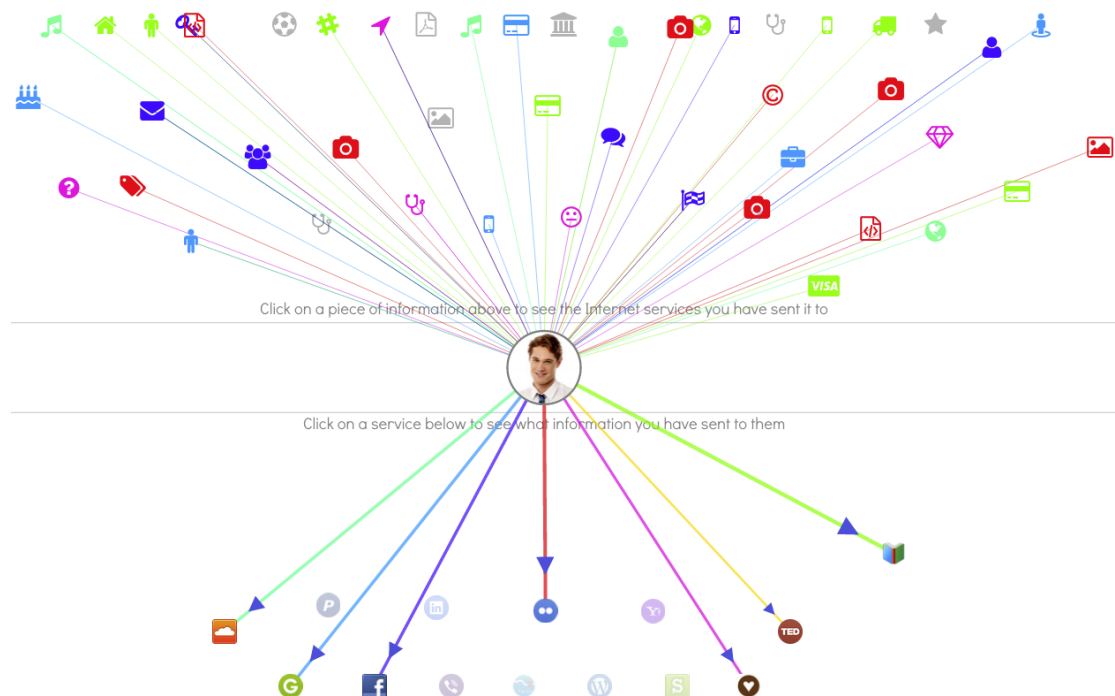


Figure 9: Selecting many service providers can give users an idea of the magnitude of their data disclosures.

retrieving disclosures events (from the Data Track's local database) as the user scrolls down the page.

For the sake of simplicity and cleanliness of the UI, each disclosure box only shows four of the attributes contained within the disclosure event. If a disclosure has more than four personal attributes, the user can toggle a button that reads "Show more" if she is interested in looking at all of the attributes for a particular disclosure event (see bottom of Figure 12). A button in the form of a cloud icon is available on the top corner of a disclosure box. When clicked it opens a modal dialog displaying the personal data about the user that is located at the services' side, as explained further in the sections below, i.e. it allows the users to access their data at the services' sides online. Moreover, the user is provided with filtering and search controls to look through the data and manipulate the disclosures that are being shown on the screen, as described also in the subsequent sections.

It was obvious for us that the design of the above mentioned trace view would not scale well for devices with smaller screens. Therefore, the timeline view also considered the responsiveness of its interface in different screen sizes. We carried out sketches and mock-ups to get an idea of the look-and-feel of the timeline elements on devices with various resolutions. An example is shown in Figure 13. For the implementation of the timeline, we adapted a freely available JavaScript library provided by CodyHouse<sup>7</sup> that included responsive properties in its

<sup>7</sup><http://codyhouse.co/gem/vertical-timeline/>



styling.

This dialog, shown in Figure 14, presents not only the personal attributes that have been explicitly disclosed by the user to the service provider, but also data about the user that has been implicitly derived by the service provider from analysis of the disclosed data. Through this dialog users would also be able to request correction or deletion of personal attributes, thus being able to exercise their data subject access rights pursuant to Art.12 EU Data Protection Directive 95/46/EC.

FP7-ICT-2011-8-317550-A4CLOUD

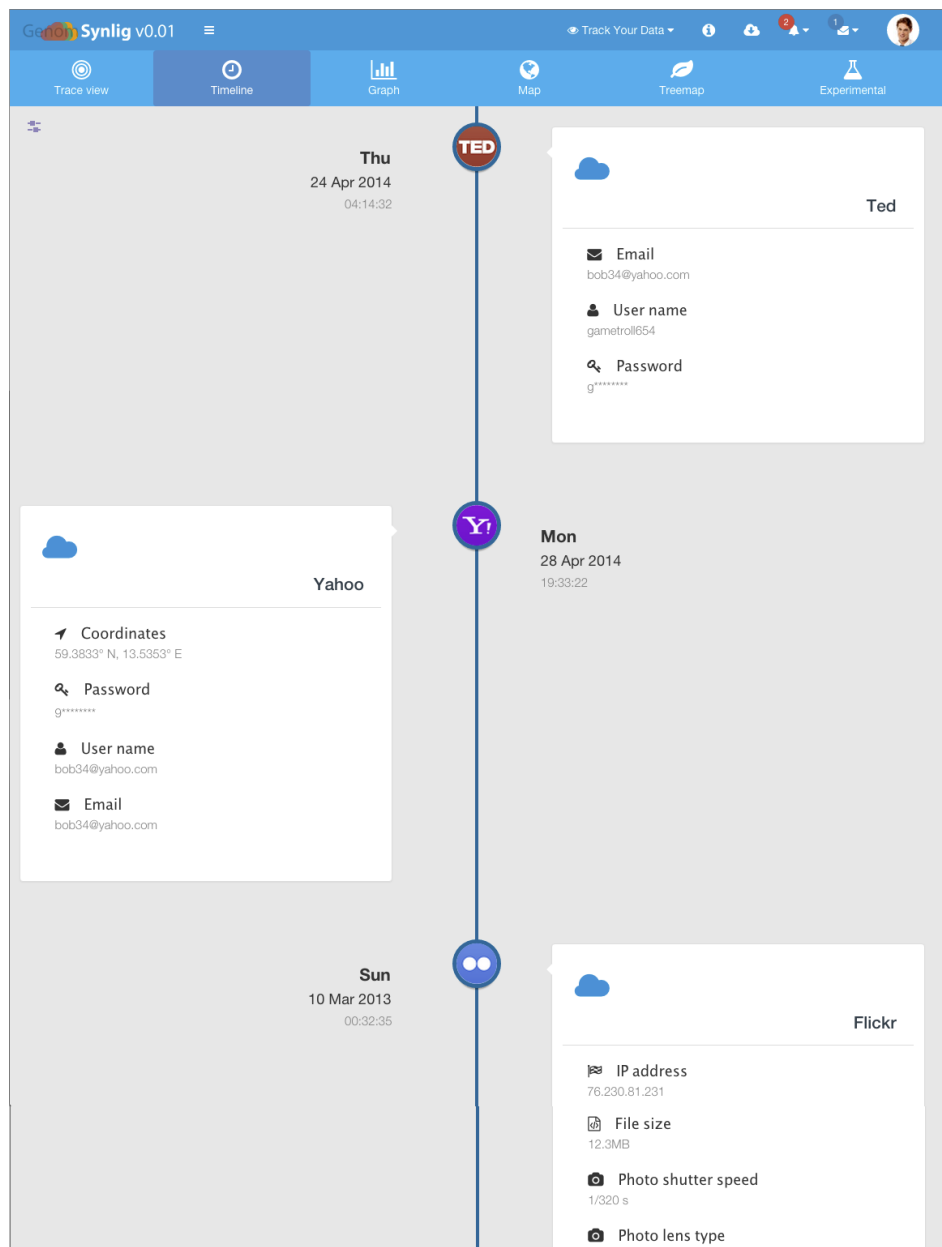


Figure 11: The timeline view of the GenomSynlig program, showing each disclosure event in chronological order.

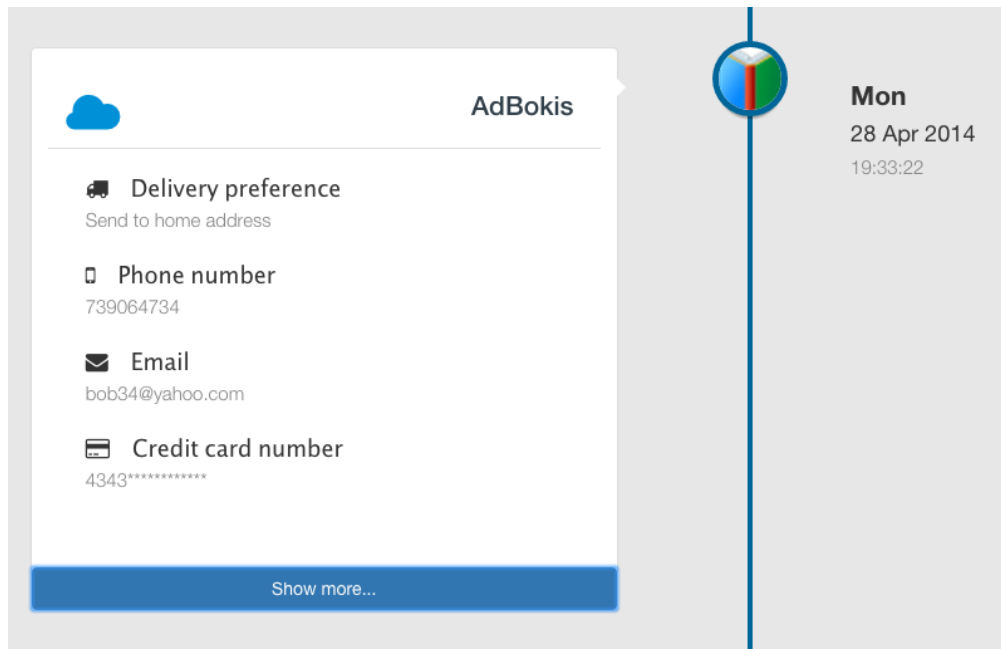


Figure 12: A disclosure event with a time stamp, showing four personal data attributes

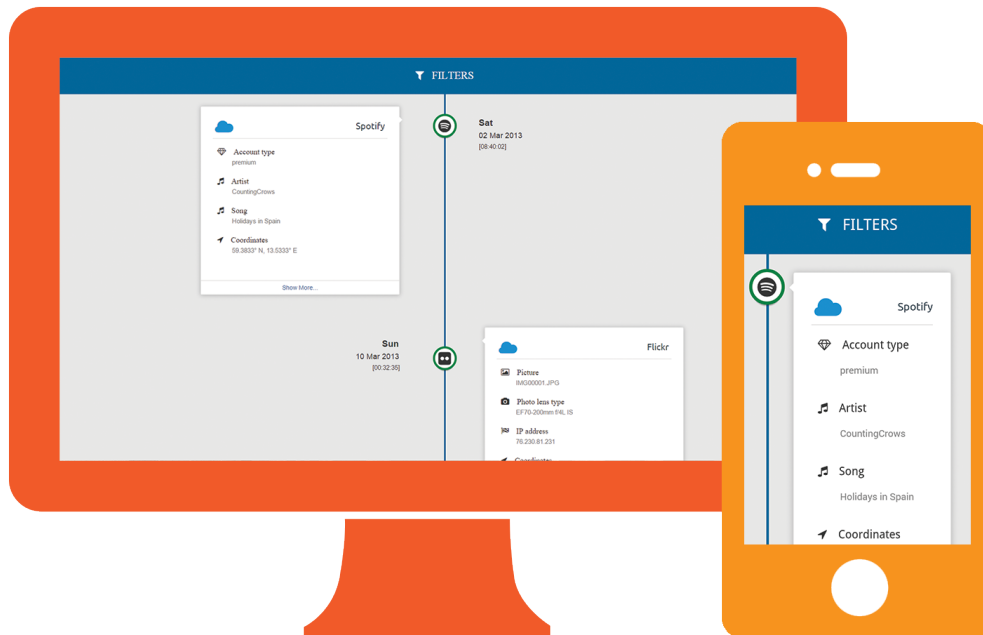


Figure 13: Sketch showing the responsive properties of the timeline view.

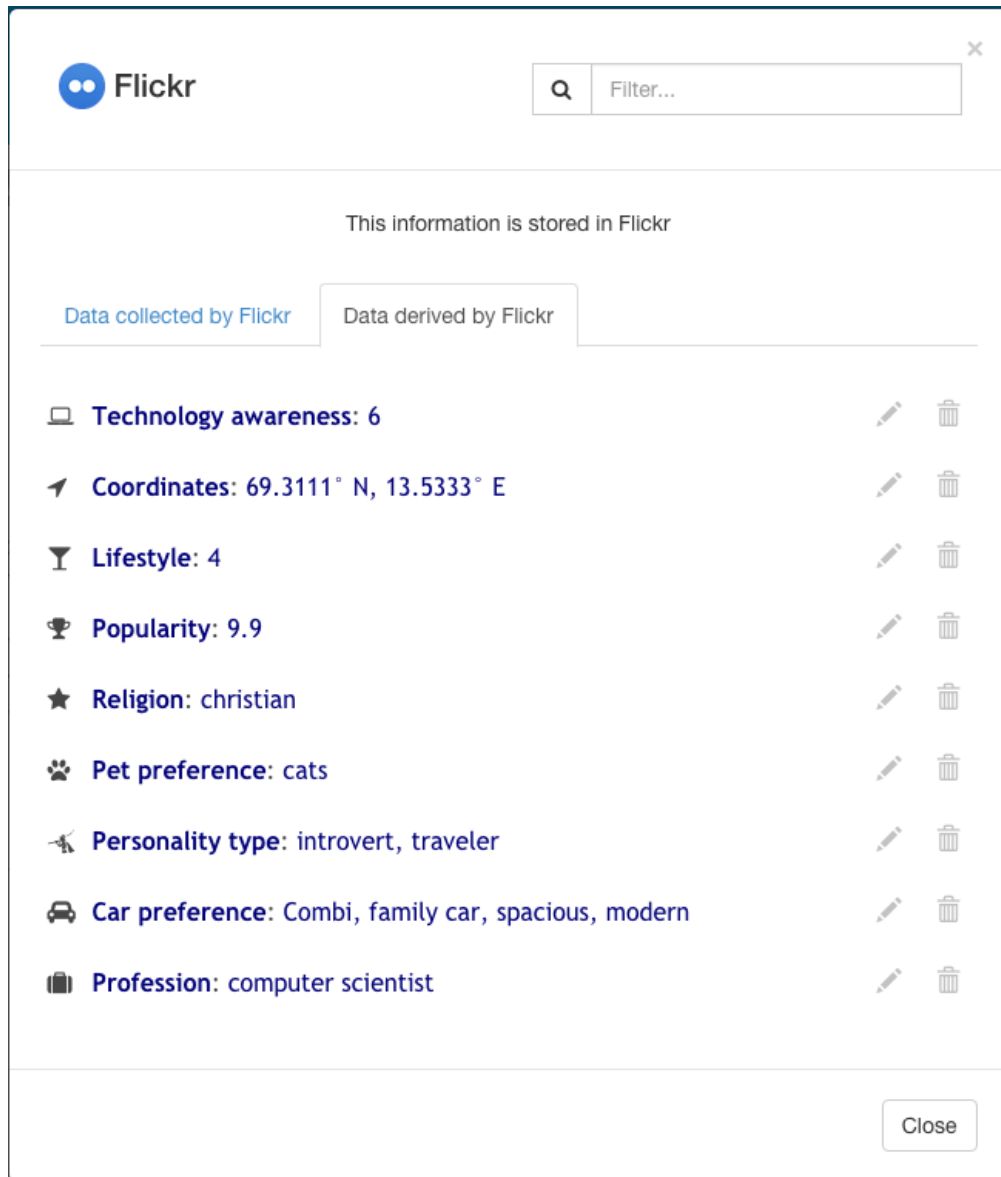


Figure 14: The modal dialog showing the explicitly sent and derived data stored at the service's side

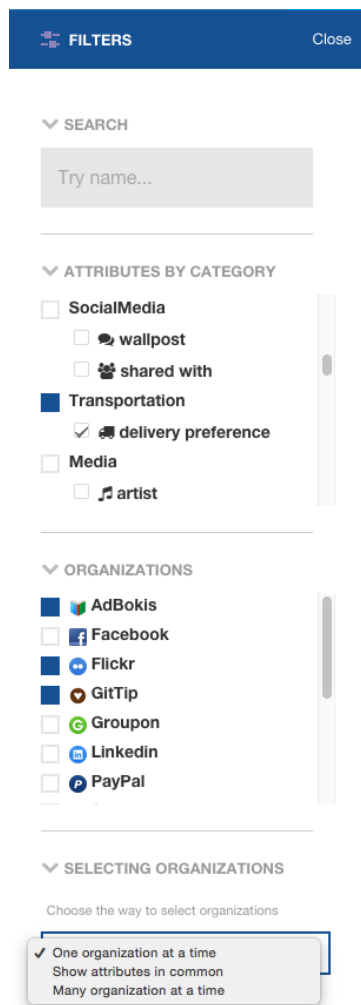


Figure 15: Some filtering and searching controls

**Filtering and searching options.** Presenting big amounts of information entities on a screen can be overwhelming for users. The version of the Data Track included in the GenomSynlig dashboard includes filtering and searching options (Figure 15) with the intention of helping users to make better sense of their personal data disclosures. By employing these controls, users of GenomSynlig can narrow down the elements being displayed on the screen in different ways.

For one, an autocomplete search function filters out items which do not match a search query. For instance, if the user starts typing the substring “Pass”, the personal attributes and service providers that match the string (e.g., “password”, “passport”, “LastPass”, etc.) will remain on the screen, while other items will be hidden from view.

Also, users can filter the elements shown by their type or by their name when choosing from a list of recognized personal attributes and/or service providers (i.e., organizations). Even more, the user can filter out personal attributes by their corresponding categories. For example, the user can select to only show elements related to medical data, then instead of scrolling through all the elements and selecting elements one by one, she can check the whole category of “Medical data”, which will only show those elements on the screen. Similarly, users can select only those service providers to be displayed on the screen, which might be useful when it might not be easy to find a service only by their logotype.

Moreover, users can select many service providers at the same time with the option to only show links to those personal attributes that the selected organizations have in common, as depicted above in Figure 10. A use case scenario for this feature is for the case when users want to keep their identities as separate as possible from different types of service providers, and protecting themselves against linkability.

In the timeline view, users are also given the option to filter the disclosure boxes by a service provider, or by a particular date range, time or day of the week. These features have been added to let users explore their data dissemination behaviours, and thus giving them a greater insight into the patterns that can emerge when disclosing (perhaps even unintendedly) personal data.

#### 4.2.2. PAPV – Plugin for Assessment of Policy Violations

In the A4Cloud project, the Plug-in for Assessment of Policy Violation (PAPV) “provides an assessment on the relevance of previously detected policy violations. The assessment made

is based on various sources, such as machine-readable policies that describes the obligations of the data controller regarding the treatment of private information of cloud subjects, as well as documents describing the cloud subjects' preferences with respect to the treatment of their data. The final assessment about a privacy violation made by the plug-in can be used in different ways to determine the way the cloud subject is informed about the particular violation." [2].

At the time of writing, no concrete decision could be found on how the PAPV would rank the detected privacy violations. The idea of the PAPV within the GenomSynlig dashboard, is that it will enable to assess these violations in a way that cloud subjects can understand the degree of severity of a particular incident. This can then be conveyed through the user interface in different ways, "for instance, in terms of its importance (e.g. by using different colours or sizes), the channel for its dissemination (either via mobile, email, a dashboard navigation bar or other), and the frequency in which it is communicated." [2].

### 4.2.3. RRT – Remediation & Redress Tool

The Remediation & Response Tool (RRT) in the GenomSynlig dashboard will not only allow to notify data subjects about possible breaches to their data or other privacy incidents that have been detected by the A4Cloud architecture, but also give them the possibility to remedy such incidents and in some cases obtain some kind of compensation.

In a related project with an external research partner, we investigated reasons for which end-users might become preoccupied about unwelcome and unexpected incidents regarding their privacy or personal data on the Internet [5]. To this end, we carried out semi-structured interviews with 16 participants and a survey with 549 respondents. Findings show that events related to account hijacking or hacking are commonly experienced by users, as well as moments when their data or online accounts become inaccessible. Getting their account hacked was also an incident that was at the top of their concerns, along with finding out that their personal data has been leaked online, that their identity has been stolen and misused, or that third parties have shared information about them.

Through our investigations, presented in [5], which included interviews, surveys and usability testing of a prototype, we identified certain characteristics that a possible remediation system ought to have in order to better assist users who are victims of unfortunate privacy incidents. These characteristics include:

**Immediate and personalized.** Victims of a privacy incident expected to be able to get help quickly and efficiently. Non-expert users expressed the need to get help that is catered to their individual problem, preferably through a human contact, like chat or customer service options. Users indicated that for a service provider to be perceived as trustworthy and transparent it should be able to remedy their situation quickly and to provide them with efficient solutions.

**Actionable and to the point.** When being notified about a possible incident, users would like to have a direct actionable strategy to remedy the incident. Thus, when possible, users should not be presented with complicated instructions redirecting them to other places where they might or might not find help, instead give them actionable steps that they can

do right in the UI. This creates the feeling that they are doing something to protect their privacy by taking an action.

For instance, the option to momentarily freeze the account(s) of the particular service provider that incurred the incident, is seen as an actionable step that could calm users experiencing an incident. Although, freezing an account might not be suitable for all types of incidents (e.g., once data has leaked out of a service provider, freezing the account with that service might do very little benefit), and it might be technically hard to accomplish, users indicated that this step might make them feel more at ease (e.g., “*at least I know that for the moment I am safe*”).


**Adaptive to their needs and proficiency.** Expert users might have a better idea of the steps to take to remedy a privacy incident and obtain redress, while non-expert users might be left clueless regarding how to proceed and how to better protect their privacy. A UI for a remediation tool, should adapt to the type of users and their needs, as well as to the context of the privacy incident. In other words, the interface should be intelligent enough to recognize which type of incident has happened and fill as much information as possible about the context of the incident. It should also find out the preferences and type of the user who is experiencing the incident.

**Reassuring while being explanatory.** Based on the type of users experiencing the incident, she or he might perceive the incident as more or less threatening than necessary. A tool that detects and assess the incident (such as the above mentioned PAPV), should make the user understand the scope and extent of the incident. This should be presented in an almost self-explanatory, but concise manner.

Our results indicate that lay users would like a tool that explains the possible consequences that the incident brings to their privacy and that reassures them, when appropriate, that there are ways to solve the problem.

**Preventive and educative.** In case that a user is victim of a privacy incident, the RRT should not only try to help the user remedy that given incident and obtain redress, but it should also guide users towards a better protection of their privacy or personal data on the Internet. For instance, the tool could guide the user towards setting up 2-factor authentication for some online services, and educate users about why the incident happened and how could it be stopped from happening again in the future.

Besides these recently identified properties, sketches for the UI of the RRT were laid out in A4Cloud project deliverable DD5-1 [2], which identified the need for different interface layouts depending on the way incidents are detected and initiated. Figure 16 shows the example of a incident report detected automatically by the Incident Management Tool (IMT), which fills information of about the incident and the affected user semi-automatically. At the time of writing, no implemented version of the RRT existed.



## Remediation request to [ Cloud Service ]

### Your details

The service needs to identify who you are in order to issue a remediation or give you redress for a possible incident.

**Name \***  
Your real name is needed for ...

**User name / Customer number / Social Insurance Number \***  
Provide a unique user name, customer number or other way in which you usually are

**Contact email address**  
Provide an email address where the service can contact you with a response

**Contact telephone number \***  
Provide a phone number where the service can contact you

This hasn't been recognized by the IRT and was not filled automatically

### Details about the incident(s)

Please corroborate that the information shown corresponds to the problem you want to solve

**Type of incident**

Short description about the incident... list of links to a corresponding service provider's URLs, etc...

Icons representing some of the types of personal data involved in the incident (three dots "..." indicate that there's more, these can be seen in the "Detailed view" of the incident). Tooltips will show what icons represent.

Icon representing the category or type of incident

Read more ...

**What does it mean for me?**

A description of the possible consequences of the incident(s) for the user in terms that the user can understand. No legal or technical jargon...

Read more ...

**Can I do something about it?**

A clear and concise list of simple steps that the user can follow, preferably with illustrations and examples

Incident reported on:

2014 / 06 / 06

Do you have information to add to this incident?

Provide information that you are aware of which can help remediate this problem.

Upload files as proof

upload

Cancel Next

Figure 16: When the RRT is triggered by the IRT, users can review and complete the remediations request.



### 4.3. User evaluations

The evaluation of the GenomSynlig program concentrated on the users' understanding and usability aspects of the features offered by the Data Track tool, touching slightly on the way people are notified about privacy incidents. Previous evaluations of the Data Track tool, described in [4, 3], have found that the purpose of the tool was clearly understood and the users were able to correctly identify to which services they had sent personal information too and what information a specific service provider had about them. It was indicated that further improvements were needed to facilitate the users access their personal information located at the services' side and also to help the users understand the difference between locally stored personal information and personal information located at the services' side.

During one of the workshop-sessions in the previous evaluation, the participants were asked "How often do you believe you would use the Data Track tool [now *GenomSynlig*<sup>8</sup>]" and 88.2% answered that they would use it at least a few times per month. Although, this high number cannot be confirmed until studies on a real working product have been made but it can still act as an indicator that users are aware of their personal information disclosures and want to keep track of them.

#### 4.3.1. Purpose

The purpose of this round of test was to evaluate the usability and user understanding of the GenomSynlig dashboard, using a use-case scenario where a participant has to disclose personal data to a fictitious online bookstore. Specifically we were testing the following features:

**An introduction tutorial:** During first time use of the GenomSynlig program, it could be useful for users to have a short introduction that shows the different parts of the GenomSynlig dashboard. As a conclusion from tests from previous versions of the Data Track, showing how to access data on the services' side might be particularly helpful.

**Many attributes and many organizations:** In earlier usability tests, we had only a few data attributes and organizations (service providers). We test for the scalability of the data items, and understandability of the icons that represent each node.

**Filtering and searching:** This version now includes the possibility to filter the amount of elements displayed on the screen as a way to support users' perceptual scalability as well as screen scalability (i.e., nodes in the trace view, or disclosure boxes on the timeline view). We test if people can locate these filters and find them useful for finding specific data attributes or answering certain questions about their disclosed data.

**Selecting many organizations:** This version allows for multiple selections of organizations. Users can see the attributes that have been disclosed to all of the selected organizations. Also, there is a toggle button that allows users to see only the attributes that many of the organizations have in common. This allows users to check how well or how bad their information is segregated among different services.

---

<sup>8</sup>During our evaluations we referred to this version of GenomSynlig as "Synlig v0.01" when communicating with our test participants.

**Services' side modal dialog:** Users can see the data about them located at a services' side. We test if users understand how to access the modal dialog displaying these attributes, and understand the list of attributes that is shown. More importantly, we evaluate the users' understanding of the difference between explicitly collected data and data that has been derived from analysis. We use the circumplex model of affect as proposed by [32] to get an idea of the users' emotional reactions to this feature of the program. Moreover, we check for the visibility of tabs and the understandability of text contained in certain places within the interface.

**Timeline:** We are going to test users' understanding of the boxes representing disclosures, the icons used, the benefit of visualizing disclosures this way, the way to open the modal dialog representing the services' side, and the way to filter data.

**Importing data into the GenomSynlig:** A page has been included that resembles the way users would connect to different online service providers in order to import their data into the Data Track and visualize it. We will test the user acceptance and understanding of such way to get their data into this program (i.e., would users be reluctant to aggregate their own data into one single service?).

### 4.3.2. Research questions

This test aimed at answering the set of questions listed below and some of the questions mentioned in the section above. These sets of questions are consistent with research questions from previous evaluation iterations found in [3], while at the same time testing for the recently implemented changes:

#### User interface features and concepts:

1. Do users find the trace view of the Data Track intuitive and comprehensible?
2. Do users find the timeline view of the Data Track intuitive and comprehensible?
3. Do users understand that there are two different views: (data records stored under the users' control (locally or in a privacy-friendly cloud infrastructure) and data records stored at the service provider?
4. What are users opinions of the trace view and the timeline view?
5. Do users find the filtering options and use them appropriately?

#### Understanding of data disclosures:

6. Can users intuitively find answers to queries regarding their personal data disclosures in a reasonable amount of time?
7. Do users understand what data they have sent to whom?

8. Do users understand that they can exercise the right to access the data they have sent online?
9. Does the interface convey the idea appropriately that the service can have more information about them, i.e. information other than the one explicitly sent, or that information was updated by the service provider?
  - a) Do users understand that there is a difference between explicitly sent data and data derived from analysis? What are their reactions to this?
10. Do users understand that Data Track data entries are stored locally, or at least, under their control?
11. Do users understand the difference between the local and the remote view and how to switch?
12. When using cloud storage for the Data Track, what are the users' beliefs regarding the location, security and privacy of their data?
  - a) Would users trust a privacy-friendly cloud storage?
13. Do users understand the way in which data can be "imported" into the data track through the use of so called connectors (connecting to the APIs of service providers)?

### **Motivation for use:**

14. Why would users make use of a tool such as GenomSynlig? Under which circumstances? Can they think of scenarios in which such personal data portals would be useful or nice to have?

### **4.3.3. Method**

The methods consisted of a usability test using a talk-aloud protocol in which participants were encouraged to express their opinions and understanding about the interface aloud. The moderator asked participants to carry through the tasks in a semi-structured interview fashion, in which already planned questions were asked and other questions that came up depending on the participants' responses. The moderator annotated in a pre-defined electronic form the successful completion criteria for each task along with some notes. An electronic post-test questionnaire was used after the participants were finished with the tasks. In the post-test questionnaire, which was filled out by the participants themselves, the participants got the chance to answer a couple of questions regarding their perceptions of the GenomSynlig program and also a few demographic questions, such as their age and occupation.

**Procedure.** In order to test the GenomSynlig's interface and answer the questions above, a scenario was setup, consisting of a fictitious online book retailer, called "AdBokis.com". Participants were asked to pretend to buy a book from "AdBokis.com" (see Figure 17).



Figure 17: Fictitious bookstore, AdBokis.com

When buying a book and paying for it, participants were asked to submit some personal details (see Figure 18), such as their name, their home address, their email, their phone number, their credit card for payment (participants was given paper with fake personal details to enter in the purchase-form). Participants were then shown the GenomSynlig trace view or timeline view where they were asked to perform some tasks and answer some questions. The tasks and questions are listed in Appendix A.2.

Figure 18: Information that is requested from participants to complete the purchase with AdBokis.com

**Tasks** Once participants were presented with the interface of the GenomSynlig portal, they were asked to answer some questions and complete specific tasks using the interface, with the purpose of answering the research questions specified under Section 4.3.2. Some of the questions to the participants were randomized in order to avoid introducing bias from the order in which the questions were asked (confounding variables). The moderator recorded one of the options, which served to calculate the Success Rate at the time of the analysis. The questions along with the list of successful completion criteria can be found in Appendix A.2.

Also, in order to minimize the bias of preference between the trace view and the timeline view, the order in which these are presented to participants were alternated (i.e., 7 participants were shown the trace view first, and 6 participants were shown the timeline view first).

A detailed description of the steps carried out during the test by the moderator are shown in Appendix A.3.

**Test participants** The test was conducted with 13 participants. The aim was to get a variety of participants, specially participants who are not technology experts. Test participants were mostly recruited in the city of Karlstad and Sunne, in Sweden, during the month of July and August 2015. Some of the participants were participants' that the test moderator already knew, and found suitable to participate in the test based on their varied backgrounds regarding occupation, age, education and computer experience and skill. The participants were recruited by the moderator, who was walking around carrying the needed equipment. The moderator asked the participant if he/she wanted to participate in a test session, explained the purpose of the test, how long it would take and what the participant would be reimbursed with. The reimbursement during this study was a chocolate bar, which the participant got after the test session was done.

Table 2 shows the participants' ID, age, technology literacy, their occupation, and their privacy score based on an instrument similar to the one used in [5].

ID	Age	Technology literacy	Occupation	Privacy concern
TP1	51 - 60	Little experienced	Self-employed	40
TP2	19 - 23	Somewhat experienced	Studying	36
TP3	24 - 30	Somewhat experienced	Working	35
TP4	24 - 30	Very experienced	Working	39
TP5	51 - 60	Somewhat experienced	Self-employed	33
TP6	24 - 30	Somewhat experienced	Working	28
TP7	24 - 30	Little experienced	Working	25
TP8	24 - 30	Experienced	Working	21
TP9	24 - 30	Somewhat experienced	Working	25
TP10	24 - 30	Little experienced	Working	26
TP11	31 - 40	Somewhat experienced	Self-employed	29
TP12	31 - 40	Little experienced	Studying	35
TP13	24 - 30	Somewhat experienced	Studying	30

Table 2: Participant overview, GenomSynlig evaluation (n=13)

**Test equipment** The tests were conducted with the use of a laptop computer and a tablet. The test used the desktop version of GenomSynlig. A short post-test questionnaire was setup electronically with the online tool Surveygizmo<sup>9</sup>. The test moderator used the tablet to keep track of the tasks that were given to the participants and also to record the observations made, since the participants were encouraged to "think-aloud". The participants used a laptop computer to carry out their assigned tasks and to answer the short post-test questionnaire.

**Test environment** The test environment varied a lot between different participants since the test moderator walked around in the city of Karlstad and Sunne in Sweden and asked people to

<sup>9</sup>[www.surveygizmo.com](http://www.surveygizmo.com)

participate in the test. About half of the test sessions were carried out in open public spaces e.g. cafés and the Karlstad public library. The rest of the tests were carried out in the participants' home environment.

### 4.3.4. Results

The results from the evaluations of the GenomSynlig program are presented in the following points. Thereafter, we list the main findings and suggestions for UI improvements.

#### Introduction tour

- All participants went through the introduction tour and no one had any comments on the tour, neither positive nor negative comments.

#### Traceview UI:

- Top panel – Most participants understood that the traceview showed information attributes about them (*"All available information about me on the Internet"*<sup>10</sup>).
- Some participants thought that it was all data about them or data in general from which some of it was about them (*"the amount [of information] that is available in the [GenomSynlig] program"*<sup>11</sup>, *"All data available in GenomSynlig"*<sup>12</sup>).
- Interestingly, some people understood the icons on the top as activities or actions they have taken on the Internet (like listening to music or paying with their credit card) rather than types of data items.
- Bottom panel – The participants' understanding of the elements in the bottom panel differed a bit but 12 out of 13 participants stated that it had something to do with services on the Internet (one participant referred to these services as *"apps"*). 5 out of these 12 participants said that it was *"Services on the Internet in general"* while the rest (7) stated that it was services on the internet that they had some kind of interaction with.
- A participant recognized that the company icons at the bottom were only icons from companies that she had imported into the GenomSynlig program (*"Online services from that I have imported my data"*<sup>13</sup>).
- Some participants mentioned the word *"apps"* (*"Various apps that have taken part of one's information"*<sup>14</sup>).
- Participants found it easy to know which information they have sent to a particular company, 77% successfully completed the question *"Using the traceview, how can you see the information that you have sent to AdBokis.com?"*. A question that asked about a similar thing, *"How can you see to which Internet services you have given your email address (bob.bobsson@hotmail.com)?"*, had a 62% success rate.

---

<sup>10</sup>Translated from: *"All information som finns om mig på Internet"*

<sup>11</sup>Translated from *"Den mängd som finns i programmet"*

<sup>12</sup>Translated from *"All den data som finns tillgänglig i GenomSynlig"*

<sup>13</sup>Translated from: *"Tjänster på internet som jag har importerat data ifrån"*

<sup>14</sup>Translated from: *"Olika appar som har tagit del av ens information"*

### Trace view filtering controls:

- People, who found the filter function, utilized it for many of the tasks that they were given. The filtering pane in the current interface was not very visible. However, the participants who found it, they used it widely.
- Presumably, making the filtering options more visible would lead to higher success rates for searching and filtering data elements presented by the interface, and thus making it easier for people to answer some questions with regards to their data disclosures). For example, when asking participants to identify all medical data about them that they have disclosed, those who were not aware of the filtering functions tried to solve the task by finding images (i.e. icons) that might have something to do with medical data (e.g., icons of a beating heart, of a stethoscope), or company names that were related to medical data.
- When filtering, some participants expected that manipulating the filtering controls would reflect their options on the UI. However, all attributes on the top were still being displayed. (e.g., if I choose Facebook in the filtering options, users expect that only attributes sent to Facebook would be shown. Same when selecting medical data, for example, Facebook does not have any medical data, so it should not be shown in the bottom panel.)
- Another question asked to the participants was “What would you do to see if Groupon and Tactiohealth have any information about you in common?”. This question was also possible to answer by using the filter function, yet many (8) participants failed to answer this question and only one participant was able to successfully answer the question. The rest (4) partially succeeded in answering this question i.e. they gave the correct answer but it was not within the time frame. The same as for the filtering pane might be applicable in this case, making the drop-down list more visible might increase the success rate.
- It was also clear that the option “Show attributes in common” (The correct option in the drop-down list in this case) was not very intuitive to the participants, because even if they paid attention to the drop-down list, not many chose to click the option. Most participants tried to solve the question by clicking on the two service providers in the bottom field, or dragged-and-dropped them on each other.

### Trace view services' side:

- To access the remote data on the services side, a cloud icon needed to be clicked as illustrated in Section 8. The icon was not completely noticed (visible) (*“I accidentally hovered over the cloud icon, otherwise I hadn't thought it was an icon”*<sup>15</sup>).
- It was hard for the test persons to distinguish the information shown inside the modal dialog representing the information stored at the services' side from the locally stored information shown in the main UI of the trace view and timeline view. The question, “What views shows the Synlig records stored on your system and

---

<sup>15</sup>Translated from: “*Råkade hovra över molnikonen, hade inte annars tänkt p att det skulle va en ikon*”



what view allows you to check what data a service have stored about you on their side?” was successfully answered by 6 participants while the other participants got really confused and gave up trying to answer the question. Some of the comments from the participants were “*don’t understand the difference between locally stored information / on the services’ side*”<sup>16</sup>, “*Believes that the elements that are highlighted when I click on the services are the information that the services have on their servers. [I] have no answer to what information is stored locally*”<sup>17</sup> and “*the elements in the top is stored locally and to see what is stored at the services’ side i click the cloud icon for each service*”<sup>18</sup> (see cloud icon in Figure 8).

- 6 participants managed to successfully answer the question, “Where would you click to see the information that AdBokis.com has stored on their servers when you purchased the book?”. Although, it was hard for the participants to understand the difference between data stored locally and data that were stored at the services’ side. And, even if they understood the difference, some participants did not understand why such a distinction was important.

### Timeline UI:

- Most participants successfully explained that the timeline view had to do with presenting data disclosures based on when they were disclosed, in chronological order (“*When i have done things, a timeline of my online activity*”<sup>19</sup>).
- Participants understood that each separate “box” in the timeline view represented one single data disclosure.
- Participants found it easy to check how many times they had sent data to a particular service provider by using the timeline view. Several questions covered the topic of being able to filter the data disclosures on specific service providers or a specific month range. The questions,
  - “What would you do to see the number of times that you have disclosed your credit card number?” had a success rate of 100%.
  - “What would you do to see all the disclosures that you made in March 2013?” had a success rate of 85% and a partial success rate of 15% i.e. success after 45 seconds.
  - “Can you tell me how many personal attributes about you were disclosed to Facebook in March 9th 2013 at 23:18?” had a success rate of 78%, partial success rate of 14% (i.e. success after 45 second) and only a 7% failure rate.
- Most of the participants didn’t notice the cloud icon, representing the services’ side, in the timeline view.

<sup>16</sup>Translated from: “*Förstår ej skillnaden mellan lokalt lagrad info / p tjänsten sida*”

<sup>17</sup>Translated from: “*Menar att elementen som markeras när en klickar på tjänsterna är den informationen som tjänsterna har p deras servrar. Har inget svar p vilken information som lagras lokalt*”

<sup>18</sup>Translated from: “*Elementen i toppen är lagrade lokalt och för att se vad som finns lagrade hos tjänsterna så klickar jag på molnikonen för varje tjänst*”

<sup>19</sup>Translated from: “*När jag har gjort saker, en tidslinje över min aktivitet p internet*”.

### Timeline filtering controls:

- Most participants tried to use the filter functions (it seemed like participants had a easier time in finding the filter function in the timeline view, maybe because the timeline view consists of fewer elements than the trace view). Because of the filter function being unimplemented in the timeline view, the participants had to scroll through the UI in order to check how many times they had disclosed data to a particular service provider.

### Timeline services' side:

- The cloud icon was even harder for the participants to notice in the timeline view than in the trace view. While the filter-function was easier to notice the cloud icon was harder to notice. For the question, "Where would you click to see the information that AdBokis.com has stored on their servers when you purchased the book?" 9 participants clicked on the "Show more" button and answered that the information shown in that list was the information stored at the services' side.

### Icons:

- The icons used in the GenomSynlig are from the open source icon library Font Awesome<sup>20</sup>. Because the GenomSynlig interface contains so many elements of personal information it wasn't possible to get one unique icon for every kind of personal information, which led to several kinds of personal information had the same icon that represented them. For instance, "Credit card expiry date", "Credit card number" and "Credit number" all had the same icon representing them. A mapping of personal attributes to Font-Awesome icon names can be found in [31].
- The repetition of icons in the user interface to represent different personal attributes caused that a couple of the test participants' felt confused when they were searching for a particular kind of personal information in the top panel of the traceview main UI.
- Another interesting thing is participants' different mental models. Some of the participants, when they were asked to "How can you see to which Internet services you have given your email address (bob.bobsson@hotmail.com)?" intuitively looked for the "envelope"-icon (which in this case was the correct one) while others were looking for an icon with the "at(@)"-sign.

### Derived data:

- The word *derived* was not completely clear for non-native English speakers. It is not a completely intuitive word to represent that data about the person has been analyzed and new insights about the person can be found (i.e., *derived*).

---

<sup>20</sup><https://fontawesome.github.io/Font-Awesome/>

- Many people understood that companies do gather as much information from the customer as possible nowadays (*"Because they do analyse my data"*<sup>21</sup>). A couple of participants showed surprise when realized that data about them was being derived from analysis of their explicitly sent data.
- 11 participants successfully noted that AdBokis had more information about them than they originally had sent to them when they bought the book in the online book store, although 3 participants weren't sure why, *"They can surely get a hold of information elsewhere, stuff in the other tab [Data derived from AdBokis] is stuff that they have gotten elsewhere"*<sup>22</sup> and *"All on the internet are crooks"*<sup>23</sup> are some of the comments from the participants regarding the companies analysis of their data.
- All participants successfully answered the question "Did AdBokis.com store the location you were at when you bought the book?" which is data derived by AdBokis (Coordinates) and it also appears on the tab "Data derived by AdBokis". Some participants also answered that the location comes from the collection of one's IP-address, and thereby it's possible to determine one's location.

### Security aspects:

- 4 people understood that the data being shown by the main UI of the trace view was stored locally and securely in their machine, another 3 participants claimed that, although it was stored in the GenomSynlig program, it was stored in some cloud-storage pertaining to the GenomSynlig program. Some participants (3) commented that the data is located in some Internet service somewhere, since the program was being run through a website. 4 participants thought that the data presented to them in the main UI were remotely located at all the various service providers that they have sent data to (*"And at the services that I have sent information to"*<sup>24</sup>).
- One of the questions, "In your opinion, who has access to the records being shown in the top panel of the trace view?" asked the participants of their perception of who has access to the data presented in the main UI of the GenomSynlig program. 6 participants answered that the government had access to their data that was presented in the program (*"Of course, I have seen Die Hard 4.0"*)<sup>25</sup>, 3 participants answered that the other service providers in the GenomSynlig program had access and 3 participants thought that only themselves and AdBokis.com had access to the presented data. Not a single participant thought that they were the only ones with access to their personal data, presented in the GenomSynlig program.

---

<sup>21</sup>Translated from: *För att de har analyserat min data.*

<sup>22</sup>Translated from: *"De kan säkert få information från någon annanstans [,]Den andra fliken är sådant de fått från andra ställen"*

<sup>23</sup>Translated from: *"Alla p internet är skurkar"*

<sup>24</sup>Translated from: *"Samt hos tjänsterna som jag har gett info till".*

<sup>25</sup>Translated from: *"Självklart, jag har sett Die Hard 4.0"*

#### 4.3.5. Results from post-questionnaire

The following points reflect results from the post-questionnaire administered to participant after the usability test session, which provided a more subjective view on the participants' opinions of the GenomSynlig program and their ideas of how this program would or could be used.

The table in Figure 19 shows the number of participants who answered statements related to the use of the GenomSynlig program.

		Strongly disagree	Moderately disagree	Slightly disagree	Neutral	Slightly agree	Moderately agree	Strongly agree
Information	This program helps me see the Internet services to which I have given my information.				1	1	3	8
	This program helps me see which information Internet services have about me.				1		3	9
	This program helps me get a good view of who knows what about me				1	1	3	8
	This program helps me see how much I have used a particular user name or email address				2		3	7
Remediation	If I regret sending information to an Internet service, I can remove that information with the help of this program.	3		1	5	2	1	1
Security	This program gives me an idea for the risk to have my identity stolen		1		3	2	3	4
	My personal information that is shown in the program is completely secure	1	1		5	2	3	1
	Nobody else can access the personal information that is shown in the program, only I have access	2	1		6		3	1

Figure 19: Participants answers to the tasks: “Rate how much you agree or disagree with each of the following statements concerning the Synlig program”

**Information about disclosures.** Participants' responses indicate that they understood the purpose of the GenomSynlig program and they saw it as a potentially useful tool to get information about their personal disclosures.

**Suspicious about security of data.** Responses to the post-questionnaire suggest that participants did not have a clear understanding of the level of security of their data, and who would have access to it.

**Uncertainty about remediation.** Thanks to the A4Cloud architecture, the GenomSynlig program would allow people to request correction and/or deletion of some of their disclosed attributes. The results from the post-questionnaire indicate that it was unclear for participants that this is possible to do with the GenomSynlig program. However, the reason why this is unclear is unknown. Presumably, because there was no tasks during the test sessions that allowed users to try the editing and deleting controls, or maybe these controls were not very obvious.

**Emotional reaction to personal disclosures.** Consistent with earlier evaluations [3], a number of participants (6) expressed feelings of astonishment and surprised by the personal data displayed by the GenomSynlig program.

**Concerns regarding Internet usage.** We measured participants privacy concerns, using the same scales as used in [5] based on [9]. From the data it can be observed that our participants were slightly skewed towards being privacy concerned, with an average privacy concern score of 30 out of 50.

**Users preferred the trace view over the timeline view.** Out of the 13 participants, 7 participants were initially presented with the trace view interface during a test session, while 6 participants were shown the timeline view first. When asked “*Which of the two views of the GenomSynlig program would you prefer to use?*” 11 participants answered that they would preferred the trace view as a way to track their data disclosures, while 2 participants preferred the timeline view.

#### 4.3.6. Findings and suggestions for UI improvements

The following points present general findings from the user evaluations and some suggestions for design improvements based on these results.

- **Who has access to the data?** Users, as for now, have a hard time in understanding that they are the only ones with access to the data presented in the main UI of the GenomSynlig interface. The interface should make it intuitive to the users that they are the only ones with access to their own data that is presented in the main UI in the trace view and timeline view. If the users understand that they are the only ones with access to their data, i.e. that their data will be under their full control, they might experience the GenomSynlig program as more trustworthy and secure. In the introduction tour, the text “The data imported into GenomSynlig program is secured and under your control” is displayed in several frames but the text is very small (with the exception of the last frame).

One possible solution would be to also incorporate that information in the main UI of the trace view and timeline view at the moment of showing the newly imported data, as exemplified by Figure 20.

Another possible solution could be to clearly inform users, at the time when they are importing data from a selected service provider into the GenomSynlig program, that the data that they are importing is being securely transferred and stored in their devices and under their control. These suggestions are exemplified in the sketches of Figures 21a and 21b.

- **Increased discoverability of the filter pane.** Observations during the user evaluations showed that participants often missed the existence of filtering controls, which were accessible under a button which opens the filtering pane. This can be achieved by having the filtering and searching pane open by default when the program starts. Also by making the filtering button that opens the pane bigger, more attention-catching and in a more contrasting colour.
- **The affordance of the services’ side button has to improve.** The affordance of the services’ side button could be improved by replacing the button or by adding some text

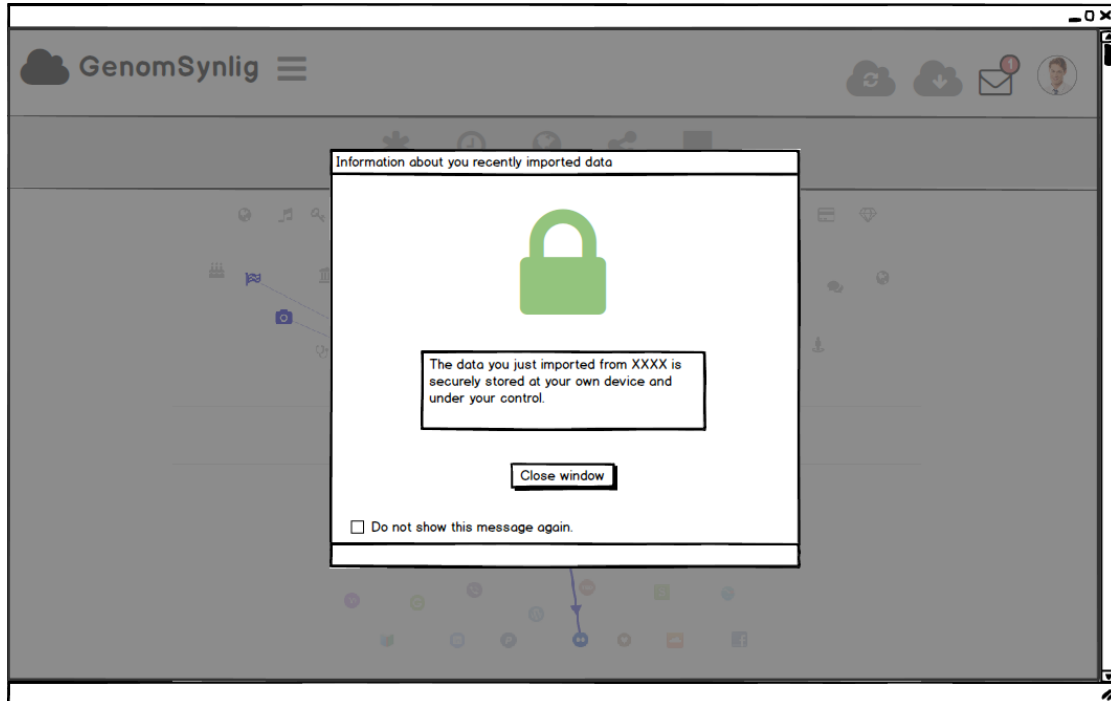


Figure 20: Conveying to the user that newly imported data is stored securely in their device and under their control.

to the button. The services' side button could also be changed to look and act the same as the button for the services' side button in the trace view (appearance and mouse-over functionality).

- Confusion between services' side and locally stored data.** The tested version of GenomSynlig lets users access the service's side by clicking in a small cloud icon that appears besides a service provider's name (see Figure 8). As the tests showed, this approach makes it difficult for lay users to understand the difference between the data stored locally on the GenomSynlig program and the data that is stored remotely in the services' side. This is a challenge that has also been commented in earlier evaluations of the Data Track tool [4], and which we, as the tests showed, did not succeed to address successfully yet for the later iterations.

Considering that the upcoming EU Data Protection Regulation will require that data subjects can exercise their data subject rights electronically, alternative UI concepts to mediate the different storage locations (local vs. remote) as well as ways of taking this up more prominently in the introductory tutorials need to be investigated.

For the next iteration of the GenomSynlig dashboard we suggest two possible ways to change this paradigm and try to address this problem:

1. One solution might be to take advantage of the menu bar or starting page of the

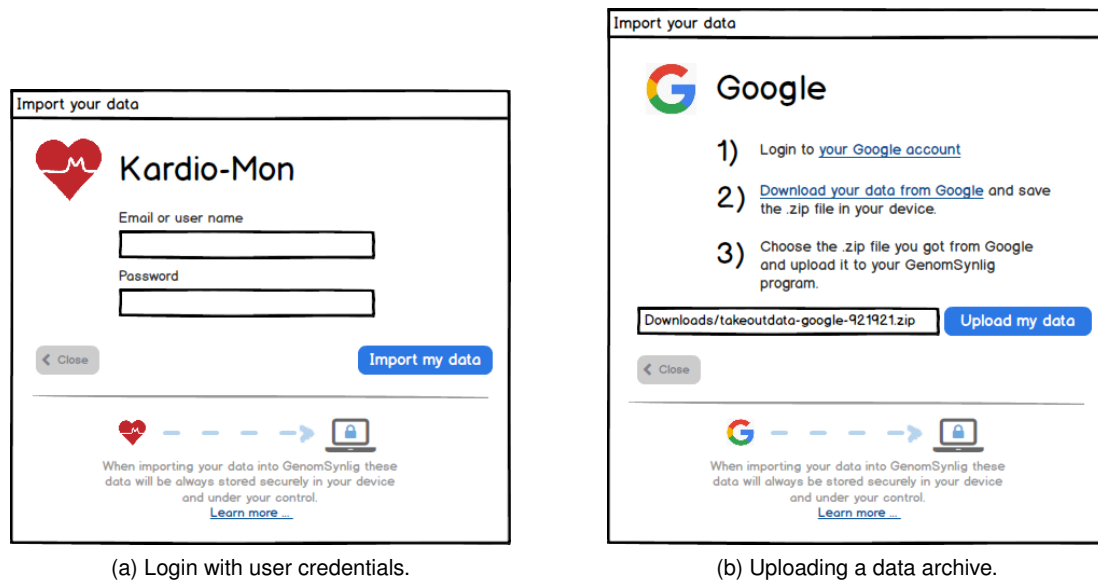


Figure 21: Suggested dialogs for importing external data disclosures into GenomSynlig.

GenomSynlig dashboard to provide users with two separate *modes* from the start. One mode would allow them to see only visualizations of the locally stored data, while the other mode would request a connection to the remote side of an specified service and visualize the remotely located data at from that service. Figure 22 shows the possible starting page giving the option to access either of these modes.

Contrary to the previous version, this option would not force users to access a service's side by locating the service provider in a visualization, but rather it would have a separate option to explore the data on a selected service's side. Colours, images and explanatory texts can be used from within a visualization to keep the users informed if they are data being visualized is stored locally or is at the service's side.

2. Another alternative could be to convey to users the idea that their GenomSynlig dashboard creates a *connection* to a particular service provider which is supported by this dashboard. One connected, users import the remotely located data into the dashboard. The visualizations of their disclosures would be a reflection of the data on the services' side. This reflection of the service's side could be out of sync with the remote database, and by clicking on a *Syncing* button the newly disclosed data would be fetch and visualized in the dashboard.

The Syncing process can be done seamlessly in the background, so if there are a lot of data disclosures being imported the user can still interact with other parts of the dashboard. A small unobtrusive indicator could be given to inform users about the status of the syncing process. In some visualizations, like the trace view, newly imported data could be even displayed in real time as it is being updated from the

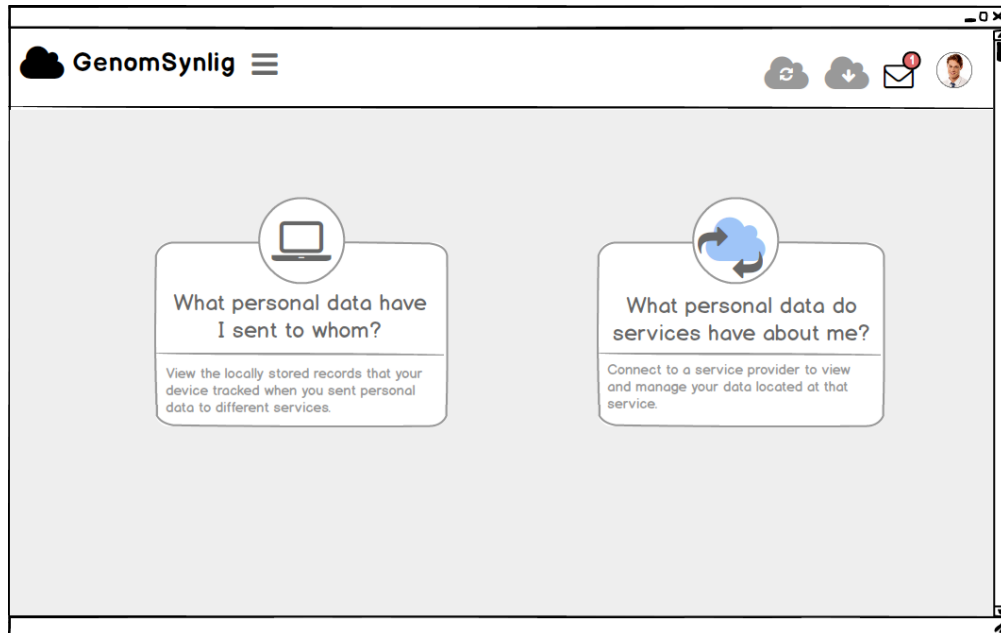


Figure 22: A redesign proposal of GenomSynlig in which users have the choice from the start to access data stored locally or control their data stored in a remote service.

remote side.

The controls that allow users to exercise their privacy rights by, for example, requesting correction or removal of disclosed attributes stored at the services' side, would be provided from within the visualization itself. Similarly, the differences between explicitly collected data and derived data can be expressed from within that same view with the use of colours, line patterns or other indicators.

In short, this alternative suggest to have only one view in the Genomsynlig dashboard, which mirrors the data located at the services. Many visualizations can be explored with these data. Figure 23 shows a proposal for a page that would list the different online services supported by GenomSynlig, and the alternative looks for each service depending on its status.

- GenomSynlig dashboard as a stand alone tool.** In order to give the impression that many of the actions of the GenomSynlig program occur locally and that the data is securely stored in the users' device, it is recommended to not show the program inside a web browser window. At the time of evaluation, some participants made comments that indicated that they believed the GenomSynlig program was a web application residing in an external server and not running on their computer. This was greatly due to the fact that GenomSynlig was shown inside a browser. Removing the chrome from the browser and having it as a stand alone application could presumably resolve this confusion, thus increasing the trust on the program that aggregates personal disclosures.



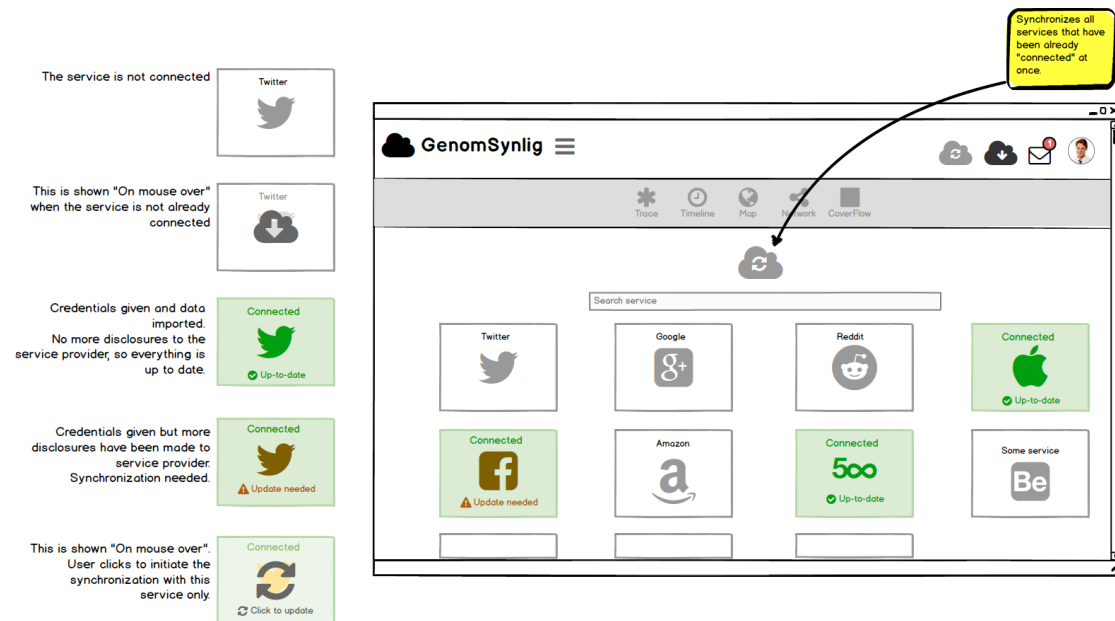


Figure 23: Connecting services to GenomSynlig – suggestions for the synchronization status.

- Mapping graphical icons to personal data attributes.** As part of our work regarding visualizing data disclosures we observed the need for having small visual graphical elements, or icons, that intuitively represent personal data attributes or service providers' logotypes. Logotypes are easier to recognize because they are usually unique and have characteristic features. However, there are no standard icons for representing personal data attributes.

We ran a small experiments with eight participants from a pilot study to explore the meaning they would assign to a commonly used open sourced library of vector-based icons. As mentioned earlier, GenomSynlig visualizations use icons from the Font-Awesome vector library, which are easy to manipulate and scale. Therefore, we decided to based the study in the existing icons provided by the Font-Awesome library.

For this preliminary study, we created a simple platform which, first, listed instructions for participants about their involvement and the task they were about to perform. Then, participants were shown a list of 20 carefully selected icons from the Font-Awesome library, and were asked to write down what they believed the icons represented in the context of data disclosures online. The purpose was to investigate which type of personal data attributes they would associate with the graphical icons being shown.

A detailed discussion of the findings from this preliminary study can be found in [23], and the mapping used for the icons presented in the GenomSynlig prototype can be found in [31]. To mention a few of the observations, it was hard for participants to couple a particular icon to the intended meaning in the context of personal disclosures. In Figure 24 icons that are grouped together were noted by participants as unclear, since they

could represent similar attributes. It was also noted in [23] that graphical icons by themselves in the context of personal data disclosures can create confusion if they are not accompanied by a short description of their meaning.

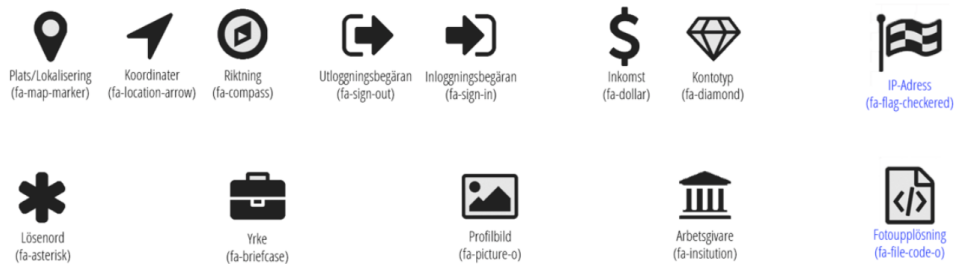


Figure 24: Font-Awesome icons which participants pointed out as unclear in the context of data disclosures. Taken from [23]

Based on the findings of this preliminary test, we modified the icons used in the trace view and timeline view of the GenomSynligg interface.

In general, we observed the need for standard icons representing personal attributes. Using small graphical icons in various visualizations of data disclosures would allow for better screen scalability of the big data created by several disclosures, as well as for user recognition of attributes of interests after some time of interacting with the program. We suggest to carry out a larger scale test with additional icons from standard icon libraries to unveil the meaning that participants would assign to those graphical representations.

## 5. User Interface Development for Cloud Customer Tools

Within A4Cloud, some tools have been developed to assist cloud customers in assessing risks and choosing appropriate cloud services for their purpose. In this section, the user interface and evaluations of these are presented and discussed.

### 5.1. Data Protection Impact Assessment Tool (DPIAT)

The Data Protection Impact Assessment Tool (DPIAT) is aimed at helping cloud customers such as SMEs to identify and assess the risks for a given configuration and environment of carrying out a certain business transaction such as buying a new cloud service.

The tool will be used to show:

- Whether data is personal data and how sensitive the data in question is
- How personal or sensitive data can be secured in the cloud
- What risks exists in relation to data breaches and privacy of cloud service users

**User Interface** It seems that the tool has adopted some of the advice given in D:D-5.1 [2], like the progress bar and the final report. Figure 25, 26, and 27 show the user interface of DPIAT as it is implemented at the time of writing this deliverable.

**A4 Cloud Data Protection Impact Assessment Tool**

**Please choose a Questionnaire**

This tool is a decision support tool to help you identify the risks involved in a transaction such as buying or using new cloud service/service provider. The tool is built on a risk and trust model to perform a thorough risk assessment to your configuration and environment. It will also help you understand the risks by providing information about their meanings and consequences. If you don't know already, use the 'Easy Mode Screening' to see whether you need the extended risk assessment mode.

Select a service provider

Map-On-Web

**Pre-Screening Questions**

The privacy quick scan mode indicates whether an extended Data Protection Impact Assessment would be necessary or recommended. It includes a set of 6 questions, which assesses if the information you deal with constitute personal data or not, and then it evaluates the kind of information processed, its sensitivity, the purposes of the processing, the actors involved and the extent with which the information is likely to be diffused.

For a consistent and accurate result regarding the risks of particular processing operations, the completion of both questionnaires is necessitated: the Easy Mode Screening is but a pre-screening apt to tell you whether you would need to undertake the extended Privacy Impact Assessment or not.

[take this questionnaire](#)

**Screening Questions**

The extended Privacy Impact Assessment includes 56 questions. The questions are grouped into five topical areas, which refer to: 1) the type of project, 2) the collection and use of data, 3) the project's storage and security policies, 4) transfer of info, and 5) cloud specific issues.

The aim of this set of questions is to assess in a granular manner how the interactions between you and the CSP you deal with impact your users' rights to privacy and data protection, and how your system is designed – if so – to prevent or mitigate the potential adverse outcomes of those interactions.

You are to answer all questions to the best of your knowledge, if necessary asking the relevant professionals in your undertaking before answering; some questions, though, allow you to answer "I do not know" (yet!), but please do mind – you are supposed to know.

[take this questionnaire](#)

**Disclaimer**

No information or content displayed in this tool should be construed, interpreted or relied upon as constituting legal advice, or a recommendation in respect of taking any course of action to comply with data protection laws, or legal obligations of any kind, and within any jurisdiction in which the European data protection law applies.

Figure 25: The starting point when using DPIAT. The user selects pre-screening or screening questions

The front page in Figure 25 contains four boxes of information; the topmost box includes a description of the tool and the possibility of selecting the provider to assess risk on, the bottom

box contains legal information and disclaimers, while the two centre boxes contain information about two different questionnaires the user might chose to use.

The questionnaire in Figure 26 contains information about the questionnaire, a progress bar, category of question, questions, help text and answers.

The Questionnaire Results in fig 27 contains an overall risk based on the answers, and allows the user to drill down into different categories to examine which risk was designated to which attribute.

**Evaluation** We have conducted a heuristic evaluation based on the pictures in Figure 25, 26 and 27. This paragraph summarizes the results from the evaluation.

### **Start Screen (Figure 25)**

- The start screen contains many elements, all given the same importance, and there is large amounts of text. Giving everything the same importance often leads to all items being perceived as equally unimportant rather than important, since the clarity is reduced.
- The wording and categorisation of this page should be reconsidered; the top box states “Please choose a questionnaire”, but the user is really being asked about which provider he wants to assess risks on. Furthermore, “Easy Mode Screening” and “Pre-Screening Questions” are both used to describe the same questionnaire – “Easy Mode” being a easier name to understand for end users, but not really describing its purpose correctly. This inconsistency might confuse the users.
- The users are given information about the length of the questionnaire and thus are able to decide upfront if they have enough time to answer all the questions.

### **Questionnaire (Figure 26)**

- The end user is given information on the scope and aim at the beginning of the questionnaire. This contributes to aligning the users expectations with what the program does and provides.
- The progress bar allows the user to have an idea of how far through the questionnaire he has come, thus giving proper context and insight into the system status.
- Help text with examples makes it easier for both end users and professional users alike to complete the questionnaire with the right understanding of the questions.
- The questionnaire looks and behaves like a normal paper based questionnaire, and thus maps to the real world – allowing the user to recognize how to use the questionnaire, rather than have to recall some instructions.

### **Report (Figure 27)**

- The report gives the user an easy overview of the risks related to his particular project, the selected cloud service provider and some information on how to use the report. This provides the user with the proper context of which the report is given.

### Screening Questions

**i** The extended Privacy Impact Assessment includes 56 questions. The questions are grouped into five topical areas, which refer to: 1) the type of project, 2) the c  
The aim of this set of questions is to assess in a granular manner how the interactions between you and the CSP you deal with impact your users' rights to privacy i  
You are to answer all questions to the best of your knowledge, if necessary asking the relevant professionals in your undertaking before answering; some questions

#### Type of Project

##### 1: Is the establishment of your activities in European territory?

Whether the processing of personal information of your undertaking takes place in the European Union or not is not relevant. If you are not established in European Union territory, but you offer goods or services to individuals in the EU or monitor them, then you should answer Y to this question.

- ☐ Yes
- ☐ No

##### 2: Do you handle information that can identify other people through one or more of the following activities?

Think for instance, if you use names, identification numbers or location data. The collection of information related to individuals can be potentially intrusive to the information privacy rights of these individuals. In some types of projects information provided is more sensitive than in other ones e.g. Financial data.

- ☐ Account and/or Subscription Management
- ☐ Advertising, Marketing and/or Promotion
- ☐ Authentication and Authorization
- ☐ Banking and Financial Management
- ☐ Charitable Donations
- ☐ Communications Services
- ☐ Customization
- ☐ (Service) Delivery
- ☐ Education Services
- ☐ Government Services
- ☐ Healthcare Services
- ☐ News and Information - Arts and Entertainment
- ☐ Online Gambling
- ☐ Online Gaming
- ☐ Payment and Transaction Facilitation
- ☐ Responding To User
- ☐ Sales of Products or Services
- ☐ Search Engines
- ☐ Software Downloads
- ☐ Site and Content Management

Figure 26: The user must answer questions about the service

## A4 Cloud Data Protection Impact Assessment Tool

### Questionnaire Results (selected Cloud Service Provider: [DataSpacer](#))

<b>HIGH</b> Risk Related to Your Proposed Application		
Sensitivity	MEDIUM	Risks related to a sensitive market (i.e. elderly, children, etc.) and/or sensitive data (i.e. health or medical conditions, finance, sexual behaviour)
Compliance	HIGH	Risks related to compliance with external standards, policies, laws, etc.
Trans-Border Data Flow	LOW	Risks related to transfer of information across national borders
Transparency	HIGH	Risks related to transparency in the areas of notice/user messaging and choice/consent
Data Control	HIGH	Risks related to control of the data lifecycle (i.e., collection, usage, quality, and/or retention)
Security	HIGH	Risks related to security of data and data flows
Data Sharing	MEDIUM	Risks related to sharing data with third parties
Risk Related to the selected Cloud Service Provider		
Usage of this Report within a Broader Data Protection Impact Assessment (DPIA) Process		

Figure 27: Upon completing the questionnaire, the user is presented with a report of the risks associated with his answers

- The overall risk is presented as a colour coded value with a prominent place in the top left corner, giving the user easy access to the risk. This allows the user to obtain the most important information at first glance at the report, just like one would place the conclusion early in a normal report – the solution thus match the real world.
- Breaking the risk down into categories, each with its own risk value and explanation, makes it easier for the user to understand the overall risk. An improvement would be to include some information on how the overall risk is calculated, as this is not clear. Is it the highest value present, the average value or some scoring algorithm based on the answers of the end user?

**Suggested improvements** Based on the findings of the evaluation, we suggest the following improvements: The large amount of partly confusing text and the equal importance given to elements of the front page might hinder a natural workflow when using the tool, which could be *Introduction*, *Select provider*, *Questionnaire* and finally *Results*. The introduction could give the user short and concise information about what the tool does and inform the user that the questionnaire has between six and 62 questions. The select provider element would allow the user to select the provider of his choice, preferably with more information than just a select box with names, as providers might have similar names. When arriving at the questionnaire screen, the user could be asked if he needs a risk assessment and be given the alternatives “Yes” and “I don’t know”. “Yes” would take him directly to the full questionnaire, while “I don’t know” would guide him through the “Pre-Screening”.

## 5.2. Cloud Offers Advisory Tool

The Cloud Offerings Advisory Tool (COAT) is aimed at helping cloud customers in selecting the right cloud service provider based on the requirements of the user and knowledge of the services in question.

Guidance will be provided to potential cloud customers on:

- How to understand and assess what a cloud service provider is offering from a privacy and security perspective
- How to compare offerings from a data protection compliance and provider accountability point of view
- How the meaning of the comparison attributes are to be interpreted

**User Interface** By the time work started on D-5.1 [2], the first version of the COAT user interface was already made, and the work therefore focused on improving the existing UI. The main UI, as implemented, is shown in Figure 28, 29 and 30.

Please indicate your requirements

What types of services do you need?

Software as a service	Platform as a service	Infrastructure as a service	Other Services
<input type="checkbox"/> Billing <input type="checkbox"/> CRM (Customer Relation Management) <input type="checkbox"/> Collaboration <input type="checkbox"/> Content Management <input type="checkbox"/> Digital Media <input type="checkbox"/> Document Management <input type="checkbox"/> ERP (Enterprise Resource Planning) <input type="checkbox"/> Emails and Office Productivity <input type="checkbox"/> Financials <input type="checkbox"/> Human Resources and Sales <input type="checkbox"/> Manufacturing <input type="checkbox"/> Order Management <input type="checkbox"/> Portals/Search <input type="checkbox"/> Social Network <input type="checkbox"/> Utilities/Management	<input type="checkbox"/> Application Deployment <input type="checkbox"/> Business Analysis <input type="checkbox"/> Business Intelligence <input type="checkbox"/> Databases <input type="checkbox"/> Development & Testing <input type="checkbox"/> Networks Operations <input type="checkbox"/> Open and Custom Clouds Platforms <input type="checkbox"/> Web Hosting	<input type="checkbox"/> Backup & Recovery <input type="checkbox"/> Communication <input type="checkbox"/> Computing <input type="checkbox"/> Infrastructure Service Management <input checked="" type="checkbox"/> Storage <input type="checkbox"/> Virtualisation	<input checked="" type="checkbox"/> Integration <input type="checkbox"/> Metadata <input type="checkbox"/> Security <input type="checkbox"/> Service-bus

Figure 28: The user is asked to select services categorised by deployment type

Figure 28 shows the list of services offered, categorized by hosting alternatives. The user might select one or multiple services.

## Advisor

### Business Questionnaire

Please indicate your requirements

**Price Range**

From: € 0 To: € 5000

**Acceptable Storage Locations including Backup**

- ☐ Europe (EU)
- ☐ United States
- ☐ Europe (Non-EU)
- ☐ China
- ☐ Local
- ☐ Any

**Acceptable Data processor location**

- ☐ Europe (EU)
- ☐ United States
- ☐ Europe (Non-EU)
- ☐ China
- ☐ Local
- ☐ Any

**Data transfer in case of emergency?**

☐

**Do you want Encryption?**

☐ Yes  
☐ No  
☐ Doesn't Matter

**Is it important that any disputes are resolved in your own country?**

☐ Yes  
☐ No

**Should unlimited backup be included?**

☐

**Notified in case of security breach?**

☐

### 8 Matched Offers

**Cirrus Thinking**

€10.00/Month

Storage Location: United Kingdom

Processor Location: Netherlands

client-side encryption

[More info](#) [Go to offer](#)

**Cloud Corner**

€50.00/Month

Storage Location: United Kingdom

Processor Location: Netherlands

client-side encryption

[More info](#) [Go to offer](#)

**Dropbox**

€7.50/Month

Storage Location: United States

Processor Location: United States

256bit ssl

[More info](#) [Go to offer](#)

**Jottacloud**

€6.00/Month

Storage Location: Europe

Processor Location: Europe

ssl

[More info](#) [Go to offer](#)

**Acceptable Data processor location**

This question concerns where personal data is processed and what laws apply to protect it. Personal data is data that relates to identifiable people. In countries within the EU, the data protection laws are similar so transferring and processing data within the EU is treated on the same basis as if you process data locally. Processing data is very wide and it means carrying out any operation or set of operations on the information or data (for example organisation, retrieval, consultation, deletion or use of the information or data).

In countries outside the EU, data protection laws are different. You should not transfer personal data outside the EU without checking whether this data will be adequately protected. This may involve getting contractual guarantees from your Service Provider that this data will be protected. If this data is not adequately protected, you may be in breach of local data protection law.

Figure 29: The user can view offers and add further requirements



After having selected the services he needs, the user is redirected to a page of offers and given the possibility to refine his criteria as demonstrated in Figure 29.

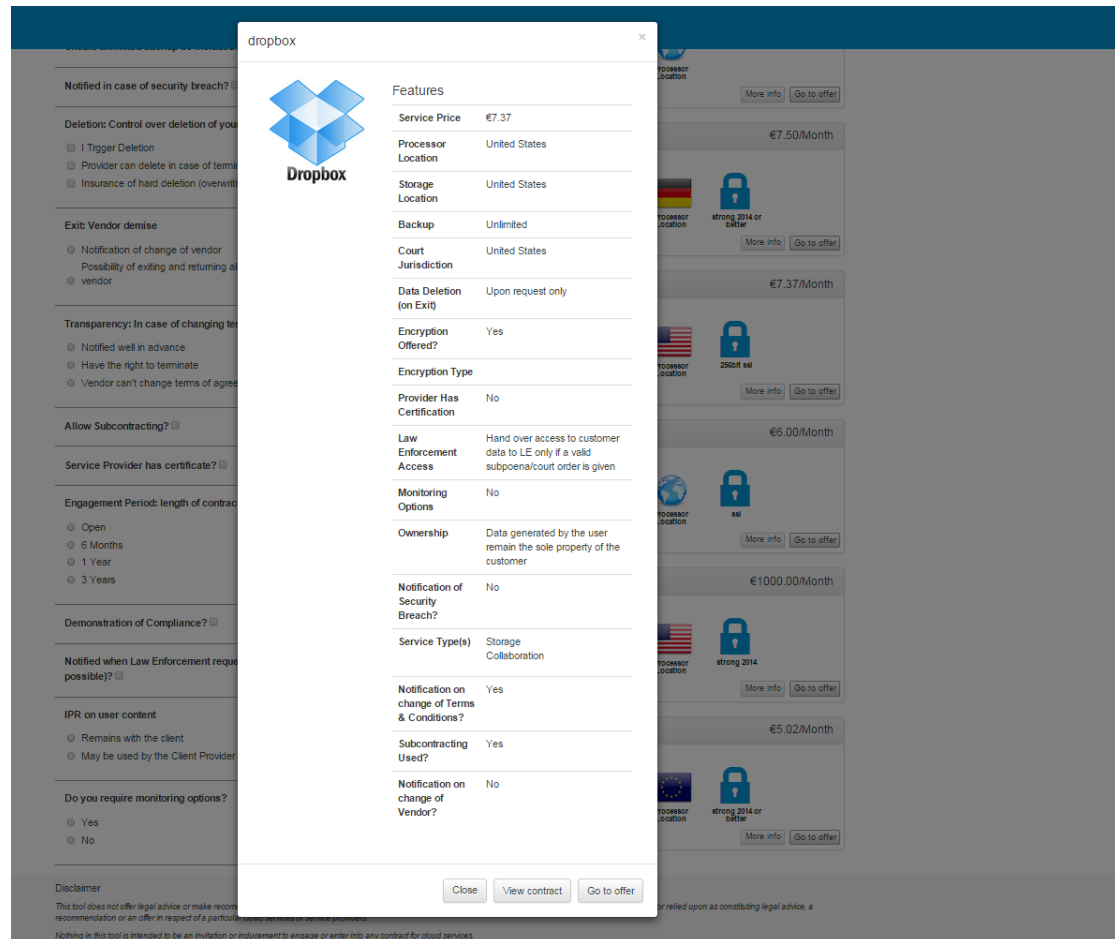


Figure 30: The user can view details of the offer

By clicking on an offer in Figure 29, the user might examine details about each service as demonstrated in Figure 30.

**Evaluation** In the context of WPB-2, documented in D:B-2.3 [10], two workshops were arranged in order to test the tool. The workshops were held in Paris and Trondheim, with 41 and 11 stakeholders representing cloud providers participating in the first and cloud customers in the second. The workshop included information about COAT and a demonstration video, before a round table discussion was initiated. We summarize the findings relating to usability here. They found the need to have different user interfaces for end users and SMEs when being asked about service type, and therefore developed the interface for SMEs to contain more information than the more user friendly page for end users. The participating cloud customers did not find the tool complex to understand and found it easy to use and learn. Most of the

attendants found the functionality useful, and some suggested adding a reputation system to rate service providers. It is important to note that the participants did not interact with the tool themselves, but rather watched a video demonstration of how the tool operates. Therefore it is possible that the results are more focused on the general use of the tool rather than its usability. More details on how the workshops were conducted can be found by consulting D:B-2.3.

In addition to the two workshops, TiU have conducted internal usability tests, and used this information to improve their demonstrator of COAT. Their findings included the cloud services list being too technical, focusing on technology rather than functionality and services needed. The questions were not considered filters, but rather an obligation.

**Suggested improvements** It is recommended that COAT implement the simplifications of the service list that we proposed in our previous deliverable D:D-5.1 [2, p. 30]. This would allow the user to focus more on functionality or need than on technology. It is also recommended to make the question about who the user is, the first question to be asked. This way it is possible to make the question “Where are you?” less confusing, as it can be worded “Where do you live?” or “Where is your business located?” Allowing the user to choose the importance of different security attributes like availability and privacy and update the offer list in real time could help the user understand how the offers are chosen.

## 6. User Interface Development for Cloud Provider Tools

Within A4Cloud, several tools have been developed to assist cloud providers in auditing and assuring systems comply with policies, construction of A-PPL policies, and handling security incidents. In this section, the user interface and evaluations of these are presented and discussed.

### 6.1. Audit Agent System (AAS)

The Audit Agent System (AAS) is aiming at helping an auditor in auditing a system or a chain of systems.

The tool will automatically audit cloud infrastructures and services for compliance with policies. The result of the audit is presented to the auditor for review. The auditor can act on behalf of a cloud customer or a cloud provider.

The users interact with the tool through a graphical user interface, which allows the user to define audit tasks, to administer audits and to view audit reports.

**User Interface** The user interface of this prototype has changed slightly during the spring 2015. It has been available for inspection by project members via a web server. Furthermore, deliverable *D:D-5.1 User Interface Prototypes V1* [2] gave an overview of the first sketches.

The initial sketches of the UI for the AAS presented in [2] are based on the descriptions of the AAS that were provided in an internal project report. Figure 31 gives an example of an early sketch of the AAS.

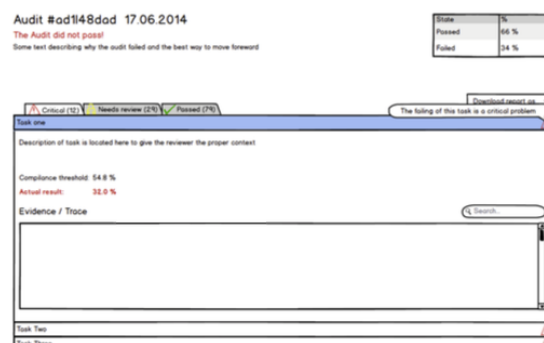


Figure 31: An example of the initial sketched of the UI for AAS.

AAS, developed at Hochschule Furtwangen, has been available to the HCI group in Karlstad via a web server. The web server that has been used for inspection is the AAS development environment. The first mockup created for the AAS evaluation was based on the actual Audit Agent System as it appeared on the Furtwangen web server (see Figure 32 for a screenshot of the web server version of AAS that were used during the development of the first mockup for the first usability test).



Figure 32: Screenshot of the original AAS UI used for the mockups in the first test session

The next iterations and mockups were instead based on the recommendations from the previous test iterations. To see a screenshot from one of the mockups used in the third and final evaluation, see Figure 33.

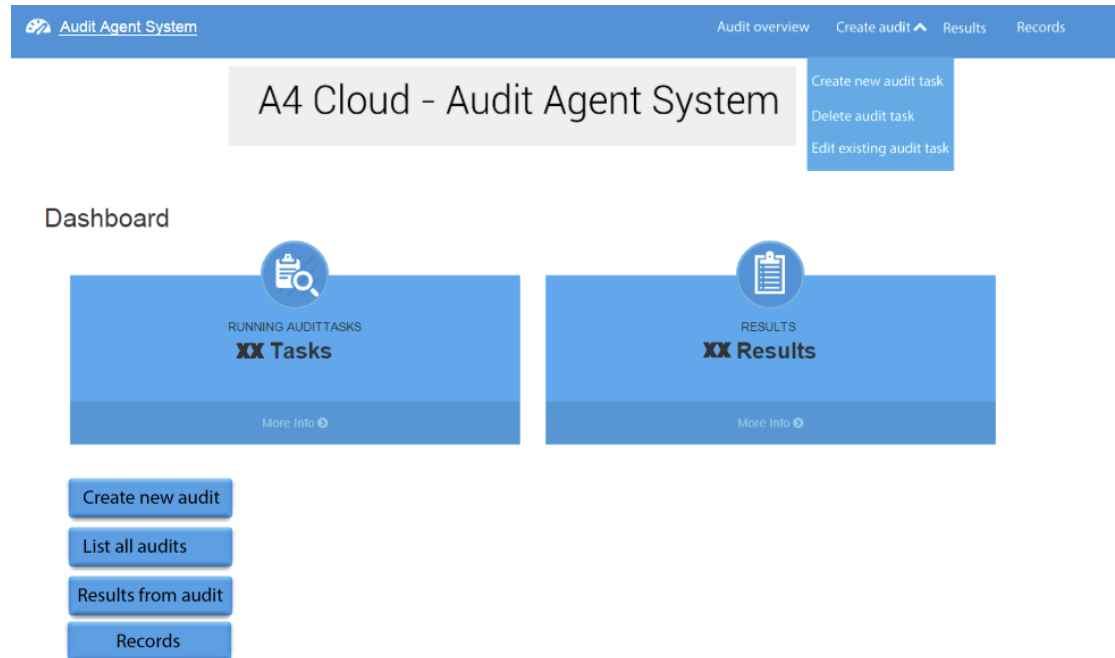


Figure 33: Screenshot from one of the mockups used in the final test iteration

**Evaluations** In an iterative design process, three slightly different versions of the User Interface have been evaluated with expert users concerning intelligibility and available functions. This process has been conducted on interactive mockups in order not to disturb the work of the AAS developers. Thus, the web version has not been directly used. This has made it possible for the UI evaluators to experiment with parallel designs simultaneously. Feedback has been given continuously to the AAS developers and also after each of the three UI evaluation cycles. Similarly, feedback has been provided by the AAS developers upon requests from the UI developers. The UI developers have had several questions regarding different tasks, scenarios and the workflow of the system which all were commented with the feedback by the AAS developers. The AAS developers also made a video presentation of the AAS system to the UI developers, in order to add to their knowledge and understanding of the AAS system.

The usability test sessions conducted in this evaluation have been carried out in the following manner: Participants were sought among system administrators, security experts, and data auditors. Each of them participated in one (or in some cases two) out of the three test iterations that were arranged (in total 13 sessions were conducted; 10 unique participants). The Wizard-of-Oz technique ( 1.2) was used to evaluate a mockup of the user interface by letting test participants interact with the feigned system and perform some tasks.

In the first and second test iteration, each test session was followed by a walkthrough of the mockups where the test participants were asked some questions about their perception of AAS, and they were also given the opportunity to comment freely on the AAS. In the third iteration, a post-test questionnaire was used instead of a walkthrough. Because the third test iteration

aimed to evaluate which of two versions of the UI was more suitable, only a few questions regarding the differences in the two versions and some open questions about the participants' general perceptions of the AAS were enough to fulfill that purpose. A few of the last test sessions in the third iteration were conducted via Internet (Ozlab and Skype). Each session lasted about 30 minutes, with 5-10 minutes on solving the tasks, and the rest of the time on the walkthrough and post-test questionnaire.

When the mockup imitating the UI of the AAS prototype was ready for inspection, a pilot test was made with a lab assistant from the university's usability lab. This resulted in changes in how the interactive mockup was structured, some links were rearranged and some interactions were automated. This was done in order to ensure a seamless interaction with the system for the participants. Prior to the second and third test iteration no pilot test was conducted since the alterations were so small that no re-structure was necessary. In the third test iteration, prior to the tests conducted at a distance, a pilot test was conducted in order to prepare the moderator to the "new" way of conducting the tests (presented further below).

Below follows an account of the research questions for each iteration of the evaluation of the mockups used in the test iterations (the mockups of the AAS does not exactly reflect how the actual development of the AAS UI progressed). The mockups of the AAS UI were re-designed before each new test cycle based on the recommendations from the previous test cycle (the first mockup used in the first test iteration was based on the actual AAS UI, available on the web server explained above).

### **Iteration 1, N = 2 (number of test participants N = 2)**

The questions asked for the first test iteration were quite general:

1. Is all relevant information available in the system?
2. Is all information available in the system relevant?
3. How quickly can users perform common tasks?
4. How closely does the flow of the system reflect how the user thinks of the work flow?
5. How easily and successfully do users find the functions or options they want?
6. What are the major usability flaws that prevent users from interacting with the system in the way the users want?
7. How can the AAS-system be improved?

Two test subjects were sought at Karlstad university and consisted of experts from the Computer Science Department at Karlstad University in Sweden.

The results from the first test sessions indicated that the content of the AAS is sufficient and good although there is room for some improvement. For example, the tests showed that the test participants had some troubles in knowing where in the system they were because of the lack of indications on the links that the user navigates through e.g. highlighted or underlined. The tests also showed that the icons used in the system deviate from what the test participant

had expected. For instance, a wrench-icon is used to represent a Dashboard-page, while the test participants thought this icon signified Settings or Configurations. Five specific recommendations were given for further evaluation in the next test iteration.

The first test iteration had a lot of similar characteristics as a *expert review*. Domain experts, in this case, experts on Access Control Rights and Access Rule Sets were presented to the AAS prototype, one screen at a time until the whole prototype was covered during which they evaluated it based on their prior experience and knowledge. The results from the first two expert reviews yielded so much data, that it were considered sufficient to make recommendations for the next test iteration.

### **Iteration 2, N = 3 (number of test participants N = 3)**

The mockups for the AAS UI were re-designed for the second test iteration to incorporate the five specific recommendations from the first test iteration, four recommendations were about the mockup and one was about how to introduce the participants to the test. The overall evaluation questions were the same as in Iteration 1. The tasks given to the test participants were:

1. Edit the audit task Apache access log monitoring for the Web traffic policy.
  - a) Change the audit type to “Continuous”.
  - b) Change the container to “CardioMonService”.
  - c) Fill out the Log file path with whatever you think is appropriate
2. Run the Audit task.
3. Check the results for the audit and answer the following questions:
  - a) What is the ActionID for the violation?
  - b) What were the “Violated rules”?
  - c) At what time was the violation detected?

In this iteration three subjects were chosen from the IT services unit of Karlstad University instead of from the Computer Science Department. One was the IT Security Coordinator with a lot of experience of manual auditing of logs. The two other test users were software developers with experience of in one case access rights and manual auditing, and for the other case log management, firewall rule sets, and wireless access rights. This round showed that the alterations made from the first usability test turned well out because no test participant commented on the design of the GUI during the second pilot usability test. The most evident results from this test were that the participants asked for a more interactive dashboard, with the ability to get a better overview of the status without having to navigate to the Results tab or the Audit overview tab. It is also evident that the participants had a hard time to tell Save from Submit, or at least, to tell the different meanings of the two terms.

### **Iteration 3, N = 8 (number of test participants N = 8)**

This third iteration compared four slightly different variants of the UI of the AAS system based on the recommendations from the two previous test iterations. Because the second test iteration concluded with a set of recommendations including alternatives, four different variants have been developed for this third test iteration.

- Which of the UI alternatives are perceived as the preferred one by the participants?
- Which of the UI alternatives are evaluated to be most usable?
- What are the strengths and weaknesses of each UI alternative?
- How can the AAS-system be improved?

Each test participant only tested two of the four alternatives, and the alternatives (and the order in which they were encountered) was balanced on the two sets of test participants, which were system administrators and data auditors, respectively.

Table 3 presents the test participants and the order in which they were presented the different alternatives.

Group 1 - Auditors		Group 2 - Sys. admins	
TP#	Sequence	TP#	Sequence
1	A, C	2	B, D
5	C, A	3	D, B
6	A, C	4	B, D
7	C, A	8	D, B

Table 3: Participants and the order and sequence of their respective test sessions.

These eight persons were given five tasks with some subtasks as in iteration 2 (see above) with two additional ones to see if test subjects would understand that the menu alternatives for several of the menus directly reflects the categorization of audit tasks, and one extra question to see whether they would use the “Record” menu to search for old audits:

0. How does the categorization of audit tasks (policies) look like in the Audit Agent System?
4. Is it possible to get old audit results in Audit Agent System?

The results from the third iteration were in essence that the small differences between the four variants did not matter. Menus introduced already in the original prototype UI and changed during the mockup evaluations, were not used but instead 6 of 8 participants preferred to use the buttons that now had been introduced in the AAS dashboard. (The dashboard in Figure 33 has not been endowed with a frame around it, and one might as well skip the label “Dashboard” but such a decision is depending on whether such a term would make it easier to refer to the group of controls in some help file or other tool.)

For all 8 subjects, the first task was difficult in the first round. In the second round everything went smoothly. Thus, a conclusion is that it is quite easy to learn the purpose and means of



the AAS through any of these UI proposals A, B, C, and D (Figure 33 shows what is common to B and D), but menus are not as essential as buttons. Almost everyone asked for tooltips or other kinds of help, and this should of course be provided in a future version of the tool. Other solutions are also possible such as providing more buttons, which would make alternatives visible, and organising controls according with work-flows. To be convincing, the last suggestion would need very definitive and complete use scenarios rather than something that fits only a few scenarios presented within A4Cloud project.

## 6.2. Accountability Lab (AccLab)

The Accountability Laboratory (AccLab) tool is aimed at helping cloud customers creating abstract accountability obligations in Abstract Accountability Language (AAL). Based on these AAL policies, AccLab generates A-PPL policies that can be enforced by A-PPLE.

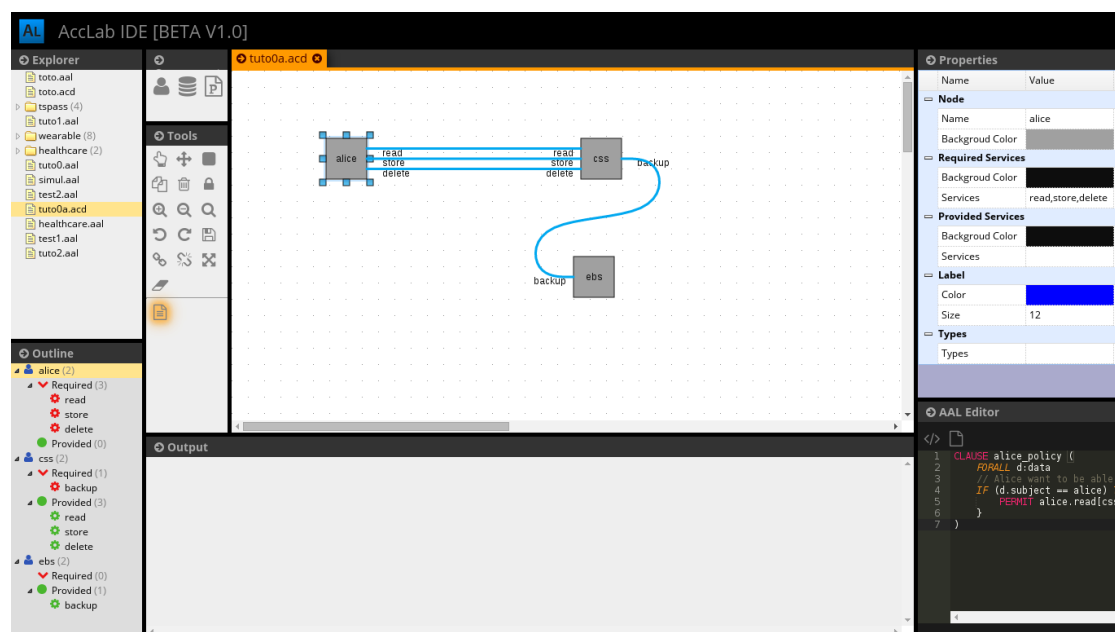


Figure 34: The interface of AccLab as implemented

**User Interface** Figure 34 shows the user interface as created by the tool developer. This was developed before work started on D-5.1 [2]. In D-5.1, we therefore designed a wizard to make it easier to create policies in AccLab.

Based on Figure 34 we created a mock-up suggesting an improved organization of the layout for the entire editor. This is shown in Figure 35. The mock-up restructures the tool to have fewer nested panes of actions and information, it also makes the AAL editor less prominent.

Based on our mock-up in Figure 35, Julie Spens, Pierre Teilhard and Anqi Tong – students at Mines Nantes – then created the sketch in Figure 36 on how they would improve the UI of AccLab. Compared to the current version of AccLab, as can be seen in Figure 34, the most

## D:D-5.4 User Interface Prototypes V2

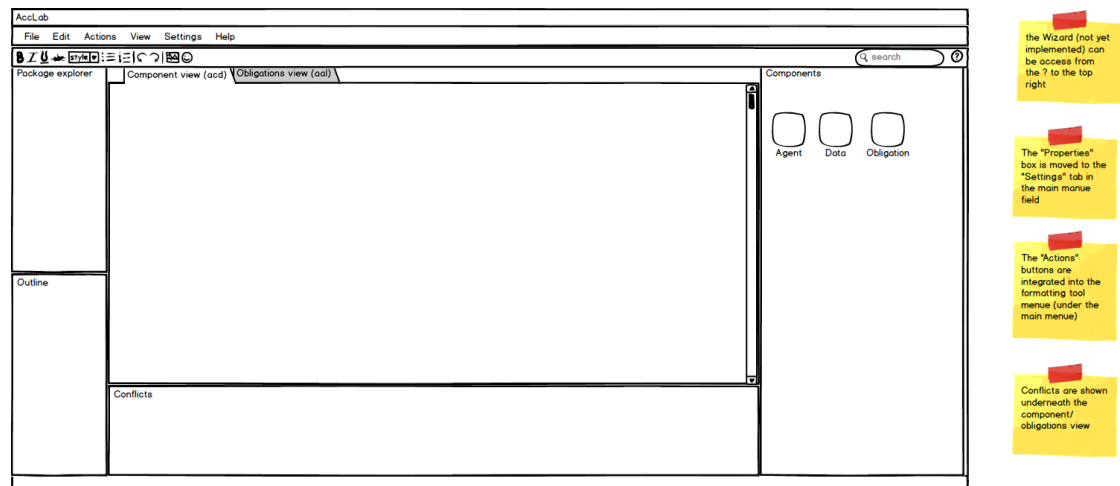


Figure 35: Mockup demonstrating how to clean up the interface

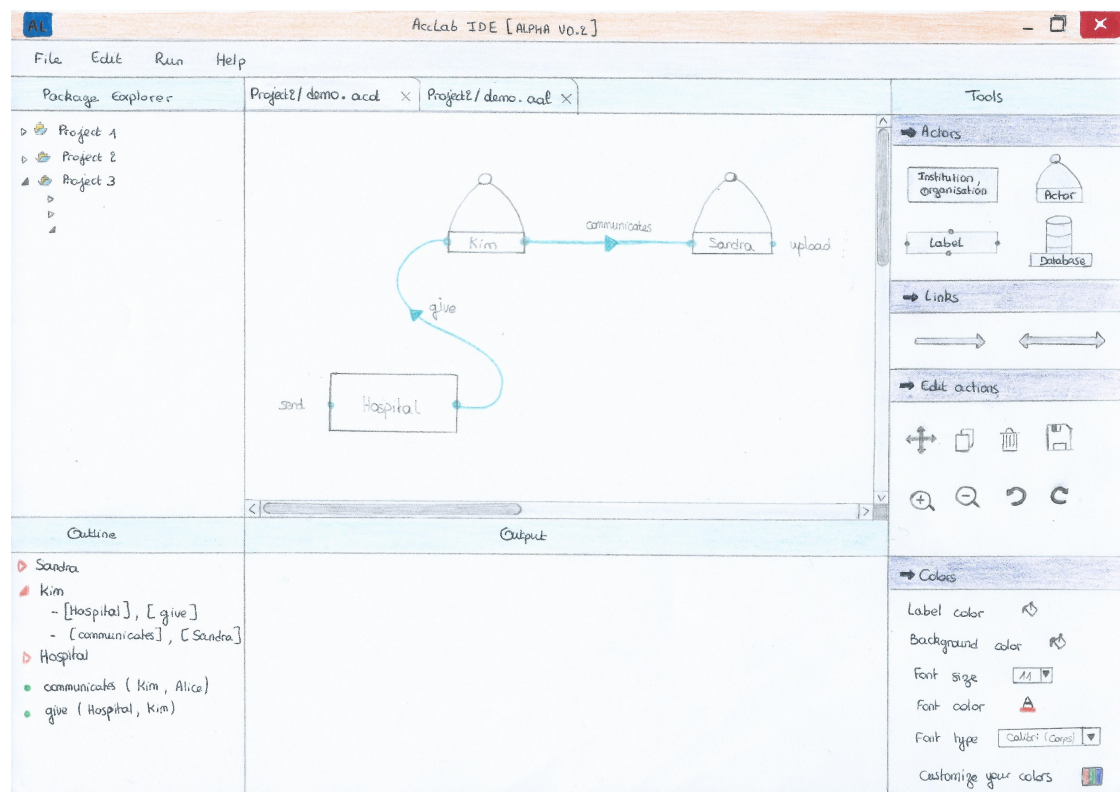


Figure 36: Updated UI for AccLab by students at Mines-Nantes

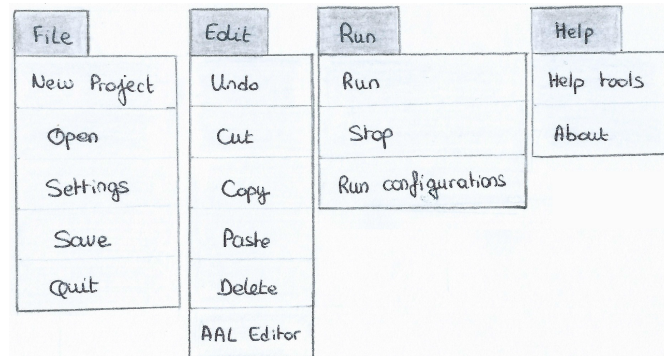


Figure 37: The Web Application Menu for AccLab by students at Mines-Nantes

apparent changes are the restructuring of tool pane placements and improved organization of available tools. There are also some changes with regard to how relations between entities are represented. Figure 37 displays the Web Application Menu envisioned for AccLab.

The elements of the UI are a package explorer pane, an outline pane, an output pane, a policy canvas and a tool pane. The outline pane gives an overview of the actors and relations on the policy canvas. The tool pane contains the actors and relations used to draw a policy on the policy canvas, as well as several options for formatting and editing the policy canvas.

**Evaluation** We conducted the evaluation as an expert evaluation, examining the prototype image in Figure 36.

- The web interface looks a lot like an integrated development environment (IDE) – which might be good for those familiar with such development environments, but also be seen as complex for those not familiar with them.
- The File/Edit/Run/Help menu in Figure 37 is rarely seen in web applications. Some tools, such as Google Docs, use Web Application Menus, but they should be used with caution, unless one need space for a large amount of commands. In the guidelines by the Web Accessibility Initiative guidelines [12], they stress the importance of the Web Application Menu working in exactly the same manner as the desktop menu it tries to emulate – both in behaviour and interaction.
- It is not clear what "Run" means. It might be a bit too IDE-generic, and could preferably be replaced with very specific commands in terms of what AccLab can do like "Generate AAL policy" if this is what should happen.
- Figure 38 shows the colour options of AccLab: change label colour, background colour and some text options, which are not strictly colour options. If colours do not carry any particular semantics, they are probably not that important – and could make the model more confusing if the meaning of different colours is not made explicit.

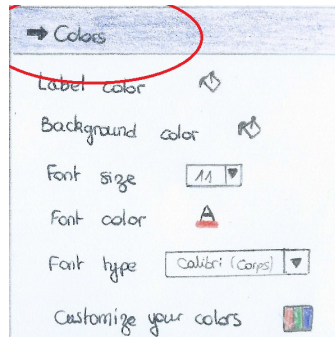


Figure 38: Color options in AccLab

- Does the tool store the user's policies in a data store, or does the user have to upload a policy to edit and download to save? If the policies are written to a data store, a sign out mechanism should be available for the user as he would have to sign in to access the data store.
- Zoom and move has been placed in the pane titled *Edit actions*, although they presumably do not edit the policy (fig. 39). This might cause confusion and extra work for the user when looking for these tools. Additionally it might induce discomfort or uncertainty for some users when only planning to view – not edit – policies, as the placement of the zoom and move tools indicate that they do edit the policy.

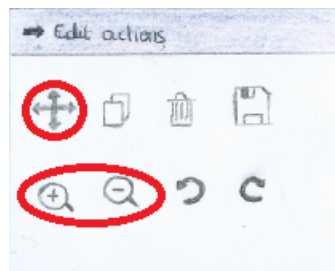


Figure 39: Edit actions in AccLab. Move and Zoom buttons highlighted with red circles

- For the institution/organization actor in the tool pane, only one name should be chosen in order to avoid confusion
- Labelling all actors with a graphical element would aid users so they do not need to read the text, and the diagram would be more readable outside the tool. Figure 40 shows how this is done by e.g. ArchiMate® [17].
- When a component is selected in the outline, it should also be highlighted in the editor as exemplified in Figure 41 – this would allow the user to learn how the two panes relates to each other as well as making it easier to locate an element in a large diagram.



Figure 40: An example from the ArchiMate<sup>®</sup> 2.1 specification on how to label actors graphically – here, a location is displayed

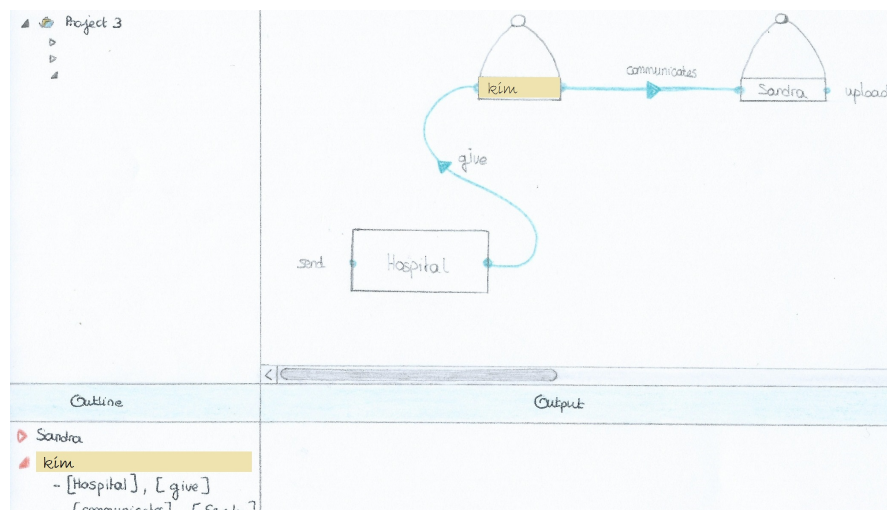


Figure 41: An example of the correct actor being highlighted in the editor when hovered or active in the outline

**Suggested improvements** While the sketches provided for evaluation in this document is a step in the right direction for usability of the user interface in AccLab, it is still recommended to implement the policy creation wizard described in [2] in addition to the remarks from this evaluation.

### 6.3. Incident Management Tool (IMT)

The Incident Management Tool (IMT) is aimed at helping cloud service providers in handling anomalies and detected violations in cloud environments. Instances of IMT are capable of sending and receiving incident reports from each other through subscriptions, thus allowing each link in the cloud delivery chain to be informed about relevant incidents. When the IMT receives an incident report, an operator can create a local version of this incident report (which belongs to another entity) and notify end users through the A-PPL-Engine and possibly other instances of IMT subscribing to this new incident.

**User Interface** The Incident list is the centre of IMT, as this is where the incident handler gets an overview of the incidents in need of attention as well as his starting point for actually handling the incidents. Figure 42 shows how such an incident list could look and how it is implemented in IMT at the moment. The UI outline of the application has three areas:

- The blue bar on top gives the user access to messages, alerts and profile management
- The dark sidebar gives the user easy access to all the features of the tool
- The light grey area is where new content appears on each page

The Incident list in Figure 42 displays information about incidents, in order to help the incident handler to prioritize which incidents to handle first. Both state and impact are colour coded, in order for the incident handler to easily get an overview of which incidents are resolved and which are not, as well as the degree of impact of each incident. The impact of the incident is a high level method for prioritizing the order in which to handle incidents, even though relying solely on that value means fully trusting the judgment of another incident handler – potentially at another organization with another infrastructure and different threat situation.

Adding an incident is shown in Figure 43. Adding incidents is done through a simple form, where the fields are grouped and placed in their order of significance. First, the handler needs to select the incident type, as the custom fields are decided by which incident type is chosen. Thereafter, the status of the incident is added, which in most cases is likely to have the value of unresolved when the incident is first added. Going on, the handler estimates the impact of the incident. Having provided this basic information, the handler is ready to create a short summary of the incident, before entering all the details necessary into the description field. At the bottom of the page, he is also able to enter information into custom fields associated with the incident type. The right hand side of the screen holds meta information about the incident: when it was detected, when it occurred, the language in which the report is written and the assigned provider liaison between the provider and the customer.



Summary	State	Impact	Type
Service 1 has slow response time due to DDoS	Unresolved	Medium	DDoS
Database storage has been breached	Resolved	High	Data breach
New version of Nginx fixes vulnerabilities	Unresolved	Medium	Configuration
Extensive port scanning of our infrastructure	Resolved	Low	Probing

Figure 42: The incident list provides some basic information about incidents, as well as indicating each incident's status

Figure 44 shows the detail view of an incident, in which the incident handler is also able to add and manage attachments. The two column layout holds multiple boxes of information and actions. The top left box contains information about the incident itself. The bottom left box holds attachments as well as allows the handler to add new attachments. Attachments are of predefined types in order to ease their handling. Above the attachments, custom fields and their values are shown, if the incident type has any associated custom fields. The top right box presents information about who has the lead on the incident in question. This is very important in order to avoid situations where different people believe someone else is responsible and the incident is never handled. By designating a specific lead for the incident, and giving this information a prominent place in the incident tracker, all involved can be sure that incidents are handled and by whom. This does not mean that the lead needs to work on the incident alone, but rather that he is responsible for the incident and its activities. The next box presents information about the incidents liaison - the person to contact if more information is necessary, to provide more information or any other matter. In this case it is a support centre, but it might just as well have been a specific person. E.g. for large customers it could have been their designated contact in the provider's incident management team.

The box titled *End user notifications* contains a list of notifications that have been sent to end users, who have been affected by this particular incident. The tool operator is also able to send new notifications to the end users by clicking on the *Send notification* button, at which time he will be asked to write a message to the end user about the incident at hand.

The bottom right box holds the actions available to the incident handler. He is able to update the information in the incident and notify the subscribers if the incident is created by his organization. If the incident is received, the incident handler needs to derive it - create a new incident based on the received one – before being able to notify subscribers. When a handler presses the button *Notify Subscribers*, all subscribers that subscribe to a notification involving the incident type and which fulfils the defined triggers, will be notified.

The image shows a user interface prototype for adding a new incident. The interface is divided into several sections:

- Incidents** (Add new): The main heading for the form.
- Incident Details**: A section containing three dropdown menus:
  - Type**: Set to 'DDoS'.
  - Status**: A dropdown menu with a placeholder '-----'.
  - Impact**: A dropdown menu with a placeholder '-----'.
- Summary**: A large text area for summarizing the incident.
- Description**: A large text area for describing the incident.
- Incident Meta**: A section containing three dropdown menus:
  - Language**: A dropdown menu with a placeholder '-----'.
  - Occurrence time**: A date/time picker with a placeholder '-----'.
  - Detection time**: A date/time picker with a placeholder '-----'.
- Liaison**: A dropdown menu with a placeholder '-----'.
- Actions**: A section containing a **Save** button.
- Additional Information**: A section containing a checkbox labeled **Reported to Police**.

Figure 43: Adding a new incident is done by filling out a simple, customizable form



1

0

Ola Nordmann

Incidents

Details

Service 1 is down

**Origin**  
Amazon AWS

**Status**  
Unresolved

**Impact**  
1.00 - High

**Type**  
DDoS

**Language**  
English

**Description**  
Service 1 is under heavy load from a large international botnet. We are actively working on blocking the nodes in question while scaling our infrastructure to meet our customers needs.

**Occurred at**  
April 29, 2015, 2 p.m.

**Detected at**  
May 6, 2015, 2 p.m.

Additional Information


**resources** ⓘ  
["country"]

**users** ⓘ  
["testuser"]

Attachments

- (iodef)

Add attachment




INCIDENT LEAD  
Ola Nordmann

Liaison

**Name**  
Company X Support Center

**Email**  
support@test.com

**Phone**  
21492350928



SUBSCRIBERS HAVE NOT BEEN NOTIFIED

Notify Subscribers

End user notifications

No notifications have been sent to end users

Send notification

Actions

Update Incident

Derive Incident

Figure 44: By opening an Incident, the handler can examine all related information. The image shows a received incident

FP7-ICT-2011-8-317550-A4CLOUD

Page 77 of 106

Figure 45 shows the right sidebar for an incident that is created by the organization to which the incident handler belongs. The indicator shows that all subscribers have been notified about this incident. If the content of the incident is changed, the indicator changes as well. Figure 45 also shows how the indicator looks when subscribers have not been notified at all, or the incident has been changed since the last notification. The incident handler is now presented with a button to notify the subscribers. After subscribers are notified, the indicator goes back to green state.



Figure 45: Shows how the right side bar of the Incident Detail view looks, when the incident originates from the organization in question and the incident handler is allowed to send notifications without first deriving a new incident

Figure 46 shows how the incident handler can get an overview of the incident type as well as the connected notification triggers that a subscriber might choose to activate. The top left box gives details about the incident type, while the middle left box lists the associated trigger types. Bottom left, the incident handler has access to decide which custom fields should be available for this particular incident type. From here, the incident handlers are able to modify the incident type and add, edit and remove trigger types as well as custom fields.

Figure 47 shows the information included in a notification subscription. In the upper left box, information about the subscription is presented: name, linked subscriber and endpoint for where to send the notification if triggers are fulfilled. In the bottom left box, incident types are listed using a card view. Incident types can be added, modified, and removed. For each incident type, the incident handler might add triggers from a list of predefined possible trigger types associated with each incident type. The triggers are displayed in-line in the incident type card, using a table to display the information. It is also possible to edit the trigger from the list.

**Evaluation** Focused interviews were conducted to test the workflow and user interface. By catalysing the focused interview with a practical session, the participants have already been exposed to the prototype and the concept. This was done to facilitate shorter and more focused talks about the subject at hand, which resulted in more effective interviews – allowing for the total session to take just over an hour per participant. Due to the early stage of conceptual development, only two participants were interviewed. They were experienced in their respective roles, an incident response team leader and an information sharing officer. Both worked in large Computer Emergency Response Teams (CERTs) with responsibility for entire sectors. One organisation has experience both as a cloud provider and cloud customer, while the other has a more supervisory role. In both organisations, different incident management ticket systems are already in use, and the participants are well acquainted with such tools.

The participants were given some tasks to solve by interacting with the tool, while speaking

1

3

Ola Nordmann

Incident Type

Details

DDoS

**Description**  
A large number of connections with the goal of making the page unavailable

**Consequence**  
1,0

Trigger Types

Name	Description	Comparators
Ping time <div>Delete</div>	The time it takes a small network package to reach the service and the service to respond	>, <

Add Trigger Type

Custom Fields

Name	Description	Type
IP-address <div>Delete</div>	The IP-address of the main perpetrator	string

Add Custom Field

Actions

Update Incident Type

Figure 46: By opening an Incident Type, the handler might examine all related information

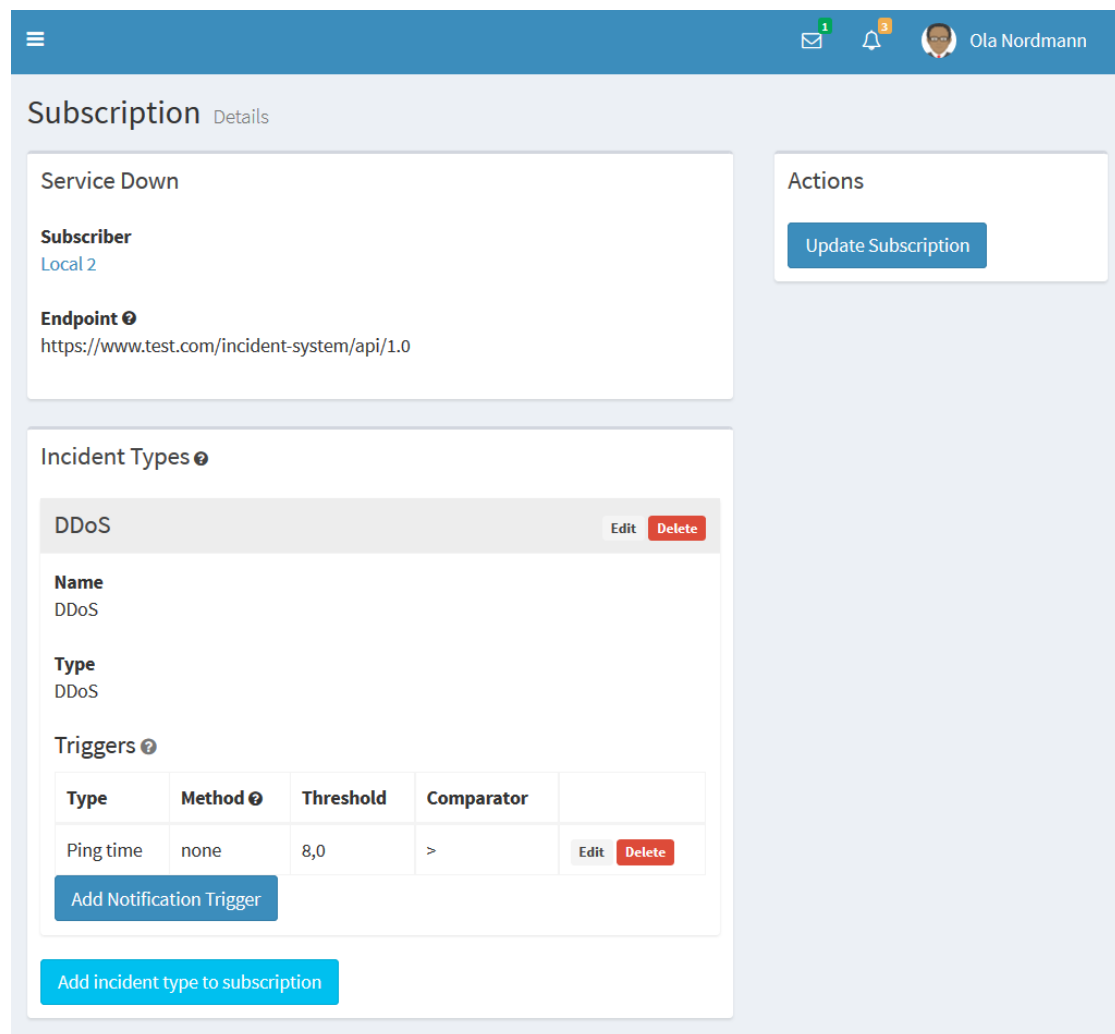


Figure 47: Each subscription can be examined and new triggers added

out loud all thoughts with regard to the process. The participants had the following remarks with regard to the user interface and workflow of IMT:

- The use of colour coded statuses in the incident list, as can be seen in Figure 42, was said to devalue the colour codes used for impact. In addition the multiple colour coded labels per incident clutters the user interface.
- The user interface does not make a clear distinction between local and received incidents, and one participant therefore wondered which organization the status field applied to. If it was resolved, was that for his organization or from the perspective of the sending organization? Furthermore, in his view, the local incident would often be resolved after forwarding information to customers, but this would not necessarily be the case for the provider which sent the incident notification as he would have to solve the root cause of the incident.
- It would be preferable if new incidents were added to a queue, and when an incident has been handled, it is removed from the queue. This results in less information the incident handler has to browse in order to find what is important at that time. It is also important to know the internal state of the incident, like who is working on it, what has been done, which information has been provided to the customer, etc. The workflow of such a tool is crucial, as usually an entire team is working on an incident. Updates to an incident, from the provider, must be added to the original incident in order to avoid extra work.
- Powerful search and filtering options, as well as the possibility of tagging incidents for easy retrieval at a later stage is important for such a tool to be productive. In addition to organizing incidents in a parent-child system, tags can be used to create sibling incidents. A main incident ticket could hold hundreds of children, and in such situations graphical illustrations of the relationships are useful.
- One participant expressed a desire to know from which reporting channel an incident originates. E.g. was it reported by phone, email, etc. He was also interested in knowing who reported the incident to the organization from which the incident originates.
- There is a need to be able to send a derived incident with another incident type than that of the received incident. E.g. the incident handler could receive an incident about DDoS, but to his customers it would only be a reduction in quality of service.
- Received incident information should be marked using the Traffic Light Protocol (TLP) [35] [13]. The TLP indicates with whom the receiving party is allowed to share the received information. E.g. only the receiving person is allowed to view the information, the CERT, security people, etc. Furthermore, it was stressed that in the absence of TLP indications on the incident information, the operator would have to contact the sender to obtain permission to share specific information like the IP-address of the main perpetrator. He might send a general message to his customers about the problem, then obtain permission from the sender, and finally update the information he provides to his customers. If the entire incident, or parts of the incident, were marked with TLP, he would not have

to do this extra work, but could act according to the TLP classification. One participant would also like to see who receives the notification before actually notifying.

- The underlying notification system in IMT should build on, or be integrated with, the organisations existing incident management system. This close connection is needed in order to avoid doing extra work, like adding the same information twice and updating incidents in two different places. They have some email notifications integrated in their current incident management system, allowing easy notification about simple incidents. Recipients are subscribed to different email lists, allowing the organization to send notifications to the relevant personnel.
- The IMT should be able to receive emails directly into the system. This would provide the proper traceability for information as incident handling is mainly about communication.
- Local incidents, derived from received incidents, should only be visible from the parent incident.
- One participant would normally reply to the incident report sender and inform him that the information has been passed on, after having sent a derived incident to his own customers. Sometimes he also asks if there are more information to be shared. He would also have used this functionality to request more information about how the relevant information was obtained, in the example of receiving an IP-address he would normally ask about how this was obtained if such information was not provided. He is used to all communication being integrated into the incident management tool, allowing external communication to be done in-line. He points out that this might become a problem if the provider receives several thousand replies, and therefore suggests to include a comment section instead. Comments could be seen by all receivers of the incident or just the provider. The provider could then decide which comments to reply to, and which questions they decide to answer.

**Suggested improvements** Based on the results from the evaluation, we propose the following items to be changed in the next iteration with regard to the user interface:

- Change IMT to imitate help desk software with ticket queue
- Replace colour on status with a more subtle icon in order to retain value of colour coded impact
- Add search and filtering options
- Clarify the distinction between local and received incident

## 7. Suggestion for Scenarios in Workshop Evaluations of the A4Cloud Demonstrator

The document D:D-7.1 describes the first attempt to instantiate the A4Cloud Accountability Framework. D:D-7.1 concludes by “Following this version of the prototype, the project aims for an intermediate user validation of the application of the A4Cloud framework and tools in the wearable use case. The results of this validation phase will join up with the work planned for the final prototype.” This chapter relates to that deliverable by briefly describing the *Demonstrator* defined there and its general demonstration scenario. The purpose of this chapter is, however, not to expound on the full scenario but instead suggest short scenarios that can be used in evaluation workshops where representatives from single stakeholder groups participate. Such targeted scenarios will improve the evaluation and refinement of user interfaces as well as of workflow descriptions and of A4Cloud functions.

### 7.1. Short description of the A4Cloud Demonstrator

The Wearable Use Case has been designed to demonstrate the accountability framework and tools developed by the A4Cloud project in a real life example of a cloud service chain. The use case is meant to constitute a realistic and topical scenario in which the involved business actors have to take the appropriate actions to ensure that the collection and processing of personal data are handled responsibly, based on the established regulations and the declared security organisational policies.

The scenario has been elaborated from the perspective of *Wearable Co*, a company that aims to build a web-based application for offering wellbeing data analysis services to their customers. The Wearable Application gathers, manages, and stores personal data of people wearing a certain physical device (“the wearable”). Thus, it is possible to keep track of their health status over time. The aim is the preserved and enhanced wellbeing of the users of the wearable. The wellbeing-related information integrates real time data that are recorded by the wearable devices provided by the Wearable Co and transmitted through the communication interface of these devices to the cloud-based Web application. Then the wearable users can track their wellbeing data, receive wellbeing recommendations, and visualise aggregated wellbeing statistics on interactive maps.

The Wearable Use Case includes four types of user. We copy a list from p.9 in D:D-7.1 but add abbreviations within brackets for these four types according to p. 70 in the same deliverable (see next section):

- The Cloud Subjects (I =Individuals), who are the customers of a company offering a service which utilises cloud resources (Cloud Customer). A Cloud Subject and the Cloud Customer interact with each other, during the following accountability paths: agreement, reporting and demonstration.
- The Cloud Customer (E = Experts), who establishes a business relationship with a Cloud Provider for processing personal data and business confidential information as part of its service provision. These actors interact during the following accountability paths: agreement, reporting and demonstration.

- The Cloud Provider (P = Providers), who on its own or in collaboration with other Cloud Providers provides the necessary resources for processing personal data and business confidential information. These actors interact during the following accountability paths: agreement, reporting and demonstration.
- The Cloud Auditors and Supervisory Authorities (A = Auditors / Authorities), who are responsible for performing external verification and compliance checks towards cloud providers and customers. These actors interact during the demonstration accountability path.

Acting in the instantiated use case are Wearable Customer (I), Wearable Device (a thing), Wearable Co (E), Kardio-Mon (P), DataSpacer (P), and Map-on-Web (P) as depicted in Figure 2 in Chapter 2 (cf. D:D-7.1, p. 12) and also auditors (A).

### 7.2. Targeted scenarios for hands-on demos

The Demonstrator focuses on four different categories of stakeholders (D:D-7.1 p.70, from the evaluation planning chapter), namely:

- (E) Business and security experts, who act as cloud customers;
- (I) Individuals, representing the non-ICT skilled end users who share data to the cloud;
- (P) Cloud providers, representing the cloud service and infrastructure vendors, who conduct their business in the cloud;
- (A) Auditors and Supervisory Authorities, representing the regulatory community, who define policy framework on data protection and are responsible for enforcing cloud service and data protection rules.

The Demonstrator can be evaluated in different ways. Hands-on demonstrations, where stakeholder representatives can experience tools by interacting with them, can result in feedback from stakeholders groups on how tenable the presented scenario is and how useful the interactive tools appear to be in addressing practical problems within the scenario and for similar tasks in other courses of events. In order to evaluate the Demonstrator by hands-on demos before putting questions to the participant, we suggest that different scenarios be developed for each of these four categories. Still, a full scenario should not be left outside of the picture, for instance as an animated video. This should provide a coherent realistic example that drives the involvement of the different stakeholder groups through the smaller scenarios suggested below. But, possibly, the design of the full scenario could need a special version for the individual data subjects ((I) above) as such users cannot be supposed to have the same understanding of legal and business factors as the other groups.

In order to be able to evaluate with individual stakeholder representatives, the scenarios furthermore have to be separated from each other; i.e., there should not be any need for actions from representatives of any of the other stakeholder groups. Otherwise a multi-stakeholder focus group would have to be arranged every time a hands-on demo is made.

The sections will present short scenarios targetting each of the stakeholder groups.



### 7.3. Scenario 1. Cloud Customers' business and security experts (E)

In this scenario, based on combining 4.2.2 and 4.2.1 in the deliverable (D:D-7.1), Wearable Co as a cloud customer is looking for a new cloud SaaS provider who will take care of the provision of a cloud service for Wearable Co concerning content processing and cloud storage requirements. To do this they use the A4Cloud tools Cloud Offerings Advisory Tool (COAT) and Data Protection Impact Assessment Tool (DPIAT).

1. First the cloud customer launches the COAT-tool (the person doing this acts in the role of the delegated privacy officer of the cloud customer).
2. The cloud customer then gets to fill out the requirements they have on the new cloud provider: in this case they need, for example, Content Management, Storage and Integration.
3. Based on the requirements, the cloud customer is presented with a list of suitable cloud providers. Now the cloud customer has the opportunity to make a narrower filtering among these cloud providers by specifying certain geographical locations for data storage, backup, processing of personal data, encryption and so on. Since the requirements of the cloud customer involve services offered by third party providers (e.g., the Storage is provided by an IaaS), this should be explicitly referred in the offered features pane.
4. When the cloud customer has done all the specific customisations there will hopefully be one or more matched offerings. The cloud customer now makes the decision on which cloud provider to choose.

After the cloud provider is chosen, Wearable Co now wants to assess the risks of their selection of cloud provider and to do this they use the DPIAT-tool.

5. The cloud customer (see step 1) launches the DPIAT-tool and selects their chosen service provider in the drop-down menu.
6. The cloud customer starts off by doing the Pre-Screening Questions which is a questionnaire consisting of six questions. Depending on the results from the Pre-Screening Questions DPIAT may then recommend the cloud customer to make the Screening Questions, which is a larger questionnaire consisting of 54 questions.
7. In this scenario, the cloud customer is advised to do the Screening Questions, so the cloud customer answers the 54 questions.
8. After the Screening Questions the cloud customer is now presented to the risk evaluation, divided into Overall Risk Level, Project-based Risks and CSP-based Risks.

This scenario is possible to carry out without having to involve any other stakeholders, although it will be hard to find suitable stakeholders because of the many questions to fill out. It will be a bit fictitious if the stakeholder representative does not have any real need for this service. Possibly, a set of pre-defined answers should be available for the user when interacting with the two tools (COAT and DPIAT).

#### 7.4. Scenario 2. Individuals (I)

Consult illustrations in D:D-7.1 for this scenario, for example Figures 28, 29, 31, and 35. The ultimate goal of this scenario is to evaluate the potential for the data subjects to be notified on the data handling procedures in the cloud chain and give them the capability for exercising their rights by requesting the appropriate remediation actions.

1. The scenario will start with the individual end user signing up for an account for the Wearable service.
2. The end user then performs some tasks in the Wearable service, e.g. checking the blood pressure (hourly metric values) and counting the number of performed activities during the last week.
3. At some point in time, the end user receives a notification from the RRT (through the DT) that a violation has occurred (in this scenario, the steps taken before an actual violation is identified are overlooked because they are outside the scope of the demonstration for this type of stakeholders, see D:D-7.1 figure 18 and 19 for the full process; updates will appear in D:D-7.2).
4. The end user can then request remediation options from the RRT, which then will suggest remediation activities for the end user.
5. Now the end user will have some alternatives on possible remediation and redress actions and will have to decide amongst them which action to take.
6. When the end user has decided on an action, the end user chooses to apply the selected action in the RRT. The RRT then submits the remediation request to the relevant tool/recipient: i) if the action refers to a data deletion action, Data Track is invoked or ii) if the action refers to a complaint to the Supervisory Authority, then this role is notified and subsequently scenario 4 can be invoked for instance in the form of a demo video.

This scenario can be carried out without the interference of another stakeholder or role that needs to respond to the end users action. Possibly, if the demonstration participant gives a set of fake data to register a new account, we can generate violations and notifications in advance including such data through RRT. For an individual non-ICT skilled user it will not be necessary to explain all the steps from the identified violation, from A-PPLE until it reaches the end user. Since it is only RRT (through Data Track) that the end user is exposed to, that interaction is what should be evaluated first.

#### 7.5. Scenario 3. Cloud Providers (P)

**Scenario 3a: Implementing the policies of the required solution** In this scenario, we refer to the contents of Section 4.2.3 of D:D-7.1. The Wearable Co as a cloud customer needs to agree on the accountability policy specification with the selected SaaS from scenario 1. To this end, the selected cloud provider Kardio-Mon receives a list of business, privacy and security requirements from the Wearable Co and uses PLA to create a set of accountability

policies, which translate these accountability requirements to machine readable policies. The policy experts of Kardio-Mon have already defined their accountability related offerings in AAL, which address the legal obligations of Kardio-Mon as well. At any time, using AccLab, the policy experts of Kardio-Mon can match the A-PPL policies from PLA with their AAL based accountability offerings.

1. The scenario starts with a list of requirements, like Table 6 of D:D-7.1.
2. Kardio-Mon security expert opens PLAT (or DPPT, Data Protection Policies Tool) and specifies requirements with respect to data access, retention and transfer.
3. He/she uses PLAT (DPPT) to generate the machine readable accountability policies (in A-PPL)
4. Then, the security expert of Kardio-Mon uses AccLab to compare the generated policies with the ones arising from their legal and normative obligations. Here, a step before is that the security expert of Kardio-Mon has already defined the AAL statements referring to their obligations and has produced A-PPL files of their general privacy policies. When coming to the specific agreement with the Wearable Co, these general policies have to be instantiated to this particular business agreement.
5. For each accountability requirement (data access, retention and transfer), AccLab provides an assessment on whether the PLAT (DPPT) output matches the privacy policies offered by Kardio-Mon.

The list of A-PPL based policies will then be used to configure the cloud service supply chain, driven by Kardio-Mon. This is manually executed by selecting the parts of the final A-PPL policies and feeding them to the A-PPLE, AAS and DTMT tools of Kardio-Mon, Map-on-Web and DataSpacer. Although, technically, this is a trivial step, it is of outmost importance in the process to make the Cloud Providers understand that the accountability policies are populated to the cloud service supply chain as required.

**Scenario 3b: Handling exceptions** In this scenario we will use the cloud provider Kardio-Mon and the scenario will cover how Kardio-Mon acts when there is an identified violation.

1. It all starts with either the A-PPLE engine, the AAS, or DTMT identifying a violation. (It must be clear here on which part of the cloud environment the violation is identified. If DTMT raises an incident, it is probably a data transfer violation happening in the DataSpacer.)
2. The tool sends a notification of the violation to the Incident Management Tool (IMT), and then the (user of) IMT decides on how severe the violation is (in this scenario it is decided that the violation is Low in severity level).
3. The IMT sends a notification to Kardio-Mons IT Admin.

4. The IT Admin assesses the severity through the IMT and then notifies the Kardio-Mons Privacy Officer (PO), which in turn notifies the PO of the Wearable Co
5. Using IMT, the PO of the Wearable Co assesses whether the incident should be notified to the Data Subjects (Individuals). If yes, IMT delegates the notification task to A-PPLE, which acts according to the policy rules.

The full process depicted in Figure 18 in D:D-7.1 contains more steps than those above but they all demand the involvement of more actors than one, and thus hard to simulate interactively in a realistic manner within a one-laptop demonstration. One can restrict the steps to the PO of Kardio-Mon and the Wearable Co. What is essential is to show that the PO of the Wearable Co is responsible for deciding whether a notification of an incident reaches the individuals or not.

#### **7.6. Scenario 4. Auditors and Supervisory Authorities (A)**

Again, Figure 18 in D:D-7.1 has been the base for an abridge scenario. In this scenario, a notification about a violation has been sent from Kardio-Mon and their Incident Management Tool (IMT) to the Supervisory Authority.

1. (a) A notification is automatically sent (by the IMT) when a violation is detected and recognised as a violation with high severity. (b) Alternatively, the Privacy Officer at Wearable Co sends a notification.
2. The Supervisory Authority then requests to make an Audit to Kardio-Mon for their data handling procedures.
3. An Auditor from the Supervisory Authority then performs an audit through the use of the Audit Agent System (AAS) (several usability tests have been carried out on the AAS; see test plans or test reports for an example of test/demo design).

It is possible to carry out this scenario without the interference of other stakeholder groups. An example of a notification with some fake (but realistic) data can be shown to the auditor from the Supervisory Authority (for the alternative (b) in step 1, also fake data can be used without involving representatives of Cloud Providers in the demo). After this, the auditor is presented to the AAS and asked to check the information presented in the notification.

## 8. Conclusions

In this deliverable, we have presented UI prototypes for the A4Cloud tools and integrated toolsets for the different stakeholders, namely cloud subjects, cloud consumers and cloud providers. We have followed an iterative user centred design process, in which the initial prototypes and mock-ups from deliverable D:D-5.1 “User Interface prototypes V1” have been further refined and evaluated. Since the current implementations of the tools vary heavily in terms of maturity, we have employed a number of different user-centered methodologies in our evaluation activities. In addition we have outlined some scenarios that can be used to evaluate the A4Cloud project demonstrator, which is currently being developed and set up at one of the project partners at their premises in Greece.

In the following section, we summarise the main results of the A4Cloud tool and toolset evaluations, emphasising specifically some open issues and improvements that we still recommend:

**Main conclusions for cloud subject tools and toolset:** The **GenomSynlig** dashboard comprises a set of A4Cloud tools aimed at cloud subjects that can help them tracking their data disclosures, exercise their rights to control their data on the services’ sides and obtain remediation in case of possible privacy breaches. Its main component is the Data Track tool, which was as a prototype described in earlier project deliverables [3] and has evolved into a higher-fidelity product. We have suggested two main designs for the visualizations of personal data disclosures, which we refer to as the trace view and the timeline view. User evaluations revealed that users appreciate the transparency properties offered by GenomSynlig, preferring the trace view visualization over the timeline. Evaluations also show the possible confusion that can arise about the way with that users can access their data on the services’ side. We have thus suggested alternatives for future improvements of the user interface of GenomSynlig which can allow users to exercise control over the data that they have disclosed in a better way.

**Main conclusions for cloud customer tools:** The **DPIAT** guides the users through a questionnaire and the UI adhere to most of the well-known usability principles. However, the large amounts of text may cause confusion amongst some users and reduce clarity. The UI of **COAT** is rather mature and the recommendations we provide are mostly about wording and use of concepts, in order to avoid misunderstandings. In particular laymen might have trouble understanding the terms of the service offerings. The issues that we have pointed out for the two tools should, however, be easy to address in their next versions.

**Main conclusions for cloud provider tools:** Parallel to the actual development of the **AAS tool**, an UI design development process have generated some ideas (partly implemented already) where a more dashboard-like approach then menu-based has been reached. The UI of the AAS tools was tested and improved in three iterations with experts users. The final tests showed that while some tasks were still difficult to perform at the start, the test users then quickly learned the purpose and use of the tool. Nonetheless, tooltips and other support functionalities are recommended to make the use of the tools more easily understood for first time users. Possibly, presenting controls according to branching work-flows can guide new users the

best but such designs have not been investigated (this would need very definitive and complete work scenarios). The UI of **AccLab** has undergone several changes that have improved the usability of the tools, however, it is recommended to implement a wizard to guide the user through the policy creation process. For **IMT**, which is in an early stage of development, the evaluation showed that the tools first and foremost need to be adapted to existing incident management software and processes at an organisation. Furthermore it is crucial that the UI provides an easy way to distinguish between local incidents and incidents that have been derived from 3rd party providers.

**General conclusions:** Having a dedicated work package for the design and evaluation of usable interfaces for the A4Cloud tools turned out to be both a blessing and a challenge. While our work package D5 was responsible for the development of the Privacy Dashboard GenonSynlig including the Data Track and their user interfaces, the main responsibility for the development of all other tools with GUIs were part of other work packages and WP D5's task was to help with the user interface design and tests. On one hand, it gave the researchers involved in the work package D5 an opportunity to focus solely on making the tools as usable as possible, without having to consider any issues related to the implementation of their functionality. On the other hand, it required additional efforts in terms of communication and cooperation with the tool owners (who did the actual development of the software). Some of the tools (such as COAT and Data Track) already had user interfaces when our work started, while others (such as IMT) were very early in the design phase, or, such as in the case of PLAT, were even only developed at the end of WP5 and thus not subject of this evaluation. It therefore varied in terms of what kind of help the tool owners wanted from our work package and to what degree they wanted to be involved in the evaluation activities. Ideally, to minimize usability problems, usability experts should be involved in the development phase as early as possible but this was feasible for all the tools.

This deliverable concludes the work with user interfaces for the tools developed in the A4Cloud project. We foresee that the mock-ups and UI prototypes that we have created, the bootstrap template, the conceptual terminology model and the stakeholder-specific UIs for toolsets that we have delivered and the recommendations for future UI work that we suggest for each individual tool will lead to improvements by the tool owners and thus to more usable tools that can be used to demonstrate the project results.

## References

- [1] R. Alnemr, S. Pearson, R. Leenes, and R. Mhungu. Coat: Cloud offerings advisory tool. In *IEEE 6th International Conference on Cloud Computing Technology and Science (Cloud-Com)*, pages 95–100, Dec 2014.
- [2] Julio Angulo, Karin Bernsmed, Simone Fischer-Hübner, Christian Frøystad, Erlend A. Gjære, and Erik Wästlund. D:D-5.1 User Interface Prototypes V1. Project deliverable D:D-5.1, A4Cloud Project, August 2014.
- [3] Julio Angulo, Simone Fischer-Hübner, John Sören Pettersson, and Mia Toresson Jessica Edbom. D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability. Project deliverable D:C-7.3, A4Cloud Project, September 2014.
- [4] Julio Angulo, Simone Fischer-Hübner, Tobias Pulls, and Erik Wästlund. Usable transparency with the data track: A tool for visualizing data disclosures. In *Extended Abstracts in the Proceedings of the Conference on Human Factors in Computing Systems, CHI '15*, pages 1803–1808, Seoul, Republic of Korea, 2015. ACM.
- [5] Julio Angulo and Martin Ortlieb. “wth..!?” experiences, reactions, and expectations related to online privacy panic situations. In *Proceedings of the 10th Symposium on Usable Privacy and Security, SOUPS '15*, Ottawa, ON, Canada, 2015. ACM.
- [6] Hila Becker, Mor Naaman, and Luis Gravano. Beyond trending topics: Real-world event identification on twitter. In *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media (ICWSM'11)*, 2011.
- [7] Harvey Russell Bernard. *Research methods in cultural anthropology*. Sage Newbury Park, CA, 1988.
- [8] Richard Mark Brown, Jesus Luna, Alain Pannetrat, Jean-Claude Royer, Mohamed Sellami, Monir Azraoui, Kaoutar Elkhayaoui, Niamh Gleeson, Asma Vranaki, Anderson Santana De Oliveira, Karin Bernsmed, Carmen Gago, and David Núñez. D:d-2.3: Initial reference architecture. Technical report, A4Cloud Project, April 2015.
- [9] Tom Buchanan, Carina Paine, Adam N Joinson, and Ulf-Dietrich Reips. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2):157–165, 2007.
- [10] Daniela Soares Cruzes, Martin Gilje Jaatun, Børge Haugset, Massimo Felici, Julio Angulo, and Simone Fischer-Hübner. D:B-2.3 Workshop 3 results (Use case domain). Project deliverable D:B-2.3, A4Cloud Project, August 2014.
- [11] Brian Dziminski, Massimo Felici, Carmen Fernandez Gago, Frederic Gittler, Theo Koulouris, Ronald Leenes, Jesus Luna, Maartje Niezen, David Nunez, Alain Pannetrat, Siani Pearson, Jean-Claude Royer, Dimitra Stefanatou, and Vasilis Tountopoulos. D:C-2.1 Report detailing conceptual framework. Project deliverable D:C-2.1, A4Cloud Project, October 2014.



- [12] E Eggert, S Abou-Zahra, and The Education and Outreach Working Group. Web application menus - w3c approved draft. Accessed 2015-08-26.
- [13] European Union Agency for Network and Information Security (ENISA). Information disclosure, 2015.
- [14] Simone Fischer-Hübner, Hans Hedbom, and Erik Wästlund. *Trust and Assurance HCI*, chapter 13, page 261. PrimeLife - Privacy and Identity Management for Life in Europe. Springer, June 2011.
- [15] Linton C. Freeman. Visualizing social networks. *Journal of social structure*, 1(1):4, 2000.
- [16] Mohammad Ghoniem, J Fekete, and Philippe Castagliola. A comparison of the readability of graphs using node-link and matrix-based representations. In *IEEE Symposium on Information Visualization (INFOVIS 2004)*, pages 17–24. IEEE, 2004.
- [17] The Open Group. ArchiMate<sup>®</sup> 2.1 Specification, 2013. [http://pubs.opengroup.org/architecture/archimate2-doc/chap03.html#\\_Toc371945162](http://pubs.opengroup.org/architecture/archimate2-doc/chap03.html#_Toc371945162).
- [18] Lane Harrison and Aidong Lu. The future of security visualization: Lessons from network visualization. *Network, IEEE*, 26(6):6–11, 2012.
- [19] Monique W.M. 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(11-12):781–795, 2004.
- [20] Sanjay Kairam, Diana MacLean, Manolis Savva, and Jeffrey Heer. Graphprism: compact visualization of network structure. In *Proceedings of the International Working Conference on Advanced Visual Interfaces*, pages 498–505. ACM, 2012.
- [21] Elahe Kani-Zabihi and Martin Helmhout. Increasing service users' privacy awareness by introducing on-line interactive privacy features. In *Information Security Technology for Applications*, pages 131–148. Springer, 2012.
- [22] Jan Kolter, Michael Netter, and Günther Pernul. Visualizing past personal data disclosures. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, pages 131–139. IEEE, 2010.
- [23] Daniel Lindegren. Visualisera personuppgifter i ett tidslinje gränssnitt & användning av font awesome-ikoner i a4cloud-projektet. Master's thesis, Karlstad University, Karlstad, Sweden, 2015.
- [24] Robert K Merton and Patricia L Kendall. The Focused Interview. *American Journal of Sociology*, 51(6):541 – 557, 1946.
- [25] Jakob Nielsen. Heuristic evaluation. *Usability inspection methods*, 17(1):25–62, 1994.
- [26] Donald A. Norman and Stephen W. Draper. *User Centered System Design; New Perspectives on Human-Computer Interaction*. L. Erlbaum Associates Inc., Hillsdale, NJ, USA, 1986.











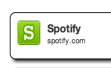







- [27] Siani Pearson, Vasilios Tountopoulos, Daniele Catteddu, Mario Südholt, Refik Molva, Christoph Reich, Simone Fischer-Hübner, Christopher Millard, Volkmar Lotz, Martin Gilje Jaatun, Ronald Leenes, Chunming Rong, and Javier Lopez. Accountability for cloud and other future internet services. In *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, CloudCom 2012, Taipei, Taiwan, December 3-6, 2012*, pages 629–632. IEEE Computer Society, 2012.
- [28] 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.
- [29] John Sören Pettersson and Malin Wik. Perspectives on ozlab in the cloud: A literature review of tools supporting wizard-of-oz experimentation, including an historical overview of 1971-2013 and notes on methodological issues and supporting generic tools. 2014.
- [30] Catherine Plaisant, Brett Milash, Anne Rose, Seth Widoff, and Ben Shneiderman. Life-lines: visualizing personal histories. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 221–227. ACM, 1996.
- [31] Tobias Pulls, Julio Angulo, Stefan Berthold, Kaoutar Elkhyaoui, Jenni Reuben, Cédric Van Rompay, Melek Önen, and Anderson Santana De Oliveira. D:D-5.3 User-Centric Transparency Tools V2. Project deliverable D:D-5.3, A4Cloud Project, September 2013.
- [32] James A Russell. A circumplex model of affect. *Journal of personality and social psychology*, 39(6):1161, 1980.
- [33] Douglas Schuler and Aki Namioka, editors. *Participatory Design: Principles and Practices*. L. Erlbaum Associates Inc., Hillsdale, NJ, USA, 1993.
- [34] Vasilis Tountopoulos and Daniele Catteddu. D:c-3.1 requirements for cloud interoperability. Technical report, A4Cloud Project, November 2013.
- [35] US-CERT. Traffic Light Protocol (TLP) Matrix and Frequently Asked Questions, 2015.




# Appendices

## A. Appendix

### A.1. Concepts in prototypes: A table for comparison of UI contents

Concepts found in A4Cloud-tools				
Basic term	Written representation in UI	Definition / Conceptual Content	Tool	Graphical representation or Longer UI text
(Policy-) Violation	I have been affected!!!	A button with the label "I have been affected!!!", which triggers the response and Remediation Tool, with information about the incident already filled in.	IRT, D:D-5.1 Mockup	
Transparency, ex post	Notifications	Notifications for incidents relevant to the user.	IRT, D:D-5.1 Mockup	 A button, which, if pressed by the user will show an overview of the incidents relevant for the user.
Preferences	Preferences	User preferences for incident notifications.	IRT, D:D-5.1 Mockup	 Users can define preferences for incident notifications: how often, for which severity level and for which incident types the user wants to be receive alerts.
(Policy-) Violation*	Data affected	Icons together with a textual explanation that represent the affected personal data. Data affected is the headline with the following data (see next column to the right) presented under. If any of these data are affected, the users avatar will be placed to the right of the affected data together with an action button, in order to take measures about the problem.	IRT, D:D-5.1 Mockup	<b>Data affected</b>  Customer names * passwords  Email addresses  Home addresses  Phone numbers <input type="checkbox"/> Credit card number The user can enter a detailed view for a particular incident, where all the affected personal data are present.
Track Data	Track your data with this provider	Action that a user can initiate. A button with the label "Track your data with this provider". <b>COMMENT:</b> Written repr sounds ungrammatical. Suggestions: Track what data this provider may have about you. Track your data kept by this provider.	IRT, D:D-5.1 Mockup	 In the detailed view for a particular incident, the user has the possibility to launch Data Track, filtered by the data hold by this service provider.
Cloud service OR Service	Service	The different services with which the user (=Data Subject) has interacted. <b>COMMENT:</b> Should the Data Track use both the terms 'service' and 'service provider'? Presently these two concepts do not seem to be kept distinct.	DT 4.0	  The icons represent the various services that have personal data about the user. Shown in the trace view.
Cloud service OR Service	Service	The different services with which the user (=Data Subject) has interacted. <b>COMMENT:</b> Should the Data Track show both 'service' and 'service provider'? Presently these two concepts do not seem to be kept distinct.	DT 3.0	 Spotify spotify.com  Company name Company homepage
Data control	on their side (In "Read more..." the text is "...under their control")	In this context, personal data that is located on the service provider's side, under their control.	DT 3.0	This is a list of the information that Spotify has stored about you on their side: <a href="#">Read more...</a>
Personal data	More info	This icon, the "cloud" triggers a popup/new dialog window which represents "more info".	DT 3.0	 Is the user clicks the Cloud-icon, more information regarding the service provider's data about the user is shown. Shown in the trace view.
Personal data	Information	Personal data types about the user.	DT 4.0	   The icons are meant to help the user see what kind of personal data the service providers have about the user. Shown in the trace view. The icons above are just examples of icons, representing specific data types.
Personal data	Information	Personal data about the user and data type.	DT 3.0	652 11 person.address.postalcode Shown in the trace view. The picture above is just an example of the data type postalcode together with the corresponding information about the users postalcode.
Personal data	Record	A set of Personal data about the user	DT 3.0	Shown in the "More info"-window.
Personal data	Information record	A set of Personal data about the user	DT 3.0	Shown in the "Read more"-popup in the "More info"-window
Service Provider	Service provider	Service providers offering services <b>In Glossary:</b> Cloud Service Provider	COAT, D-4 Video demo	







## D:D-5.4 User Interface Prototypes V2

Basic term	Written representation in UI	Definition / Conceptual Content	Tool	Graphical representation or Longer UI text
Location (Geographical storage location OR Legal storage location OR Hardware storage location )	Acceptable Storage Location including Backup	Where personal data is stored (incl. Backup)	COAT, D-4 Video demo	 <p>Example icons above.</p> <p>From COAT-questionnaire pop-up: "This question concerns where personal data is stored and what data protection and data privacy laws apply to protect it."</p> <p><b>COMMENT:</b> Note the assumption that "storage location" is about geographical location and what privacy laws apply. May the end-user mistake "storage location" to mean whether data are located on her hard drive, USB stick, or stored online at the service provider side?</p>
Personal data	Personal data	Personal data are data that relates to identifiable people	COAT, D-4 Video demo	
Location (Geographical storage location OR Legal storage location OR Hardware storage location )	Acceptable Data Processor Location	Acceptable locations for data processing	COAT, D-4 Video demo	 <p>Example icons above.</p> <p>The textual representation is "Acceptable Data processor location" while the graphical representation is labeled "Processor Location".</p> <p>From COAT-questionnaire pop-up: "This refers to where the users personal data is processed and what laws apply to protect it. Processing data is very wide and it means carrying out any operation or set of operations on the information or data (for example organizing, retrieval, consultation, deletion or use of the information or data)"</p> <p><b>COMMENT:</b> Possibly not intuitive. Does it refer to where the data are being processed, where the data processor has it's head quarter or what laws that apply. These can be three different locations.</p>
Data Transfer	Data transfer in case of emergency?	Consent for having personal data transferred in case of emergency	COAT, D-4 Video demo	<p>From COAT-questionnaire pop-up: This question asks you for your consent to have personal data transferred in an emergency situation. An emergency may involve a data breach or potential destruction of your data by a physical threat to a data storage centre (for example a fire). Giving your consent may help to help prevent any delays in an emergency and your Service Provider needs your consent to transfer this data to another storage centre.</p>
Information security	Do you want Encryption?	Encryption alternatives: SSL, 256bit SSL, Client Side Encryption, Strong 2014 ("or better" ?) <b>COMMENT Rehab Alnemr, regarding the "strong 2014"-icon:</b> Actually it was used as a placeholder for new encryption types.	COAT, D-4 Video demo	 <p>From COAT-questionnaire pop-up: Encryption is designed to guard against the data being compromised and encryption of personal data is considered be in accordance with good security policy and best practice methodologies for protecting personal information. The icon above is an example from the D-4 ScreenShots.</p>
Dispute Resolution	Is it important that any disputes are resolved in your own country? AND Dispute Resolution: Which court?	Disputes between Service provider and a cloud customer.	COAT, D-4 Video demo	<p>From COAT-questionnaire pop-up: Disputes can be resolved using various processes: arbitration, mediation, online dispute resolution and court legal action. If you are a business, you need to make a decision whether you agree to resolve disputes with your SP in another country or locally. Besides the own country, US, EU and China are the alternatives.</p>
Data Deletion	Deletion: Control over deletion of your data?	(1) User trigger deletion, (2) Provider can delete in case of termination, (3) Insurance of hard deletion (overwriting on the hard-drive).	COAT, D-4 Video demo	<p>From COAT-questionnaire pop-up: You may want full control of deleting data if you want to be sure that you store personal data no longer than is necessary, as required by data protection law. Alternatively, depending on the data that you are storing, it may be sufficient that the provider deletes it on termination of your contract particularly if your contract is not a long-term contract. Even after deletion, data may still be read by certain software (for example used in computer forensics). If you are storing personal sensitive data, you may need to have greater certainty that the data is deleted permanently by having it overwritten.</p>
Service Termination	Termination	Termination of account / contract	COAT, D-4 Video demo	<p>Termination appears in the Questionnaire, to be filled out by the user (optional).</p>
Transparency of contract changes	Transparency in case of changing terms and conditions	<b>From Glossary:</b> Transparency, the property of a system, organisation or individual of providing visibility of its governing norms, behaviour and compliance of behaviour to the norms.	COAT, D-4 Video demo	<p>From COAT-questionnaire pop-up: Service Providers change their contract terms and conditions from time to time. You may want to be notified in advance about changes because this gives you a chance to look for another Service Provider if you do not like the proposed changes. Alternatively, you can decide that your Service Provider cannot make any changes and so the contract will end if they try to change it. Another option is to have a right in your contract to terminate and this means that you can end the contract if you do not like the proposed changes.</p>

## D:D-5.4 User Interface Prototypes V2

Basic term	Written representation in UI	Definition / Conceptual Content	Tool	Graphical representation or Longer UI text
Subcontracting	Allow Subcontracting?	Sub-contracting means that the SP will use other companies or individuals (third parties) to provide some of its services.	COAT, D-4 Video demo	From COAT-questionnaire pop-up: Sub-contracting means that the Service Provider will use other companies or individuals (called 'third parties') to provide some of its services. If you allow sub-contracting then the Service Provider can use third parties to provide some of its services to you. As a result, your Service Provider may have less control of its service to you and so your data may be less secure. <b>COMMENT:</b> Can a SP really use "other individuals" (i.e. human beings) to provide some of its services?
Compliance	Demonstration of Compliance?	Compliance means obeying the law.	COAT, D-4 Video demo	From COAT-questionnaire pop-up: Compliance means obeying the law. Some companies have policies, procedures, trust marks and certificates that demonstrate that they comply with certain laws. <b>COMMENT:</b> Compliance could also relate to different standards (e.g. ISO)
LEA request	Notified when Law Enforcement requests your data (if legally possible)?		COAT, D-4 Video demo	From COAT-questionnaire pop-up: Law enforcement agencies (LEAs) may request your data from your Service Provider to help them investigate crime. This is normally done using a warrant and often the Service Provider is not allowed by law to tell you that the LEA is requesting your data. If you ask to be notified, this means that when the Service Provider is allowed to tell you that an LEA has requested your data, you will get a chance to object to the request if you believe that your data should not be disclosed.
IPR - Intellectual Prop	IPR on user client?		COAT, D-4 Video demo	From COAT-questionnaire pop-up: Intellectual property rights (IPRs) are rights that include copyright, trademarks and patents. You may want guarantees in the contract from your Service Provider that any IPRs that you develop from information that you put in the cloud will remain with you. You may also want to specify who can use these IPRs (for example, your Service Provider).
Backup location	Should unlimited backup be included?	A backup of the stored dataset <b>COMMENT:</b> Where is this backup located? In the same geographical location? On the same server?	COAT, D-4 Video demo	
Security Breach OR (Policy-) Violation	Notified in case of security breach?		COAT, D-4 Video demo	This means that the Service Provider agrees to notify you if there are security breaches affecting your data. You may have a legal right to be informed of unauthorized access or unlawful transfer of personal data in certain circumstances. Even so, if the Service Provider agrees in its contract to notify you if there are security breaches affecting your data, then you have additional reassurance that you will be told about security breaches by your Service Provider. <b>COMMENT:</b> This is just a subset of all possible security breaches that can happen.
Cloud service	buting or using new cloud service		DPIAT, C-6 Video demo	
Cloud Service Provide	Select a service provider	List of the available service providers	DPIAT, C-6 Video demo	
Risk and trust model	Risk and trust model	The model upon which the tool is built, DPIAT assesses the probability and impact risks, that is, it makes a PIA	DPIAT, C-6 Video demo	
Personal Data	Does the project involve personal data?		DPIAT, C-6 Video demo	Personal data shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social history.
Personal Data	Does your personal data include personally identifiable information (PII)?		DPIAT, C-6 Video demo	Personally Identifiable Information (PII) are information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. <b>COMMENT:</b> Is there a need for both "personal data" and "PII" to refer to the same concept?
Personal Data	Which kind of personal data does your project collect?	The user is presented to various different kinds of personal data types in alist and has to chose atleast type.	DPIAT, C-6 Video demo	
Location (Geopraghical storage location OR Legal storage location OR Hardware storage location )	Is the establishment of your activities in European territory?		DPIAT, C-6 Video demo	Whether the processing of personal information of your undertaking takes place inside the European territory or not is not relevant. If you are not established in European Union territory, but you offer goods or services to individuals in the EU or monitor them, then you should answer Y to this question. <b>COMMENT:</b> Is the word "establishment" good? The explanation says that territory does not matter but to whom the offer is made.


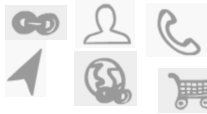
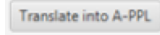

## D:D-5.4 User Interface Prototypes V2

Basic term	Written representation in UI	Definition / Conceptual Content	Tool	Graphical representation or Longer UI text
Risk	Probability	The probability that the identified event turns out. (Risk = probability * impact.)	DPIAT, C-6 Video demo	
Risk	Impact	This is how serious the identified event is, if it actually turns out. (Risk = probability * impact.)	DPIAT, C-6 Video demo	
Cloud Service Provider	CSP	The abbreviation CSP is used in the box "Screening Questions" in the first view of the DPIAT C-6 Video demo	DPIAT, C-6 Video demo	
Privacy	Which potentially privacy intrusive technologies does the project use?	The user is presented to some privacy intrusive technologies to chose among	DPIAT, C-6 Video demo	Some technologies are considered privacy intrusive by providing additional risks if the necessary measures to protect data are not ensured, although no definition of these privacy intrusive application/technologies occur in the tool nor do any examples.
Privacy	Is the application area of your project privacy intrusive?	Yes/No question	DPIAT, C-6 Video demo	If the application area is privacy intrusive, the privacy impact or a risk scenario can be more severe. Some examples for privacy invasive applications: patient and elderly monitoring, vehicle tracking, security surveillance, smart metering.
Data Transfer	Is personal data being transferred to other organizations for processing or other purposes?	Yes/No question	DPIAT, C-6 Video demo	If the project obtains personal information for a particular purpose, your organisation may not use the data for any other purpose, and you may not divulge the personal data to a third party, except in ways that are 'compatible' with the specifies purpose
Privacy Enhancing Tool	Explorer	This panel contains a tree view of the workspace (two types are handled : -aai a simple text format that contains AAL code; -acd a json file format that contains the components diagram (see appendix))	AccLab, D-3 AccLab Demo	
Privacy Enhancing Tool	Outline	The outline contains a tree view of the current components (with blue icon) in the opened acd file, and for each agent its required services (in red icon) and provided services (green icon).	AccLab, D-3 AccLab Demo	
Privacy Enhancing Tool	Components	Contains the elements that can be used in the diagram (agent : a simple agent with types, required and provided services; data : same as agent but with an additional attribute subject (the data owner) ; macro : insert a macro call in the generated AAL program (more details will be provided soon)).	AccLab, D-3 AccLab Demo	
Privacy Enhancing Tool	Tools	A panel containing different tools to be used while editing acd/aal files (copy- /past/zoom/save/etc).	AccLab, D-3 AccLab Demo	
Privacy Enhancing Tool	Diagram	The diagram workspace.	AccLab, D-3 AccLab Demo	
Privacy Enhancing Tool	Properties	A grid containing the properties of a selected element in the diagram, in which you can edit its name, style properties (color, font, etc) and also types/services.	AccLab, D-3 AccLab Demo	
Privacy Enhancing Tool	Output	The output where we show the result coming from the back-end.	AccLab, D-3 AccLab Demo	
Privacy Enhancing Tool	AAL editor	Allows to edit quickly a component's policy, before generating the AAL program.	AccLab, D-3 AccLab Demo	
			AAS, web prototype	There is a web prototype, <a href="http://aas.cloud.hs-furtwangen.de/">http://aas.cloud.hs-furtwangen.de/</a> , which we haven't thoroughly evaluated yet.
Audit	Audit overview	The Audit overview is the main window of the AAS tool. Here three different types of policies are presented to the tool user, Data handling policies, Access control policies and Custom policies. These are presented in three tabs, which can be seen to the right in column Comment / Graphical representation.	AAS, web prototype	
Audit	Create audit	In the Create audit window the auditor can create and run audit tasks on different services for compliance with their policies. The audit tasks are separated by the same tabs as in the Audit overview window and the tasks are presented under each tab. There is also the possibility to edit or delete each task.	AAS, web prototype	
Audit	Results	The Results window presents the results from the audit and divides the task into three different categories, Violation, Need review and Passed.	AAS, web prototype (July and Feb 2015)	 
Audit	Records	<b>COMMENT:</b> In this window, is it possible to obtain old audit results? The term "Records" is also used in DT 3.0, do the term mean the same thing in both tools? (I.e., is there a risk that a AAS user sends a message about "records" that a DT user will read?)	AAS, web prototype	
Risk	Violation	The most critical severity level. (In AAS mockup D:D-5.1 this is called Critical instead of Violation.)	AAS, web prototype	
Risk	Need review	Second most critical severity level. <b>COMMENT:</b> Does the verb in plural fit the headline use but does the verb also occur on individual items? ("Needing review" is longer.)	AAS, web prototype	
Risk	Passed	Task that has passed the audit.	AAS, web prototype	

## D:D-5.4 User Interface Prototypes V2

Basic term	Written representation in UI	Definition / Conceptual Content	Tool	Graphical representation or Longer UI text
Cloud service OR Service	Service	Cloud service	AAS, D:D-5.1 Mockup	
Audit	Auditor	The actor which performs audit, can act on behalf of either a cloud customer or cloud provider or third party.	AAS, D:D-5.1 Mockup	
Audit	Audit	Audit cloud infrastructure and services for compliance with policies.	AAS, D:D-5.1 Mockup	
Privacy Enhancing Tool	A-PPL policies	<b>COMMENT:</b> AccLab generates AAL policies. These policies can then (in theory) be transformed to A-PPL policies.	AAS, D:D-5.1 Mockup	Before an audit can be started the relevant A-PPL policies are needed in order to compare the actual situation to what the provider has promised.
Audit	Audit task	Possibility to perform different audit tasks on different services and their policies.	AAS, D:D-5.1 Mockup	
Risk	Critical	The most critical severity level. <b>COMMENT:</b> What action needs to be taken in this case? And what does Critical mean?	AAS, D:D-5.1 Mockup	 Critical (12) This has been taken care of in the web prototype.
Risk	Needs review	Second most critical severity level, needs to be reviewed.	AAS, D:D-5.1 Mockup	 Needs review (24)
Risk	Passed	Task that has passed the audit.	AAS, D:D-5.1 Mockup	 Passed (79)
Compliance	Compliance threshold	Degree to which the threshold of compliance is met.	AAS, D:D-5.1 Mockup	
Storage location	Data location	The main view for the DTMT tool, where the users get the possibility to query for data locations and view their details of different data groups (i.e. Different categories of data). If there are any unhandled violations related to the data group, a summary will be presented to the user in this window with four different choices for the user to resolve the violation: Details about the violation, Review policy, Take action and I don't care.	DTMT, D:D-5.1 Mockup	
Personal Data	Data group	A list of different categories of data.	DTMT, D:D-5.1 Mockup, Figure 26	
Cloud Service Provider	Service provider	The different Service providers to which the user have an account / contract. <b>In Glossary:</b> Cloud Service Provider	DTMT, D:D-5.1 Mockup, Figure 26	
Vulnerability	Sensitivity	How sensitive the data within the data group is. High/Medium/Low.	DTMT, D:D-5.1 Mockup, Figure 26	
Storage location	Location	The location where the data group is stored. <b>COMMENT:</b> What does "location" really mean	DTMT, D:D-5.1 Mockup, Figure 26	
(Policy-) Violation	Policy violations	A violation against the policy.	DTMT, D:D-5.1 Mockup, Figure 27	 <b>Policy Violations</b> Shows as a summary in the Data location view and under the more Detailed view, which shows when a user clicks the "More details"-link in the summary.
Data Processor	Processors	<b>From Glossary:</b> A natural or legal person, public authority, agency or any other body which processes the personal data on behalf of the controller.	DTMT, D:D-5.1 Mockup, Figure 27	
Transparency, ex post	History	Shows a history of events and information to the user. Contains History for both Location, Policy violations and Processors.	DTMT, D:D-5.1 Mockup, Figure 27	
Transparency, ex post	Details about violation	A direct link to IRT.	DTMT, D:D-5.1 Mockup, Figure 26	This button takes the users directly to IRT, where they can get more information about the violation.
Privacy Preferences	Review policy	A direct link to AccLab. <b>COMMENT:</b> So this means that the user has to install AccLab in order to review a policy?	DTMT, D:D-5.1 Mockup	Takes the users directly to AccLab, where they could review his preferences and validate them against the providers policy.
Contact	Take action	A direct link to R&RT.	DTMT, D:D-5.1 Mockup	Takes the users directly to R&RT, where they could handle the violation.
	I don't care	Link for closing the violation notification window. Deliverable D-5.1 text: "This link could simply close the violation without handling it."	DTMT, D:D-5.1 Mockup	
Transparency	Type of incident	Can show to the user which data type that is affected by the incident. <b>COMMENT:</b> Conflict: "Incident type" is not the same as "data type".	R&RT, D:D-5.1 Mockup, Figure 37	
Transparency		The yellow callout in figure 37 "The types of personal data involved"	R&RT, D:D-5.1 Mockup, Figure 37	 This gives the possibility to indicate which kind of personal information that is involved in the accident, this is represented by a set of icons (icons above are only examples).

## D:D-5.4 User Interface Prototypes V2

Basic term	Written representation in UI	Definition / Conceptual Content	Tool	Graphical representation or Longer UI text
Contact	Contact service	Deliverable D-5.1 text (figure 37): Find a known incident about a particular service. <b>COMMENT:</b> Where does this explanation stem from? Try "regarding" instead of the word "about". If this is the conceptual content, why is function called "Contact service"? Moreover, if it is contacting, it should be "Contact service provider".	R&RT, D-D-5.1 Mockup	
Contact	Contact a local authority	Get in touch with your local data protection authority or consumer agency.	R&RT, D-D-5.1 Mockup	
Contact	Get advice	Get practical, legal or general advice about your data in the cloud.	R&RT, D-D-5.1 Mockup	
Remediation	Remediation request win	The user can choose to trigger a remediation request by him/herself, and enter all details manually. If the remediation request is triggered by the IRT, most information is provided by the IRT - which the user can preview and confirm.	R&RT	
Data Transfer (Processing of Personal Data)	Request my data	The user has the possibility to request access to the data that different cloud services have about the user. In this case, the user is able to view first the data or types of data that they disclosed to different data controllers and then send data subject access requests mails to selected data controllers, possibly with a reference to the previous disclosures of data or data types about that they would like to receive more information (in regard to how this data has been processed or whether it has meanwhile been deleted or not).	DSART, D-D-5.1 Mockup	
Cloud service OR Service	Cloud service	Cloud service	DSART, D-D-5.1 Mockup	
Personal Data	Data	The different types of personal data available to be inquired about by the user. <b>COMMENT 1:</b> If the word "data" only refers to personal data then the terms might be "personal data" instead of just "data". <b>COMMENT 2:</b> Can the word "data" refer to data that might turn into "personal data" if the data subject reveals more information?	DSART, D-D-5.1 Mockup	
Cloud Service	Service Name	Label	PLAT (D 3.3)	Data in the input field next to the label: "Hosting Servers"
Cloud Service Provider	Cloud Service Provider	Label	PLAT (D 3.3)	Data in the input field next to the label: "Hosting CSP"
Data Processing	Data Processing	<b>COMMENT:</b> Drop-down menu -> Unclear what the menu contains	PLAT (D 3.3)	
Data Retention	Data Retention	<b>COMMENT:</b> Drop-down menu -> Unclear what the menu contains	PLAT (D 3.3)	
Data Transfer	Data Transfer	<b>COMMENT:</b> Drop-down menu -> Unclear what the menu contains	PLAT (D 3.3)	
Security Measures	Security Measures	<b>COMMENT:</b> Drop-down menu -> Unclear what the menu contains	PLAT (D 3.3)	
Notification	Data Notification Breach	Drop-down menu -> Contains the next four elements below	PLAT (D 3.3)	
Event Type	Event Type	Label	PLAT (D 3.3)	Data in the input field next to the label: "Data Leakage"
Recipient	Recipient	Label	PLAT (D 3.3)	Data in the input field next to the label: "Customer Reference"
Time Frame	Time Frame	Label	PLAT (D 3.3)	Data in the input field next to the label: "1 week"
Address	Address	Label	PLAT (D 3.3)	Data in the input field next to the label: "customerRef@email.com"
Notification	Notification sending triggered by data breach event	<b>COMMENT:</b> Drop-down menu -> Unclear what the menu contains	PLAT (D 3.3)	Drop-down menu -> Unclear what the menu contains
A-PPL	Translate into A-PPL	Button to translate the policy statements to A-PPL	PLAT (D 3.3)	
A-PPLE	Send to A-PPL Engine	Button to send the policy to the A-PPL Engine repository	PLAT (D 3.3)	
<b>Slide presentation concept</b>			<b>Slide text</b>	
Data Access	Data Access	One of the incident types presented in Wearables Service Use Case-2.pptx from Stream D / D-6 / meetings / 2015-01-21-telco	Detected by A_PPLE	"The Wearable Co employee tries to access the sensitive PII raw data of the customers"
Data Retention	Data Retention	One of the incident types presented in Wearables Service Use Case-2.pptx from Stream D / D-6 / meetings / 2015-01-21-telco	Detected by A_PPLE	"The Wearable Co policy defines that the wellbeing historical data are maintained only for the last 6 months"
Data Deletion	Data Deletion	One of the incident types presented in Wearables Service Use Case-2.pptx from Stream D / D-6 / meetings / 2015-01-21-telco	Detected by A_PPLE	"The Wearable Co policy defines that the wellbeing historical data are maintained only for the last 6 months"
Storage Location	Data Location	One of the incident types presented in Wearables Service Use Case-2.pptx from Stream D / D-6 / meetings / 2015-01-21-telco	Detected by DTMT	"The Wearable Customer wants to keep the data only in Europe. A hardware failure results in data move to a third party location"
Data Encryption	Encryption vulnerability	One of the incident types presented in Wearables Service Use Case-2.pptx from Stream D / D-6 / meetings / 2015-01-21-telco	Detected by AAS	"The Map-on-Web requests the wellbeing raw data for all the CardioMon users to generate the weekly statistics per geographical area"
Data Access	Right to know vs Need to know	One of the incident types presented in Wearables Service Use Case-2.pptx from Stream D / D-6 / meetings / 2015-01-21-telco	Detected by AAS	"Too many accesses to a data record, or by a given administrative user. Detect cases where an authorized party makes too many requests to fulfil its function, indicating an abuse of its right, hence a (probable) security violation"

## D:D-5.4 User Interface Prototypes V2

---

Basic term	Written representation in UI	Definition / Conceptual Content	Tool	Graphical representation or Longer UI text
Service Unavailability	Service unavailability	One of the incident types presented in Wearables Service Use Case-2.pptx from Stream D / D-6 / meetings / 2015-01-21-telco	Detected by AAS	"The Wearable Customer requests the wellbeing status profile from CardioMon, but this profile has been moved"





## A.2. GenomSynlig usability study: Tasks and Questions

Trace view	Answers RQ #
<p>What do you think the elements on the top represent?</p> <p>[1] All of my own information [2] My own information I have sent to online services [3] Other people's information [4] Other _____</p> <p>Comments</p>	1
<p>What do you think the elements at the bottom represent?</p> <p>[1] Services on the Internet [2] Services on the internet that have information about me (I have given information) [3] Other _____</p> <p>Comments</p>	1
<p>Using the GenomSynlig's trace view, how can you see the information that you have sent to AdBokis.com?</p> <p>[1] Success (clicked on the AdBokis.com service on the bottom panel) [2] Partial success (succeeded after ~45 seconds) [3] Failed</p> <p>Comments</p>	1; 2; 6; 7
<p>How can you see to which Internet services have you given your email address (<a href="mailto:bob_bobsson@hotmail.com">bob_bobsson@hotmail.com</a>)?</p> <p>[1] Success (looks for the email address and clicks on it. Or opens the filter controls and search for the mail) [2] Partial success (succeeded after ~45 seconds) [3] Failed</p> <p>Comments</p>	1; 6; 7
<p>What would you do to see all information about you that has to do with medical data?</p> <p>[1] Success (Opens the filter controls and check the "Medical data" box) [2] Partial success (succeeded after ~45 seconds) [3] Task failed but managed to answer correctly (Succeeds by checking all attributes with icons that might be related to medical data). In this case moderator should ask the question in a different way. [4] Failed</p> <p>Comments</p>	5
<p>What would you do to see if Groupon and Tactiohealth have any information about you in common?</p> <p>[1] Success (Opens the filter controls, turns on the "Common" button, and selects both of the organization.) [2] Partial success (succeeded in more than 2 minutes) [3] Task failed but answered correctly (Selects each company one at a time and deduces if there are information in common). Moderator should try to re-ask the question. [4] Failed</p> <p>Comments</p>	5
<p>The GenomSynlig program gives you an overview of the information you have given to different Internet services. In your opinion, where are the records shown in the top panel of</p>	10

## D:D-5.4 User Interface Prototypes V2

<p>the trace view program stored?</p> <p>[1] On the GenomSynlig program (cloud)</p> <p>[2] On the GenomSynlig program (locally in computer)</p> <p>[3] On the Internet somewhere</p> <p>[4] On the services that I have given information to</p> <p>[5] I have no idea</p> <p>[6] Other: _____</p> <p>Comment</p>	
<p>In your opinion, who has access to the records being shown in the top panel of the trace view?</p> <p>[1] Only me and no one else</p> <p>[2] Only me and AdBokis.com</p> <p>[3] The GenomSynlig employees and AdBokis.com</p> <p>[4] Other services shown by the GenomSynlig (including AdBokis.com)</p> <p>[5] Everybody using the GenomSynlig program and AdBokis.com</p> <p>[6] Everybody on the Internet</p> <p>[7] The government</p> <p>[8] Other</p> <p>Comments</p>	10, 12
<p>Where would you click to see the information that AdBokis.com has stored on their servers when you purchased the book?</p> <p>[1] Success (clicks on the "cloud" icon on the AdBokis.com service on the bottom panel)</p> <p>[2] Partial success (succeeded after ~45 seconds)</p> <p>[3] Failed (if failed, moderator should show correct way)</p> <p>Comments</p>	3; 8
<b>Timeline</b>	
<p>Explain what you think this view is showing you?</p> <p>[1] Success (Mentions that boxes show personal data disclosures in chronological order)</p> <p>[2] Partial success (Mention something about things being display by time)</p> <p>[3] Failed</p> <p>Comments</p>	2
<p>By looking at this interface, could you tell me what information about you was disclosed to Spotify in March 2<sup>nd</sup> 2013 at 8:40?</p> <p>[1] Success (Mentions that boxes show personal data disclosures in chronological order)</p> <p>[2] Partial success (Mention something about things being display by time)</p> <p>[3] Failed</p> <p>Comments</p>	5; 6; 7
<p>What would you do to see the number of times that you have disclosed your credit card number?</p> <p>[1] Success (Opens the filtering options and tries to search for credit card)</p> <p>[2] Partial success (Mention something about things being display by time)</p> <p>[3] Failed</p>	5; 6

## D:D-5.4 User Interface Prototypes V2

Comments	
<p>What would you do to see all the disclosures that you made in March 2013?</p> <p>[1] Success (Scrolls down to find the appropriate Month range and name the disclosures. Or opens the filter controls and tries to filter by month and year)</p> <p>[2] Partial success (Succeeded after ~45 seconds or more)</p> <p>[3] Failed</p> <p>Comments</p>	5; 6
<p>Can you tell me how many personal attributes about you were disclosed to Facebook on March 9<sup>th</sup> 2013 at 23:18?</p> <p>[1] Success (Clicks on the "show more" button to reveal all the attributes released to Facebook on that timestamp)</p> <p>[2] Partial success (Succeeded after ~45 seconds or more)</p> <p>[3] Failed</p> <p>Comments</p>	5; 6; 7
<p>Where would you click to see the information that AdBokis.com has stored on their servers when you purchased the book?</p> <p>[4] Success (clicks on the "cloud" icon on the AdBokis.com service on the bottom panel)</p> <p>[5] Partial success (succeeded after ~45 seconds)</p> <p>[6] Failed (if failed, moderator should show correct way)</p> <p>Comments</p>	3; 6; 7; 11
<b>Services' side dialog and data control</b>	
<p>What information about you does AdBokis.com have on their servers?</p> <p>[1] Success (correct information given)</p> <p>[2] Partial success (succeeded after ~45 seconds or partial information given)</p> <p>[3] Almost failure (very incomplete idea, or mentions the information sent by participant, but not information in AdBokis.com)</p> <p>[4] Failed</p> <p>Comments</p>	3; 11
<p>In your opinion, who can access your data that AdBokis.com has stored on their servers?</p> <p>[9] Only me and no one else</p> <p>[10] Only me and AdBokis.com</p> <p>[11] The GenomSynlig employees and AdBokis.com</p> <p>[12] Other services shown by the GenomSynlig (including AdBokis.com)</p> <p>[13] Everybody using the GenomSynlig program and AdBokis.com</p> <p>[14] Everybody on the Internet</p> <p>[15] The government</p> <p>[16] Other</p> <p>Comments</p>	10
<p>Did AdBokis.com store the location you were in when you bought the book?</p> <p>[1] Success (Answers "yes")</p> <p>[2] Partial success (Answers "yes" because I gave it to them)</p> <p>[3] Failed (Answers "no")</p>	9; 9a

## D:D-5.4 User Interface Prototypes V2

---

Comments	
<p>Is the information that AdBokis.com have about you more or less that what you gave to them? Why do you think this is?</p> <p>[1] Success (Answers "more, because they can store more information or collect more when I make a transaction")</p> <p>[2] Partial success (Answers "more", but is not sure why)</p> <p>[3] Failed (Answers "less")</p> <p>Comments</p>	9; 9a
<p>What view shows the GenomSynlig records stored on your system and what view allows you to check what data a services side has stored about you?</p> <p>[1] 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)</p> <p>[2] Partial success</p> <p>[3] Failed</p> <p>Comments</p>	3; 11

### **A.3. GenomSynlig usability study: Procedure**

#### *Setting up the test:*

1. (5 min) Moderator sets up the test
  - a) Start server, running the program and clean any cached data on the browser (incognito mode)

#### *Carrying out the test:*

2. (1 min) Moderator welcomes participant to the test (Build rapport)
3. (3 min) Moderator introduces participant to the test
  - a) Read introductory text
  - b) Sign consent form
4. (2 min) Moderator asks participant to navigate to the introduction page of the Data Track and pretend is the first time the tool is being used.
  - a) Participants go through the introductory tour
5. (2 min) Moderator asks participant to navigate to fictitious online book store
  - a) Participant enters address in browser `http://hci.cse.kau.se/hemsfly/Synligv02.new_scenario/scenario/scenario_index.html`
  - b) Participant fills in personal information needed to buy the book
  - c) Participant buys book, by clicking some Buy button.
  - d) Data Track icon is shown, confirming that data has been tracked.
6. (2 min) Moderator indicates user to open the Data Track program
  - a) Participant enters address in browser `http://hci.cse.kau.se:8000`
  - b) Participant examines the interface for around a minute
7. (2 min) Participant gets asked to connect his Adbokis.com account to the Data Track
  - a) Navigate to the page with connectors and enter credentials for AdBokis
8. (10 - 15 min) Participant goes to the series of tasks specified in Appendix XX.
  - a) Moderator encourages participant to think aloud
  - b) Moderator makes observation notes and asks questions
  - c) An electronic questionnaire for the moderator might be setup so that it is easier to record the participants responses.
9. (5 min) Participant answers a short electronic post-questionnaire and moderator asks questions to clarify observations.
10. (2 min) Moderator thanks participants, rewards him/her accordingly and answers any questions.