CLOUD
ACCOUNTABILITY
PROJECT

D:D-5.1 User Interface Prototypes V1

Deliverable Number: D45.1

Work Package: WP 45

Version: Final

Deliverable Lead Organisation: Karlstad University (KAU) and SINTEF

Dissemination Level: PU

Contractual Date of Delivery (release): 31/08/2014

Date of Delivery: 31/08/2014

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

Contributors
Julio Angulo (KAU), Karin Bernsmed (SINTEF), Simone Fischer-Hübner (KAU), Christian Frøystad (SINTEF), Erlend Andreas Gjære (SINTEF), Erik Wästlund (KAU)

Reviewers
Rehab Alnemr (HP Labs), Vasilis Tountopoulos (ATC)

A4Cloud
www.a4cloud.eu
Accountability For Cloud and Other Future Internet Services

FP7-ICT-2011-8-317550-A4CLOUD

SEVENTH FRAMEWORK
PROGRAMME

Executive Summary

This deliverable "*User Interface Prototypes V1*" presents the user centred analyses of A4Cloud tools for developing selected user interface prototypes, mostly in the form of mock-ups or lo-fi prototypes, for these tools and for stakeholder-specific toolsets. These user interface prototypes and analyses can then, through this document, be used as a basis for discussion and comparing/refining alternative approaches that can be tested, also in comparison with other interfaces that tool owners may already have prototyped, in the next stages of the development. The A4Cloud tools, which are subject to these user centred analyses and user interface prototype developments reported in this deliverable, are:

- **Accountability Lab (AccLab)**, which aims to help data protection officers (DPOs) at the cloud services side to define and check accountability obligations and to generate their corresponding A-PPL policies;
- **Audit Agent System (AAS)**, which will allow auditors check for compliance with accountability policies;
- **Cloud Offering Advisory Tool (COAT)**, which will help cloud customers to find a cloud service provider that fulfills their security and privacy needs;
- **Data Subject Access Request Tool (DSART)**, which will complement the Data Track tool with functions for individual cloud users to exercise their data subject rights offline;
- **Data Track (DT)**, which, combined with the Transparency Log, will allow individual cloud subjects and cloud customers to track and control their personal data in the Cloud by allowing them to electronically exercise their data subject rights;
- **Data Transfer Monitoring Tool (DTMT)**, which will help cloud providers and auditors to verify that a service provider is fulfilling the accountability obligations specified in A-PPL policies;
- **Data Protection Impact Assessment Tool (DPIAT)**, which will help individual cloud subjects and cloud customers to identify and assess risks related to data protection in a cloud configuration or environment;
- **Incident Response Tool (IRT)**, which will allow cloud customers to handle privacy and security incidents in cloud environments;
- **Remediation and Redress Tool (RRT)**, which will assist individual cloud subjects and cloud customers to respond to (perceived) incidents and to seek redress when policy violations have occurred;

Usable user interfaces for stakeholder-specific toolsets, i.e. combination of tools assembled to address stakeholder-specific needs into, for instance, coherently designed dashboards, are also discussed in the deliverable for the stakeholder groups cloud subjects, cloud customers, and DPOs.

All user interface prototypes have been developed by various user centred design methods. The methods used range from workshops with novice end users to expert evaluations by tool owners. Additionally, project personas and use case descriptions have been used to clarify the purpose of the tool and its intended use throughout the design process. In most cases, the user interface development has been based on a formal task analysis specifying the user requirements and goals. User interfaces prototypes have then been created to ensure that users are able to reach the goals specified in the task analysis. As a last step, the user interfaces were verified against the use case scenarios in [BFS+13].

Most of the mock-ups that are presented in this deliverable have not been subject to thorough usability tests yet. As mentioned, they rather serve as a starting point for further discussions, user testing and refinements. The prototypes do not necessarily cover the entire breadth of a tool either, but may rather focus in-depth on particular parts of the functionality. In some cases, feedback from tool owners and next design steps are also included in the deliverable[1].

A final implementation of hi-fi user interface prototypes, which will be subject to more thorough usability evaluations, will be presented in the upcoming deliverable D:D-5.3 that will be delivered in September 2015.

[1] As an exception, the user interfaces for Data Track tool were usability tested in two iteration cycles. The test results will be reported in the deliverable D:C-7.3 "*Report on end-user perceptions of privacy-enhanced transparency and accountability*", whereas this deliverable presents and discusses the improved Data Track user interfaces that try to address the detected usability issues and thus resulted from those tests.

Contents

List of Figures

List of Tables

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
HCI	Human Computer Interaction
IRT	Incident Response Tool
PAPV	Plug-In for Assessment of Policy Violations
PETs	Privacy Enhancing Technologies
RRT	Remediation and Redress Tool
SME	Small and Medium-sized Enterprise
TETs	Transparency-Enhancing Technologies
UCD	User Centred Design
UI	User Interface
UML	Unified Modelling Language

1. Introduction

1.1. Project Scope and Background

The A4Cloud project deals with accountability for the cloud and other future Internet services. It conducts research with the objective of increasing trust in cloud computing by developing methods and tools for different stakeholders through which cloud providers across the entire cloud service value 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, comprise according to the A4Cloud Conceptual Framework (MSC-2.3), so called individual or organisation cloud subjects that are entities whose data is processed by a cloud provider, either directly or indirectly; individual or organisation cloud customers that are entities that maintain a business relationship with, and use services from a cloud provider; as well as cloud providers and cloud auditors including data protection officers (DPOs).

The A4Cloud project is creating solutions to support cloud subjects and customers in deciding and tracking how their data are used by cloud service providers [PTC$^+$12], including tools that are developed to combine risk analysis, policy enforcement, monitoring and compliance auditing with tailored IT mechanisms for security, assurance and redress. In particular, the project develops the following tools for the different stakeholder groups:

- **Accountability Lab (AccLab)**, which aims to help data protection officers (DPOs) at the cloud services side to define and check accountability obligations and to generate their corresponding A-PPL policies;

- **Audit Agent System (AAS)**, which will allow auditors check for compliance with accountability policies;

- **Cloud Offering Advisory Tool (COAT)**, which will help cloud customers to find a cloud service provider that fulfils their security and privacy needs;

- **Data Subject Access Request Tool (DSART)**, which will complement the Data Track tool with functions for individual cloud users to exercise their data subject rights offline;

- **Data Track (DT)**, which, combined with the Transparency Log, will allow individual cloud subjects and cloud customers to track and control their personal data in the Cloud by allowing them to electronically exercise their data subject rights;

- **Data Transfer Monitoring Tool (DTMT)**, which will help cloud providers and auditors to verify that a service provider is fulfilling the accountability obligations specified in A-PPL policies;

- **Data Protection Impact Assessment Tool (DPIAT)**, which will help individual cloud subjects and cloud customers to identify and assess risks related to data protection in a cloud configuration or environment;

- **Incident Response Tool (IRT)**, which will allow cloud customers to handle privacy and security incidents in cloud environments;

- **Remediation and Redress Tool (RRT)**, which will assist individual cloud subjects and cloud customers to respond to (perceived) incidents and to seek redress when policy violations have occurred;

1.2. Aims and Scope of this Report

This report on "*User Interfaces Prototypes V1*" is delivered by task T:D-5.1 of WP D-5 of the A4Cloud project, which has the objective to develop usable user interface (UI) prototypes for various combinations of tools assembled to address stakeholder-specific needs by following human-centered design processes.

This deliverable presents the first iteration(s) of user interface prototypes for A4Coud tools and stakeholder-specific toolsets. The main focus has been on user-centered analysis for each tool, building up to selected UI (User Interface) artefacts rather than horizontally complete prototypes. Most of the UI mock-ups that we present have not been user tested yet, nor are they final yet[2]. These first iterations of mock-ups rather serve as a starting point for further discussions, user testing and refinements. The prototypes do not necessarily cover the entire breadth of a tool either, but may rather focus vertically (in-depth) on particular aspects of critical tool functionality. In the next phase we will work more closely with the tool owners, using our UI artefacts as a basis for discussion and to compare and refine alternative approaches that can be tested against each other (and what tool owners already have prototyped/implemented).

1.3. Relationship to other A4Cloud Work Packages and Deliverables

This project deliverable is related to the work of several other work packages in A4Cloud, especially those work packages that have elicited requirements.These are the stakeholder-related requirements elicited in WP B-2, the social requirements elicited in WP B-4, the legal requirements elicited in WP B-5 and most importantly the HCI (Human Computer Interaction) requirements elicited in WP C-7, as well as requirements originating from all the work packages in stream D that will do the actual development of the tools and the toolsets, for which initial UI prototype proposal are presented in this deliverable.

This project deliverable is particularly based on, or related to, several other A4Cloud project deliverables:

- The deliverable D:C-7.1 "*General HCI principles and guidelines*" [AFHP+13] by work package C-7 provides HCI principles and Guidelines for A4Cloud tools that have been elicited in the first project year. These principles and guidelines have to a large extent been guiding the UI prototype designs and are also referred to in this document at several places.

[2] An exception is the UIs for the Data Track tool, which were usability tested in two iteration cycles. The usability test reports are however not within the scope of this deliverable, as they will be presented within the deliverable D:C-7.3 "*Report on end-user perceptions of privacy-enhanced transparency and accountability*". Also an early prototype version of COAT (that is not presented in this deliverable), which has been developed by work package D-4, has been user tested in two stakeholder elicitation workshops organised by work package B-2.

- The deliverable D:B-3.1 "*Use Case Descriptions*" [BFS+13] by work package B-3 defined three use case scenarios related to cloud computing with the help of personas that were developed to define different actors and roles in these scenarios. In this deliverable we verify that our proposed mock-ups and tool descriptions fulfill these use case scenarios.

- The deliverable D:C-7.3 "*Report on end-user perceptions of privacy-enhanced transparency and accountability*" will, as mentioned above, report about the result of user tests of the Data Track tool UIs that are presented in this deliverable;

- The upcoming deliverable D:D-5.3 "*User Interface prototypes V2*" will presents the final user interfaces for toolsets for the different stakeholders. D:D-5.3 is due in September 2015.

1.4. Deliverable Outline

The remainder of this deliverable is structured as follows:

In Chapter 2 "*User Centred Design*", we present and discuss the user centred design processes that we followed for the development of the the initial user interface prototypes.

Chapter 3 "*Preliminary User Interface Prototypes for A4Cloud Tools*" describes the initial user interface prototypes that we developed for the A4Cloud tools listed in subsection 1.1 above.

Chapter 4 "*Toolset Integration*" presents and discusses UI prototypes for various combinations of tools assembled to address stakeholder-specific needs.

Finally, chapter 5 "*Concluding Remarks*" rounds up this deliverable by drawing conclusions and discussing the next steps.

2. User Centered Design (UCD)

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 [ND86]. Nowadays the term UCD is often used interchangeably with other similar approaches, such as Participatory Design [SN93], 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 these methods that have been used in our work for A4Cloud when following a UCD approach.

2.1. Personas

Developing and using personas is a common method for defining and getting to know the target users of a computer system. The personas are not real users but fictional portraits of users. Attributes that are common to include when describing a persona are his/her name and age, a picture, motivation/goals, computer skills, a short personal history, employment and job description. According to Cooper et al. [CRC03, p. 78], personas can help designers at *determining* what a product should do and how it should behave, *communicating* with stakeholders, developers and other designers, *building consensus and commitment* to the design, *measuring* the design effectiveness, and *contributing* to other product-related efforts.

In WP:B-3 of A4Cloud a set of personas have been developed to define different actors or roles in three business use cases that are related to cloud computing [BFS$^+$13]. Through a series of workshops and interviews with important stakeholders in the different business use case domains (efforts which have been driven by WP:B-2), different types of stakeholders who are likely to interact with the accountability tools developed in A4Cloud were identified. Different personas were created to reflect the human aspects of stakeholder user types we encounter.

The personas further play a part in a number scenarios to elaborate on their goals and needs (see next section).

2.2. Use case scenarios

Scenarios are narrative descriptions of the envisioned usage of a possible system with the purpose of guiding the development of such system with its users in mind. Scenarios propose a narration of a concrete activity that a user can engage in when performing a task [Her03].

While sketches can capture the look-and-feel of a design, scenarios are intended to capture the essence of the *interaction* of the design of an interactive product [RC02]. Like interactive prototypes, scenarios are also efficient tools for communicating to developers and stakeholders about possibilities of usage under various contexts.

Scenarios used in A4Cloud are described in project deliverable DB3.1 [BFS$^+$13]. The work done in this deliverable considers these scenarios for designing the user interfaces of the tools that support the different actors portrayed in these scenarios. In particular, we verify that the proposed user interface prototypes and tool descriptions remain true to the goals and needs reflected in the use case scenarios.

2.3. Eliciting UI requirements from the A4Cloud WPs

User interface requirements were collected from D:C-7.1 [AFHP$^+$13], D:B-3.1 [BFS$^+$13] and survey responses from thw A4Cloud tool developers made available by WP:D-2, which were guiding the development of user interface prototypes. For eliciting requirements, stakeholder workshops and focus groups were held, and experiments, surveys and user tests were conducted as described in the those deliverables.

In addition requirements were elicited from informal discussions with the A4Cloud tool owners, industrial and academic experts outside the A4Cloud project and the A4Cloud advisory board.

2.4. Users' goals and task analysis

In order to gain an overview of input from the analysis of user needs and goals, we have created a UML Use case diagram for each of the tools. These diagrams, which will be presented in the next chapter, show the involved stakeholders/actors, and provide a high-level view of what the users of a tool will be able to achieve by using it. Note that the diagrams do not represent functional specifications but aggregate what was learned in the user-goal-based part of our analysis. While the goal-based output is *what* each respective user should be able to achieve, it is further used to as a basis of analysing *how* it should be achieved. Importantly, there should be no sense of *process flow* in the UML Use case diagrams, i.e. not a path to follow. Relationships between use cases can simply be read as natural sentences in the direction of the arrow.

Before actually creating graphical prototypes, we have performed a task analysis for each tool. This follows a natural continuation of the UML Use case diagrams, in terms of how to implement something that fulfils the user goals. Few tools will follow an entirely deterministic sequence of actions, but rather allow some choices to be made be the users. The purpose of the task analysis is to break down goals into explicit tasks and sub-tasks, which show what the user will be required to do in terms of actions in order to fulfil a goal. The goal of this process is to understand the system and how information flows within it while still leaving room for different implementation options in the later prototyping and development phase. The flow of actions and cognitive processes to achieve a task is in focus, and will give a good analytical basis to understand a system and how information flows within it. In this document the task analysis is located in Appendix A, and should be read for each tool in conjunction with the UML use case diagram.

2.5. Prototyping

Prototyping involves using different techniques, tools and materials, ranging from paper, pens and cardboards to wireframes and more advanced programming languages [Fal03]. One of the main purposes for creating prototypes during the development process is to facilitate communication between designers, developers, managers and end users. This deliverable, part of WP:D-5 of the A4Cloud project, is concerned with the creation of initial ideas of the tools for accountability to be developed, which will be communicated through the use of sketches and prototypes of higher fidelity.

The prototypes are based on the task analysis, described in section 2.4, and survey responses made available through WP:D-2 as well as the focus groups and workshops described earlier.

The focus when creating the initial prototypes has been on fulfilling the tool owners' functional descriptions, the HCI requirements that we elicited earlier for A4Cloud (see section 2.3), the task analyses and best practice of user experience design.

2.6. Evaluation

It is important to note that most of the UI prototypes presented in this deliverable have not been user tested yet (apart from some smaller heuristic evaluations for some of the mock-ups), nor are the sketches final. For most mock-ups, this is the first iteration in the process of defining the user interfaces of the A4Cloud tool kit, and are meant to serve as a starting point for further discussion, testing and refinement.

An exception is the Data Track tool, which has already evolved from previous projects. As described in section 3.5, the Data Track user interfaces have been further enhanced within the scope of the A4Cloud projects and have already been usability tested in two iteration cycles. These usability test results are described and discussed in the Deliverable D:C-7.3 "*Report on end user perception of privacy-enhanced transparency and accountability*" and are therefore not reported in the deliverable.

Moreover, as a combined effort between WP:B-2 and WP:C-7, a focus group with 19 participants, who represented individual cloud subjects, was carried out with the objective of eliciting further functional requirements while at the same time obtain feedback on the usability and design progress of the Data Track tool (Section 3.5). More information about the process and results of this focus group are also reported in the deliverables D:B-2.3 and D:C-7.3.

3. Preliminary User Interface Prototypes for A4Cloud Tools

In this chapter, the first versions of user interface mockups for the A4Cloud tools will be presented and discussed. Each tool has a description which summarizes our understanding of the tool in question based on the tool descriptions that were available to us and discussions that we had with the tool owners.

Then a UML use case diagram is provided, as well as a textual summary of the use case diagram and the task analysis to be found in appendix A.

Continuing, each tool has a section on initial UI prototypes. This is how the writers envisions, from the users' perspective, that tools can be used based on the understanding presented in the tool description. As mentioned in section 2 and as indicated by the title of this deliverable, these are initial prototypes to be used as a foundation for further discussions, user testing and refining. As mentioned earlier, the exceptions are Data Track and COAT. The Data Track tool has evolved from previous projects, and for which we have already developed, tested and enhanced two iterations of graphical user interfaces within the scope of A4Cloud (in addition to further user interface iterations that we conducted earlier within the PRIME and PrimeLife EU projects). As the user interfaces of the Data Track are already at a more advanced state, we did not start with conducting a task analysis and defining an UML diagram for the Data Track tool in section 3.5, but rather discuss the Data Track user interfaces in more detail. The other example is COAT, for which a complete prototype has been designed and developed by WP D-4 in parallel to the UI work that is presented in this deliverable. The COAT UI designed by WP D-4 has already been tested it in two workshops using end users representing cloud providers and cloud customers.

Finally, in this chapter every tool is validated against the use case scenarios.

3.1. Accountability Lab (AccLab)

The purpose of the Accountability Lab tool (AccLab) is to help data protection officers define and generate machine readable accountability obligations that specifiy the processing rules for personal and/or business confidential data. The tool will assist him in formulating abstract accountability obligations (specified in the AAL policy language developed in WP C-4), which can then be checked for consistency and compliance, and to generate the corresponding machine readable obligations (specified in the A-PPL policy language developed in WP C-4). Thus, the tool will enable its users to experiment with accountability obligations and to evaluate their adequacy. The tool might also be used directly by a data subject in order to check whether a service provider's policies are consistent with the data subject's accountability preferences.

The user provides input to the tool through a smart wizard, which will help him specify the accountability obligations.

The tool has three sections:

- A section for visually declaring system resources (i.e. agents, services and data)
- A second section for the wizard with lists of choices to write obligations
- A third section for the code editor where the AAL clauses can be edited directly

A toolbar will also be present to allow the user to check for consistency and compliance and to generate the A-PPL policy.

3.1.1. Users' goals and task analysis

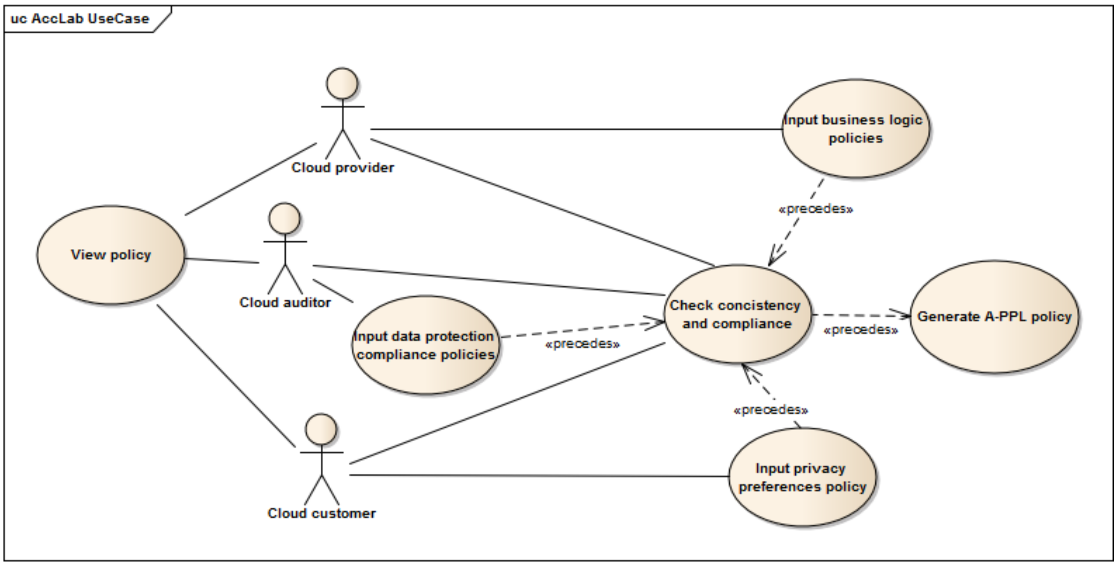

uc AccLab UseCase
Cloud provider
Cloud auditor
Cloud customer
View policy
Input business logic policies
Input data protection compliance policies
Check concistency and compliance
Generate A-PPL policy
Input privacy preferences policy
«precedes»
«precedes»
«precedes»
«precedes»

Figure 1: A UML use case diagram for AccLab

The task analysis for the AccLab tool is presented in Appendix A.1. As can bee seen, there are two main tasks for the AccLab tool:

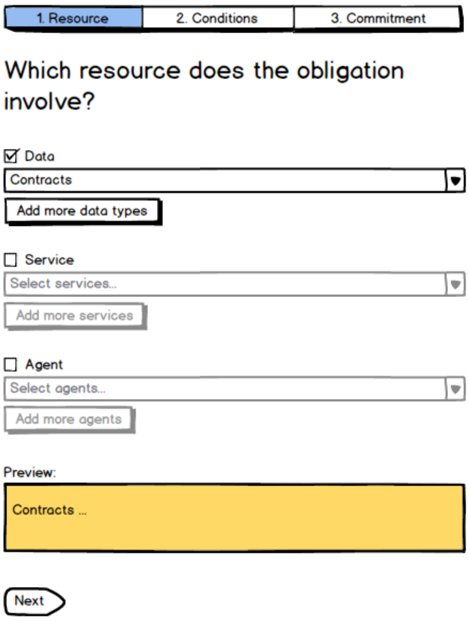
1. To create policies
2. To check the policies for consistency and compliance

The tool can be used by three different categories of users; cloud providers (who are responsible for providing policies for their business logic) cloud auditors (whose main focus are on data protection compliance) and cloud customers or cloud subjects (who want to specify their accountability preferences). It is necessary that all relevant policies are specified before a consistency and compliance check is run.

The UML use case diagram depicted in Figure 1 provides a high-level view of what the tool should actually do.

3.1.2. Initial UI prototypes

The following reflections and mock-ups are based on the description of AccLab, which is available in A4Cloud deliverable MS:D-2.2 by WP:D-2.



Which resource does the obligation involve?

☑ Data

Contracts

□ Service

Select services...

□ Agent

Select agents...

Preview:

Contracts ...

Figure 2: The user chooses the resouces to create an obligation

Obligation wizard If the users chooses to use the wizard to create a new obligation, the wizard will lead them through several simplified steps. The steps could be: Resources, Conditions and Commitments.

In resources, as exemplified in figure 2, the users could specify which resources the obligation relates to. The users could be allowed to choose the relevant resources from lists based on the information provided when the resources were defined.

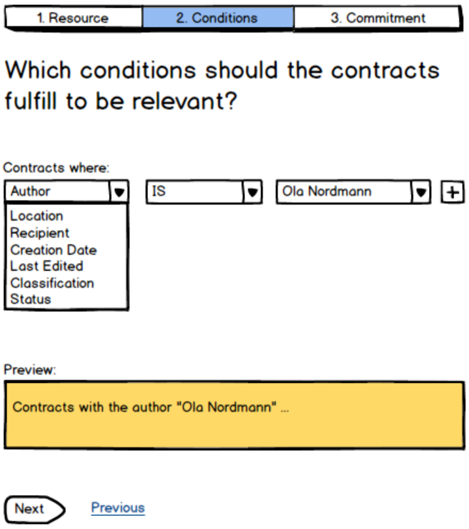
If the users want the obligation to include multiple resources of the same type, the tool could either allow the users to add a new select box by clicking on ”Add more data types” or the select box could be of the same type as the one suggested in section 3.2.2.

As shown in figure 3, the tool could update its text to be in accordance with the selection of resources. Instead of the header saying ”Which conditions would you like to include?” it could say ”Which conditions should the contracts fulfil to be relevant?”

The tool could also focus on the flow of the language in the interaction with users, as exemplified in figure 3 and 4. This will help the users to build sentences, which they might be able to understand, rather than complicated mathematical expressions they might not understand.

The choices could be dynamically updated to provide the users with the correct alternatives based on the prior selections. For example, if the users choose to condition on “Author”, a selection of users or authors can be provided.

Figure 2 and 3 show two different examples of how adding another row could be done. Using a button under the previous item, as shown in figure 2, supports the natural work flow and provides enough space for the title to be explicit. Using a plus sign at the right of the previous item, as shown in figure 3will lead to less visual clutter but has some drawbacks. First, it does not support the natural work flow of working from the top down, but requires the users to go



Which conditions should the contracts fulfill to be relevant?

Contracts where:

Author ▾ | IS ▾ | Ola Nordmann ▾ | +

Location
Recipient
Creation Date
Last Edited
Classification
Status

Preview:

Contracts with the author "Ola Nordmann" ...

Figure 3: The user defines conditions on the resources

to the right of the elements and thus breaks the work flow. Second, it is not explicit what will happen when the users press the button; it might mean that a new row will be added, but it might also mean that the current row is added.

To pick the best solution both alternatives must be user tested. One alternative should be chosen and implemented for both situations.

At the end of the form, the users could be presented with the obligation under construction. When the users have completed the wizard, they could be presented with the completed obligation in understandable terms. Figure 4 shows how this could be done. The summarizing sentences could be grouped by data type and commitment, which would give one sentence per pair of data type and commitment.

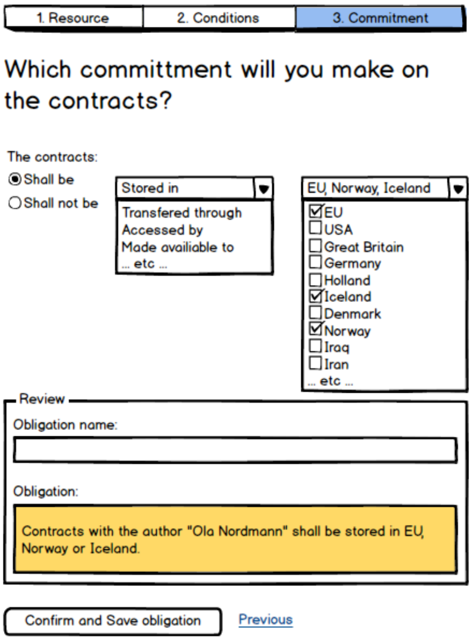
Browse obligations The users could be provided with the ability to browse all obligations, as shown in figure 5, to view obligation details and to perform actions on the obligations. Examples of relevant actions are to edit or delete an obligation. It could also be possible to add another obligation by clicking new, which would start the wizard.

In this view, the tool could include a button that allows the users to check the consistency of the defined obligations.

The left pane gives the users and easy way to find what they are looking for. This feature is created to be consistent with the Incident Response Tool (section 3.8.2, figure 33).

3.1.3. Verification against use case scenarios

In this subsection we analyse to what degree the current version of AccLab is able to address the concerns of the personas described in the A4Cloud project deliverable DB3.1 [BFS$^+$13].



Which committment will you make on the contracts?

The contracts:

● Shall be
○ Shall not be

Stored in ▼
Transfered through
Accessed by
Made availiable to
... etc ...

EU, Norway, Iceland ▼
☑ EU
□ USA
□ Great Britain
□ Germany
□ Holland
☑ Iceland
□ Denmark
☑ Norway
□ Iraq
□ Iran
... etc ...

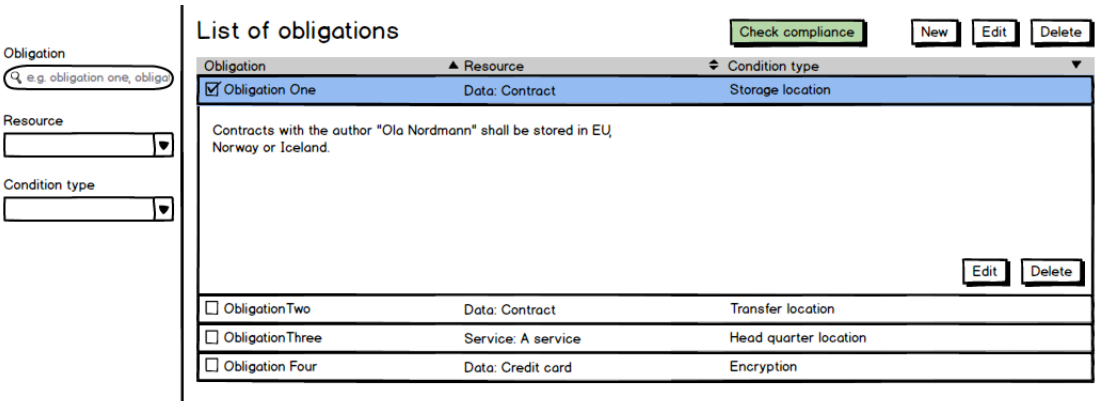
Review

Obligation name:

Obligation:

Contracts with the author "Ola Nordmann" shall be stored in EU, Norway or Iceland.

Figure 4: The user defines commitments on the conditioned resources, gives the obligation a name and then saves the obligations



List of obligations

Obligation	▲ Resource	⇕ Condition type ▼
☑ Obligation One	Data: Contract	Storage location
□ ObligationTwo	Data: Contract	Transfer location
□ ObligationThree	Service: A service	Head quarter location
□ Obligation Four	Data: Credit card	Encryption

Contracts with the author "Ola Nordmann" shall be stored in EU, Norway or Iceland.

Figure 5: The user is provided with the ability to browse all obligations

First we outline the scenarios that describe the activities that happen in relation to defining policies or preferences and then we briefly summarize whether AccLab will be useful in these scenarios.

Scenario 1.1.1a: Kim This scenario describes how Kim, who is an individual end user, uses a tool to view the data policies for his personal data. The Accountability Lab will be of some help with this task (since it provides its users with the possibility of viewing existing accountability policies), however, the terms of service agreement or the Data Track tool might be a better place to look for this information though.

Scenario 1.1.2a: Kim This scenario describes how Kim, who is an individual end user, uses a tool to set his preferences on which sensor data about him he allows to be collected. The Accountability Lab tool can help Kim with this task, provided that it is the cloud service provider that controls what data will be collected from the sensors and not just a local setting in the sensor application itself.

Scenario 1.1.2b: Kim This scenario describes how Kim, who is an individual end user, uses a tool to disallow any non-relevant actors to access his data. The Accountability Lab tool can help Kim to include such restrictions in the accountability policies.

Scenario 2.1.1a-b: Sandra These scenarios describe how Sandra, who is an individual end user, has disabled an applications ability to collect any information about her location. Similarly to Kim's situation in Scenario 1.1.2a above, AccLab might be of help with this task. If it is a local setting in an app that Sandra controls, AccLab is not of help. If it is a central policy created that requires the service provider not to store the position, AccLab can be of help with this task.

Scenario 3.1.1a: Michael This scenario describes how Michael, who is a privacy officer at a cloud customer, creates policies for data based on end users privacy preferences as well as the restrictions implied by applicable law. The Accountability Lab tool can be of help with this task.

Scenario 4.1.1a-b: Peter These scenarios describe how Peter, who is a senior system architect at a cloud service provider, uses a tool to support him in the process of establishing contracts with one of their cloud customers as well as with other cloud providers. AccLab can be of help here, by allowing Peter to create policies and validate them against the policies from the other parties (including possible preferences from the cloud customer).

Scenario 4.1.2a: Peter This scenario describes how Peter, who is a senior system architect at a cloud service provider, uses a tool to renegotiate the contract of a cloud customer. As in scenario 4.1.1a-b, AccLab can be of help here by allowing Peter to propose changes and to validate the new contract clauses against the policies and preferences of the cloud customer.

Scenario 7.1.1a: Alice This scenario describes how Alice, who is an individual end user, accesses, corrects, removes data and changes the services right to access a group of data. In this scenario, AccLabcan be of help with the last issue; to configure access rights.

Scenario 9.1.1a: Charles This scenario describes how Charles, who is a developer at a cloud service provider, uses a tool to define accountability policies in a machine readable format. AccLab will help with this task.

Scenario 13.1.1b: Sandra This scenario describes how Sandra, who is an individual end user, sets data policies to be associated with specific personal data. AccLab can be of help with this task.

Scenario 14.1.1b: Paul This scenario describes how Paul, who is the Chief Privacy Officer of a SME, sets data policies for the cloud services adopted by his IT Company. AccLab will be of help with the creation of these policies.

Scenario 15.1.1b: Roger This scenario describes how Roger, who is the Chief Technology Officer of a cloud service provider, drafts different contracts with cloud users as well as other cloud providers depending on the service levels required and risk/trustworthiness profiles of involved parties. AccLab can be of assistance when creating the policies or contracts by allowing for the policies to be validate against the users, customers, external providers or own internal policies.

Scenario 15.1.1f: Roger This scenario describes how Roger, who is the Chief Technology Officer of a cloud service provider, actively searches for the needs and concerns of cloud users and decides what action he can perform based on that information. AccLab can be of help with this task, provided that the users have entered their preferences into the tool. Roger would then be able to validate his suggested actions against the users' preferences.

Scenario 18.1.1a-b: Sandra These scenarios describe how Sandra, who is an individual employee and end user, wants specific assurance about how personal data is treated by a cloud service provider as well as be able to hold the provider accountable. AccLab can be of assistance in checking the provider's policies.

All identified use case scenarios are fulfilled by mock-ups and tool description.

3.2. 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 administers audits and to view audit reports.

3.2.1. Users' goals and task analysis

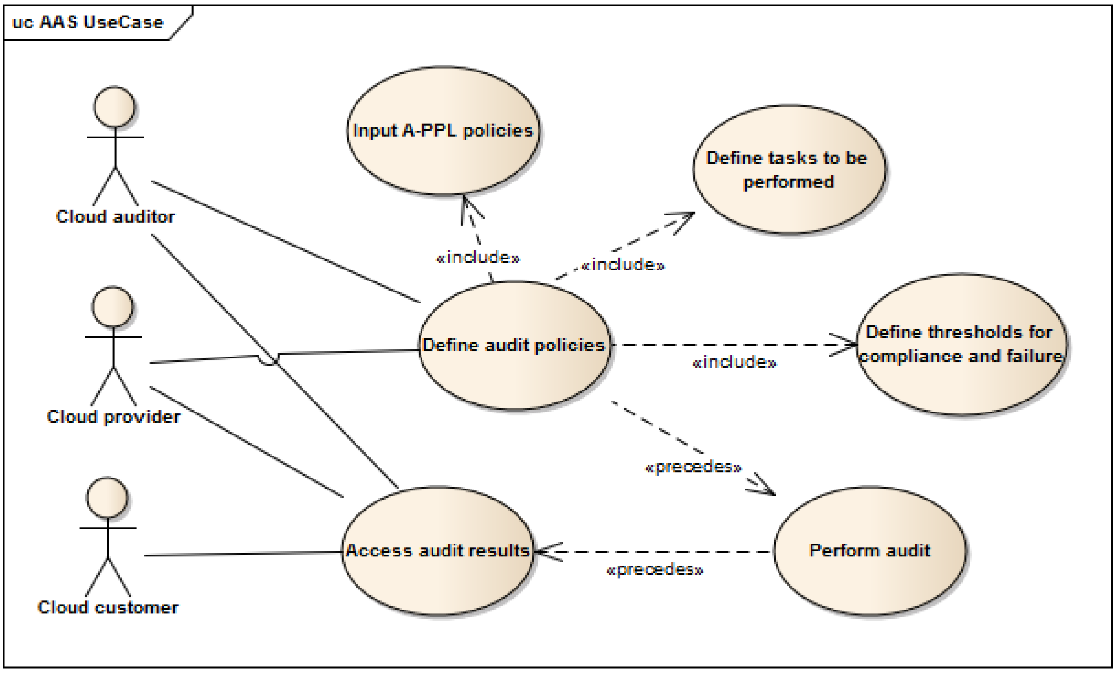


Figure 6: UML use case diagram of the Audit Agent System

The task analysis for the Audit Agent System is presented in Appendix A.2. As can bee seen, the main purpose of the tool is to help the auditor and the cloud provider to define audit tasks. It also lets the users access the audit results.

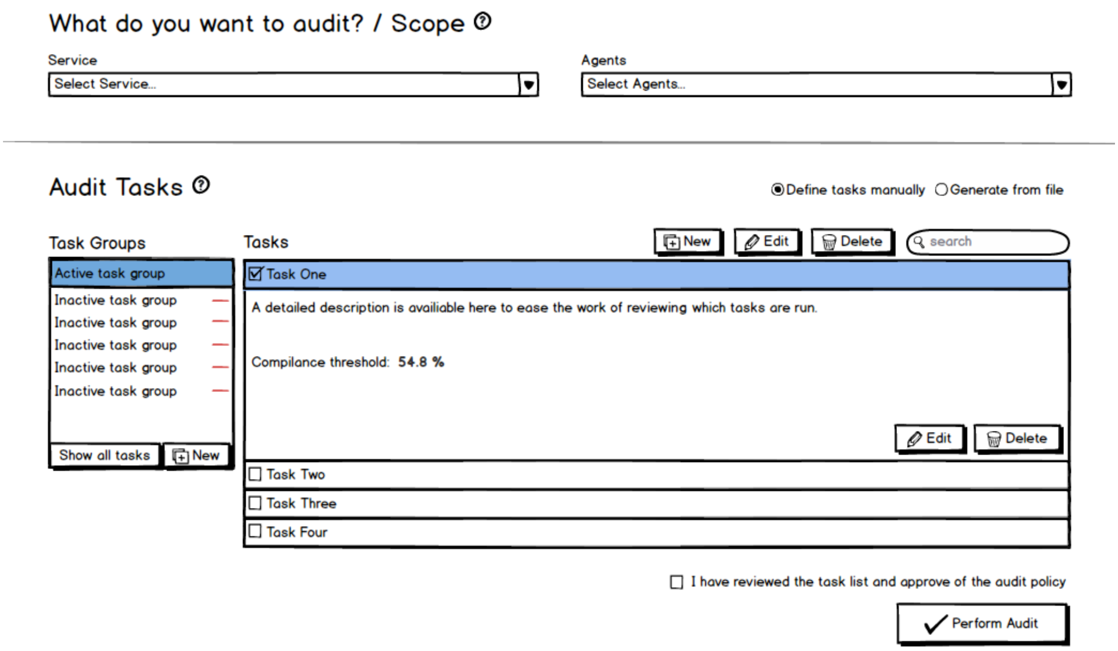
Before an audit can be started, the relevant A-PPL policies are needed in order to compare the actual situation to what the provider has promised (the A-PPL policies can be generated by AccLab, as described in the previous section). The auditor also needs to define the audit tasks to be performedEach task should have a threshold for compliance and failure. This is to make it easy to classify a task as failed or compliant.

When all the above is defined, the audit can be started and the audit results eventually accessed.

The UML use case diagram depicted in Figure 6 provides a high-level view of what the tool should actually do.

3.2.2. Initial UI prototypes

The following reflections and mock-ups are based on the description of the Agent Audit System, which is available in A4Cloud deliverable MS:D-2.2 by WP:D-2.



What do you want to audit? / Scope ⓘ

Service: Select Service...

Agents: Select Agents...

Audit Tasks ⓘ

● Define tasks manually ○ Generate from file

Task Groups

- Active task group
- Inactive task group
- Inactive task group
- Inactive task group
- Inactive task group
- Inactive task group

Tasks

☑ Task One

A detailed description is availiable here to ease the work of reviewing which tasks are run.

Compilance threshold: 54.8 %

☐ Task Two

☐ Task Three

☐ Task Four

☐ I have reviewed the task list and approve of the audit policy

Figure 7: An example of how a user can define an audit by using AAS

Perform Audit When defining a new audit, the tool could present the users with a screen allowing them to define the service and the agents to be involved in the audit. It could also allow the users to either upload a file that defines the tasks to be performed, or the user could define the tasks themselves using the graphical UI.

The interface could be divided in two units as shown in figure 7; one part defining what to audit and the other defining how the audit should be performed. This could be implemented as a wizard, however, we think such a solution would introduce unwanted complexity for expert users. (The main target group of users of this tool is auditors, who might be considered expert users.)

If the users choose ”Generate from file”, they could be presented with a form allowing them to upload a file containing pre-defined tasks to be executed during the audit. To further enhance the usability of the system, the users could be allowed to create collections of tasks to choose from at a later point of time, instead of having to define tasks manually or uploading files.

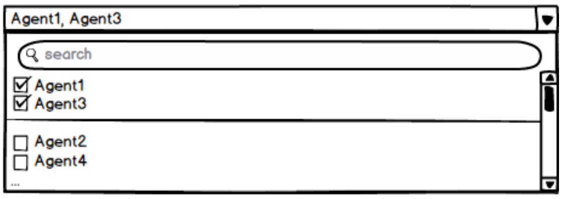
The buttons on top of the task list in figure 7 should only be active when applicable, that is when one or more tasks have been selected. The notable exception is the ”New”-button, which could be active at all times.

Grouping of tasks could be provided as a way for the users to organize and keep track of all the tasks that are to be executed. Providing the users with an easy way of getting an overview of the tasks will lead to be users feeling more in control and as such being more comfortable with using the tool.

When the users clicks on a task, the task could open and present the users with details about the task as exemplified with ”Task One” in figure 7. The tool could also provide the users with the ability to search the list of tasks. It should then provide results in two categories: results in the selected group and results in all other groups.

The ”Perform Audit”-button could be placed to the right as this form is multi column. This should be adjusted to be consistent with the rest of the A4Cloud tools.

All of this is part of fulfilling a requirement identified in A4Cloud’s deliverable D:C-7.1[AFHP+13], stating that a standard way of performing audits across the chain of services should be provided.



☑ Agent1
☑ Agent3
□ Agent2
□ Agent4
...

Figure 8: Selecting multiple agents in AAS could be done using a composition of well-known widgets

Multi select When selecting multiple agents to be involved in the audit, an alternative approach to the common multi select widgets might be needed. The common multi select widget has some serious usability issues like e.g. it is not intuitive how to use it; if a user forgets to press CTRL or CMD while clicking an item, all prior selections disappears.

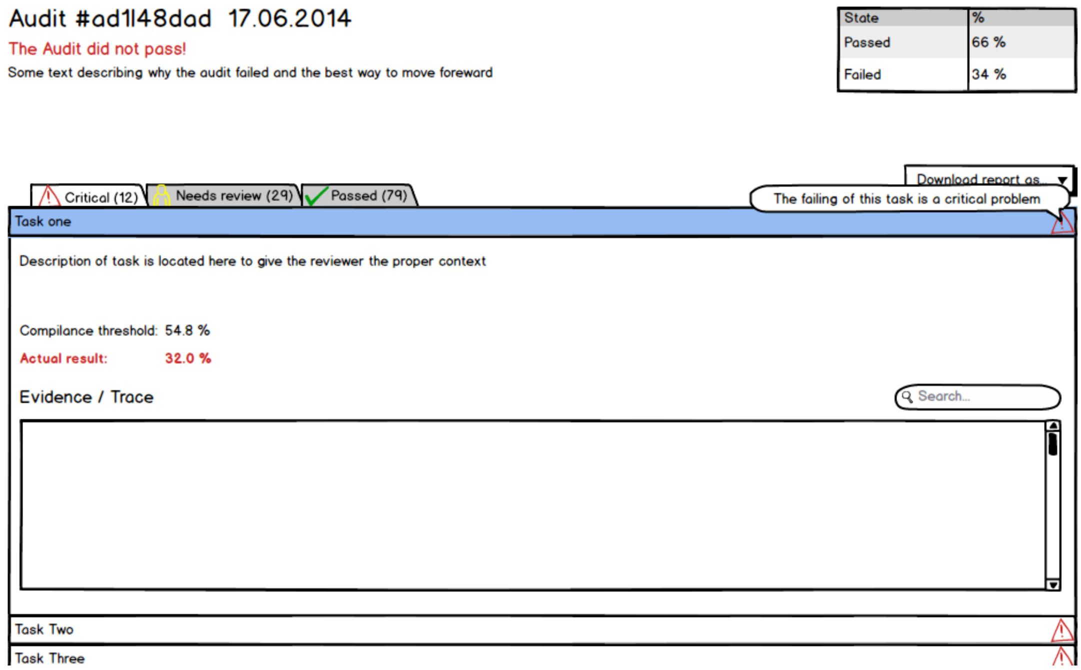
One possible way of solving this issue is combining elements well known to most users, creating an alternative and hopefully more intuitive way of doing multiple selects. This is exemplified in figure 8.

The users could be allowed to search for items in the list, making it easier to find what they are looking for in long lists. Selecting an item could be done with checkboxes as these are well known to most users.

In order for the users to easily keep track of which items are selected, the tool could move selected items to the top. This would help the users to get an overview with very little effort, thus feeling more in control. Usability tests should be conducted on whether the selections should be moved to the top, duplicated on the top or only written in the select header.

When a selection is made, the text visible when the dropdown is closed could be updated with a list of the selections. This would give the users an overview of the selected items, in cases with few selections, without opening the dropdown. For cases with many selections, the text could be ”Agent 1, Agent 3 ... and 15 more”.

Similar implementations include e.g. tagging people in Facebook and Bootstrap Multiselect.



Audit #ad1l48dad 17.06.2014

The Audit did not pass!

Some text describing why the audit failed and the best way to move foreward

State	%
Passed	66 %
Failed	34 %

Description of task is located here to give the reviewer the proper context

Compilance threshold: 54.8 %

Actual result: 32.0 %

Figure 9: The user is provided with an overview of the results. If needed, more details can easily be viewed.

Access audit results The audit results could be presented like exemplified in figure 9.

The users could be provided with general information about when the audit was run, the identification number and some statistics about how many percent of the tasks that have passed and how many failed.

A simple statement could also be added, giving the users a clear statement on whether the audit passed or not. The tool could also offer the users an explanation on why the audit failed and some advice on the best way to move forward from a failed audit.

The audit tasks could be divided in groups, making it clear to the users that the failings has different severity levels as well as making the failings more navigable for the users. A possible grouping could be: “Critical”, “Needs review” and “Passed”. The tab with critical failings should be selected as default.

As with the user interface for adding tasks, one could allow the users to review the details of each failing inline by clicking on a particular task. When displaying the details of the failed task, the tool should provide the users with information about the required as well as the actual result.

The evidence (or trace, depending on the nature of the audit task), should be easily accessible to the users. If the evidence is a textual trace, it could be displayed directly in the tool for the users to inspect. If the evidence is located in one or more files the tool could allow the users to download them.

Since the format of the evidences might vary, it might not be practical or even desired for all users to review and investigate the audit results directly within the tool. The users could therefore be offered the ability to download the audit results in an appropriate format, e.g. PDF for text or a .zip archive for evidence files.

3.2.3. Verification against use case scenarios

In this subsection we analyse to what degree the current version of the Agent Audit System is able to address the concerns of the personas described in the A4Cloud project deliverable DB3.1 [BFS+13].

First we outline the scenarios that describe the activities that are related to auditing a system and then we briefly summarize whether the Agent Audit System will be useful in these scenarios.

Scenario 1.1.1c: Kim This scenario describes how Kim, who is an individual end user, uses a tool to confirm whether his data has been used in accordance to what has been agreed and in accordance with legal requirements. Even though Kim is not an intended user of the Agent Audit System (the tool is targeted towards cloud auditors, providers and customers), the tool will indirectly be of use, since Kim can be provided with copies of the audit reports that the tool produces.

Scenario 3.1.1c-e: Michael These scenarios describe how Michael, who is privacy officer at a cloud customer, uses a tool to check the service providers compliance towards the agreed upon contracts and collect evidence about whether policies are enforced or not. The Agent Audit System will help Michael with these tasks.

Scenario 4.1.3a: Peter This scenario describes how Peter, who is a senior system architect at a cloud service provider, uses a tool to audit cloud infrastructures getting an overview of current configuration of sub providers and notify him on policy violations. The Agent Audit System can be of help with this task.

Scenario 5.1.1a: Bruce This scenario describes how Bruce, who is an infrastructure manager at a cloud provider, uses a tool to audit cloud infrastructure. The Agent Audit System can be of help with this task of auditing a cloud system. By examining the collected evidence, he is able to identify locations, verify transfers and identify who had access to the data.

Scenario 6.1.1a: Leslie This scenario describes how Leslie, who is a senior advisor at a data protection authority, uses a tool to review evidence of the collection and processing of data at a cloud provider. The Agent Audit System can be of help with this task, allowing for collection, review and downloading evidence.

Scenario 7.1.1b: Alice This scenario describes how the cloud provider is able to provide evidence of correct data handling. The Agent Audit System can be of help with that task.

Scenario 8.1.1a: Bob This scenario describes how Bob, who is a business analyst on personal data, uses a tool to perform an internal audit to verify that data is deleted on time. The Agent Audit System can be of help with this task, provided that one can define the time span to examine in each task defined in the Agent Audit System.

Scenario 9.1.1a: Charles This scenario describes how Charles, who is a developer working on a cloud service, uses a tool to check the compliance with the defined policies by audition to ensure that the mechanisms were correctly enforced. The Agent Audit System can be of help with this task.

Scenario 12.1.1a-b: Frank This scenario describes how Frank, who is a data protection officer with experience in auditing IT systems, uses some tools to evaluate policy violations, access evidence and verify whether the necessary risk and privacy impact assessments were correctly conducted and mitigation plan were put in place. The Agent Audit System can be of help with evaluating violations, collecting evidence and verifying risks and mitigations – provided that the evidence collector has access to the logs of the other tools in the A4Cloud tool chain.

Scenario 14.1.1a: Paul This scenario describes how Paul, who is the Chief Privacy Officer of a SME moving most of their services to the cloud, uses a tool to provide evidence of compliance with respect to relevant legislative regimes. The Agent Audit System can be of help with this task.

Scenario 15.1.1a: Roger This scenario describes how Roger, who is the Chief Technology Officer of a cloud service provider, accesses policy compliance information about alternative cloud infrastructure providers. Provided that his company is part of the accountability chain, the Agent Audit System can be of help with collecting evidence and accessing information about policy compliance.

Scenario 16.1.1a-b: Michael These scenarios describe how Michael, who is a cloud auditor, assesses regulatory and data policy compliance of cloud service providers by accessing collected evidence. The Agent Audit System can be of help with these tasks by collecting evidence and presenting it to Michael.

Scenario 17.1.1a: John This scenario describes how John, a regulator at a data protection authority, investigates reported data protection infringements by reviewing evidence of parties involved. The Agent Audit System can be of help with this task, collecting and presenting the required evidence.

Scenario 18.1.1b: Sandra This scenario describes how Sandra, an individual employee and end user, holds the cloud service provider accountable for the handling personal data. The Agent Audit System might be of help with this task, even though she is not an intended user, in a similar manner as in Scenario 1.1.1c.

Scenario 20.1.1a: Peter This scenario describes how Peter, who works for a healthcare cloud service provider, can be held accountable for the handling of Personally Identifiable Information. The Agent Audit System can be of help in this area by allowing Peter to audit the systems and providing relevant information to correct any discrepancies, thus making him less liable.

Most identified use case scenarios are fulfilled by mock-ups and tool description. Scenario 1.1.1c and 18.1.1b is only fulfilled if unintended users are given access to the tool.

3.3. Cloud Offering Advisory Tool (COAT)

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

The users will also be provided with explanation of potential risks.

In order for the tool to give the users relevant comparisons, the users need to provide the tool with the necessary information. This is done by answering questions. This is the first way the tool interacts with the users through a graphical user interface.

The second way the tool interacts with the users through the graphical user interface is when presenting the report that includes the comparison between different service offerings.

3.3.1. Users goals and task analysis

As can be seen in the task analysis in section A.3, the main purpose of the Cloud Offering Advisory Tool is to help the users select an appropriate service.

In order to accomplish this, the tool supports the users by allowing them to select services and user types, or to search for specific services, and tries to make it possible for the users to understand the service offers and properties.

Based on the selected service and user type, the tool is able to provide suggestions for requirements that the users might use, or the users can provide their own requirements using a parameter interface. Based on these requirements, the tool presents relevant service offers to the customer.

When the users searches for a specific service or views a list of service offers, the tool presents each service offer to the users upon their request and, as such, helps them understand the service offers and their properties. It is also possible to select service offers for comparison.

The cloud provider is able to add his service offer to the offer repository. The UML use case diagram depicted in Figure 10 provides a high-level view of what the tool should actually do.

3.3.2. Initial UI prototypes

The following reflections and mock-ups are based on the description of the Cloud Offering Advisory Tool, made available in A4Cloud deliverable MS:D-2.2 by WP:D-2.

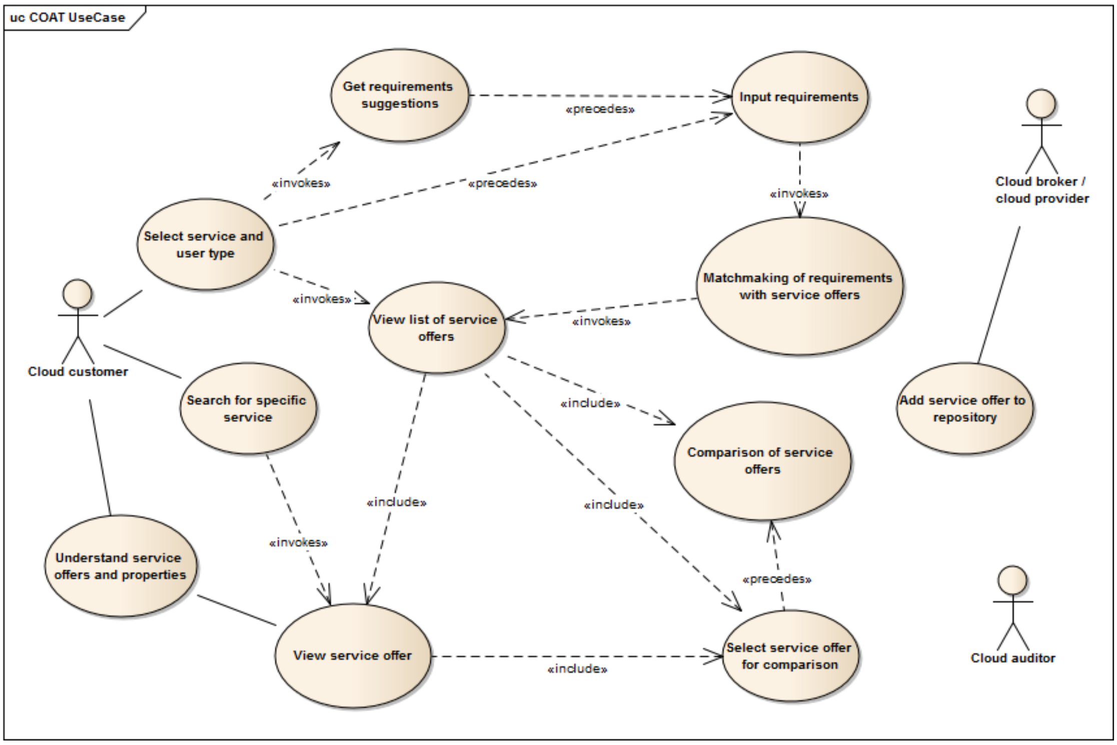
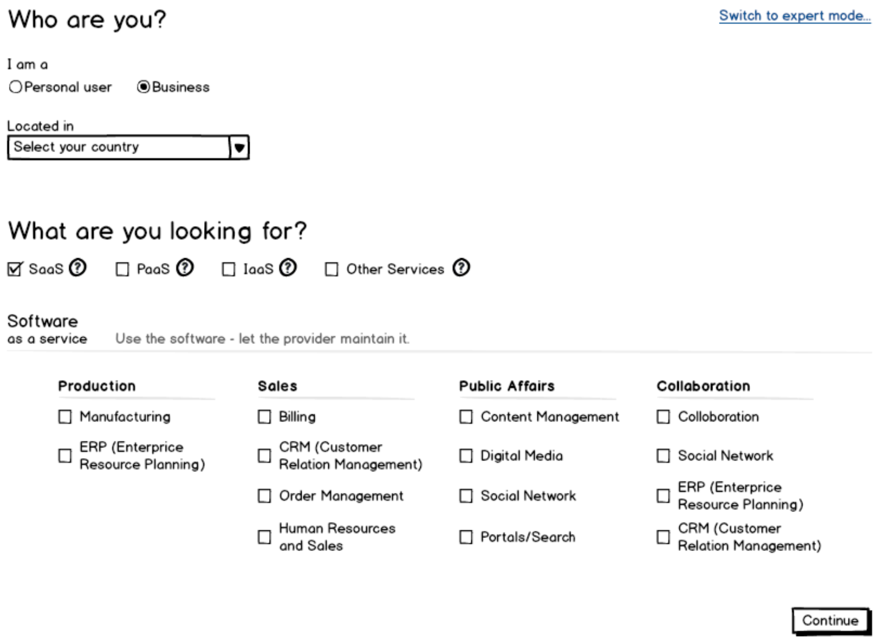

uc COAT UseCase
Get requirements suggestions
«precedes»
Input requirements
«invokes»
«precedes»
«invokes»
Cloud broker / cloud provider
Select service and user type
Matchmaking of requirements with service offers
«invokes»
View list of service offers
«invokes»
Cloud customer
Add service offer to repository
Search for specific service
«include»
Comparison of service offers
«include»
«include»
«invokes»
Understand service offers and properties
«precedes»
Cloud auditor
View service offer
«include»
Select service offer for comparison

Figure 10: UML use case diagram for COAT



Who are you?

Switch to expert mode...

I am a

○Personal user ●Business

Located in

Select your country ▾

What are you looking for?

☑ SaaS ? □ PaaS ? □ IaaS ? □ Other Services ?

Software
as a service Use the software - let the provider maintain it.

Production

□ Manufacturing

□ ERP (Enterprise Resource Planning)

Sales

□ Billing

□ CRM (Customer Relation Management)

□ Order Management

□ Human Resources and Sales

Public Affairs

□ Content Management

□ Digital Media

□ Social Network

□ Portals/Search

Collaboration

□ Collaboration

□ Social Network

□ ERP (Enterprise Resource Planning)

□ CRM (Customer Relation Management)

Continue

Figure 11: The user provides context through a parameter interface

Parameters and offers When the users chooses to seek the advice of COAT, they could be presented with a simple screen asking them if they are an individual person, or if they are representing a business. They could also be asked where they are located (for example in Europe). They could also be asked what type of service they are looking for. This can be seen in figure 11.

Then only the type of services that the users are looking for could be shown. This is to avoid a wall of text, and the users spending an unnecessary amount of time to locate the ones of interest. To further simplify the users' search for the relevant option, the options could be grouped under generic headers, as exemplified in figure 11. One option could belong to multiple groups.

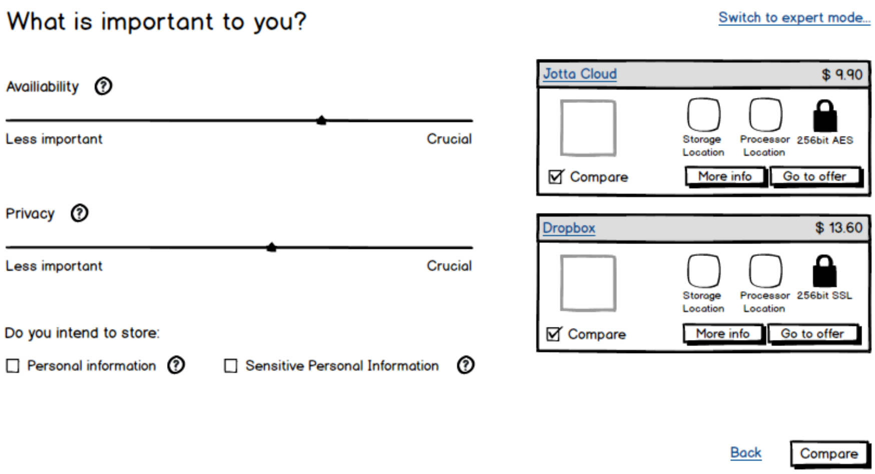


Figure 12: The user provides requirements through a parameter interface

Based on the answers provided, they could be presented with another round of parameters, seeking to get a high level overview of what is important for the particular user in this particular use case - as shown in figure 12. This would enable the tool to pre-set all the parameters in the easy mode, while contributing to sensible defaults in expert mode.

The users could also be asked if they intend to store personal data, and if yes, if these data are sensitive (such as medical information). The selection of either one, combined with the information about what country the users are located in, could give the user service offers that comply with the legislation that applies in the stated country. This information could be communicated to the users, thus teaching them about the applicable laws. If the users choose to switch to expert mode, this would contribute to sensible defaults.

When the users select the checkbox stating that sensitive personal data will be processed, and tries to set "Privacy" as "Less important" they could be informed that this might cause compliance issues with applicable legislation.

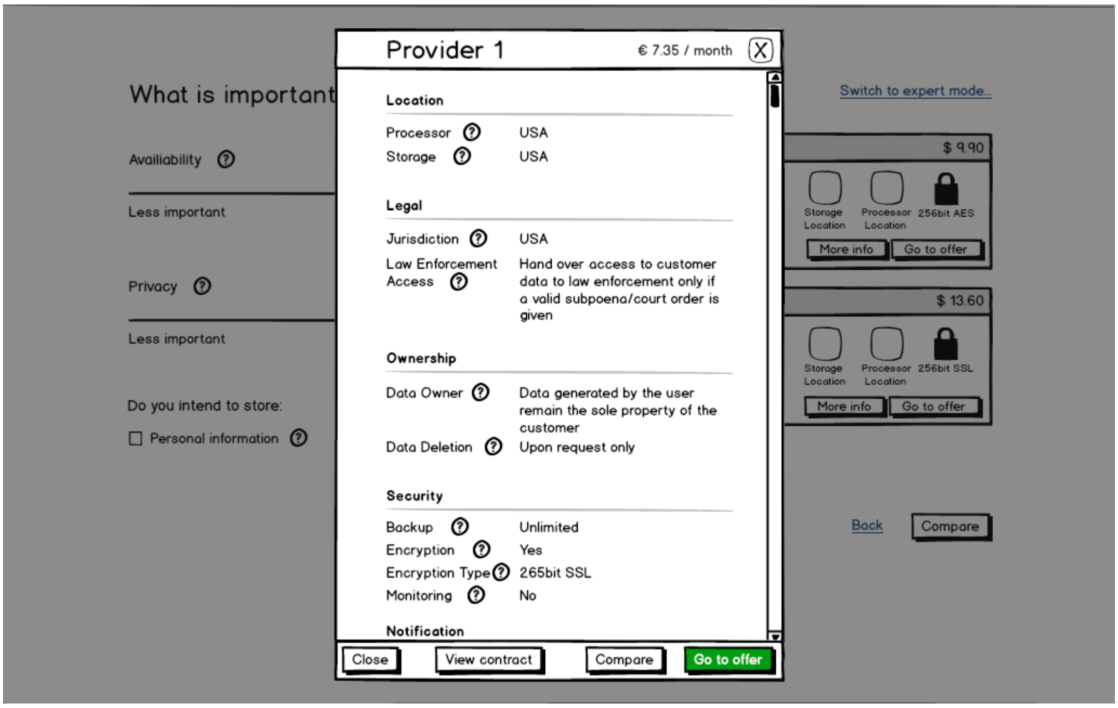
Allowing the users to be in control is an important principle to making the users feel comfortable and confident using a user interface. Therefore, the help system should not be automatically engaged, but rather be activated by the users upon need. In the prototype developed by WP D-4, the help text is shown when the user hover with the mouse over the requirement question to make the user aware of the explanation.

The users could be offered the opportunity to use the tool in expert mode, which would present more questions and require more in-depth knowledge.

The list of offers matching the criteria specified by the users, are placed on the right. The list is dynamically updated as the users update their criteria. Ideally this will contribute to a raised awareness amongst the users as they see service offers disappear from the list when conflicting criteria are selected. This might also lead to users adjusting their criteria to match those of their favoured service, but that would a judgmental error on the users' part – not necessarily something to handle within this tool, other than to inform and warn the users against choices of non-ideal nature.

The sketch in figure 12 uses a padlock to indicate encryption. At the moment the same padlock is used independent of the encryption strength, which might be a problem as padlocks are used to reassure users that a system is secure while not all SSL encryptions really is (e.g. 64bit DES). As users are trained to recognize the padlock as a sign of trust, some indicator should be used to inform them about the level of trust. This could be, for example, another type of icon, different colours on the padlock (e.g. red for insecure, yellow for acceptable for non-sensitive information, green for good) or a visual indicator for security completeness (e.g. a cake diagram combined with colours like red, yellow and green).

By selecting multiple offers and pressing "Compare", the users are able to compare the properties of two or more different offers.



Provider 1 € 7.35 / month

Location

Processor ⓘ USA
Storage ⓘ USA

Legal

Jurisdiction ⓘ USA
Law Enforcement Access ⓘ Hand over access to customer data to law enforcement only if a valid subpoena/court order is given

Ownership

Data Owner ⓘ Data generated by the user remain the sole property of the customer
Data Deletion ⓘ Upon request only

Security

Backup ⓘ Unlimited
Encryption ⓘ Yes
Encryption Type ⓘ 265bit SSL
Monitoring ⓘ No

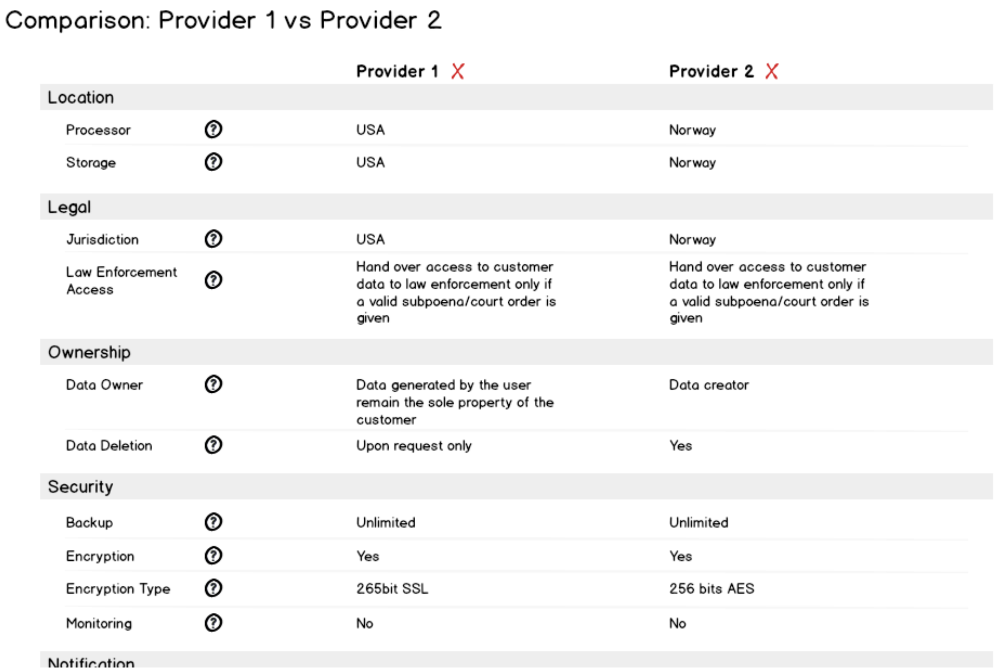
Notification

Figure 13: The user reviews the details of a provided offer

Details When the users choose to examine an offer in more detail, they could click the “More info”-button and get an overlay on the screen similar to the one exemplified in figure 13.

The information should be structured and grouped in order to increase the comprehensibility, and each parameter or property should offer help to the users. This help should also use a pane on the right as mentioned above. Presenting the policies and terms of service in such a manner, will help fulfil the requirement from A4Cloud deliverable D:C-7.1 [AFHP+13], which states that easily comprehensible polices should be provided.

Given that the users have opened the offer to examine it more closely, it is likely that they consider accepting the offer. Therefore, the button “Go to offer” stands out among the others, as it is the primary button on the page. It could also be possible for the users to view the contract of the offer, to add the offer to the comparison and also to close the offer if they are not ready to take it.



Comparison: Provider 1 vs Provider 2

		Provider 1 ✗	Provider 2 ✗
Location			
Processor	?	USA	Norway
Storage	?	USA	Norway
Legal			
Jurisdiction	?	USA	Norway
Law Enforcement Access	?	Hand over access to customer data to law enforcement only if a valid subpoena/court order is given	Hand over access to customer data to law enforcement only if a valid subpoena/court order is given
Ownership			
Data Owner	?	Data generated by the user remain the sole property of the customer	Data creator
Data Deletion	?	Upon request only	Yes
Security			
Backup	?	Unlimited	Unlimited
Encryption	?	Yes	Yes
Encryption Type	?	265bit SSL	256 bits AES
Monitoring	?	No	No
Notification			

Figure 14: The user compares different offers

Comparison When comparing offers, it could be done in a table layout like the one shown in figure 14.

If the list of parameters is long, the name of the provider or the offer should be stated at the top of each information group. Otherwise it is sufficient to place it on top of the comparison table. This is to save the users the time of scrolling to the top to remember which column was which provider, should they ever forget. An alternative approach is to make the top most row stay visible on the top even when the users scroll further down the page.

Allowing the headers of each data group to have a different formatting and indentation as well as a full with visual indication, helps the users to identify information fast as well as increase readability.

The users could be allowed to remove offers from the comparison, allowing them to easily dismiss offers that turn out to not be of a desired standard. This could be done by adding a button or a red x next to the name of the offer or provider.

As can be seen in figure 13 and 14, the placement of the help icon differs. The first one has the icons placed at the end of the word in question, while the second has all the icons placed along a vertical line. The first one gives better visual feedback of where it belongs, while the second gives a more orderly impressions and as such might contribute a better user experience. One of the options should be chosen, and implemented in both cases.

The criteria specified by the users, and others affected by the high level configuration, should be presented in a highlighted way. This could be done by marking the row, placing the most relevant rows on top without breaking context or by displaying only the relevant rows in the initial comparison matrix and can allow the users to view all upon request. Usability tests should be conducted on which method serves the purpose best.

The different offers may contain lots of free text, making it hard to judge which is better. One way of making this easier could be to introduce colour coding, giving the different cells a grade on how well they fulfil the users' criteria. This might also help the users gain a better understanding on the different properties as well. Take the property of e.g. “Encryption Type”, a novice user might not be able to judge which is better if two offers state respectively “128bit AES” and “256bit MD5”. The tool could therefore educate the users by informing whether or not a property is good in the context of the users' criteria. This would contribute to fulfilling the requirement in A4Cloud deliverable D:C-7.1 [AFHP$^+$13], stating that the reasonable claims about privacy and security policies and technical capabilities should be made to promote trust.

More comparable information, such as the service providers' track records, could also be included. Rather than stating numbers that are vulnerable to manipulation and not easily understood by the users, the model from Ohloh [Ohla] exemplified by Apache OpenOffice could be used. In the example it states complex information about the OpenOffice project in a simplified manner: “In a Nutshell Apache OpenOffice has a code base with a long source history maintained by a very large development team with increasing year of year commits.” Similarly the users could be informed about the state of a provider, like e.g. ”Provider 1 is good at handling incidents and continue getting better over the years.”

The possibility of comparing the different offers, is part of fulfilling the requirement in A4Cloud deliverable D:C-7.1 [AFHP$^+$13], which states that users should be made aware of pros and cons of their possible choices in an unbiased manner.

3.3.3. Verification against use case scenarios

In this subsection we analyse to what degree the current version of the Cloud Offering Advisory Tool is able to address the concerns of the personas described in the A4Cloud project deliverable DB3.1 [BFS$^+$13].

First we outline the scenarios that describe the activities relating to the process of selecting a new cloud provider and then we briefly summarize whether the Cloud Offering Advisory Tool will be useful in these scenarios.

Scenario 4.1.4a: Peter This scenario describes how Peter, who is a senior system architect at a cloud service provider, uses a tool to find an alternative cloud provider who can deliver a given set of functionality and strong guarantees on the collection and storage of personal data. The Cloud Offering Advisory Tool will be of help with this task, allowing him to specify his requirements and provide him with a list of service offers to review.

Scenario 15.1.1e: Roger This scenario describes how Roger, who is the Chief Technology Officer of a cloud service provider, uses a tool to assess risk associated with alternative cloud providers. The Cloud Offering Advisory Tool can be of some help with this task, allowing him to specify requirements and provide him with a list of offers for comparison. However, the current version of the prototype implemented by WP D-4 and the mock-ups presented in this deliverable do not provide him with information about risk.

Most identified use case scenarios are fulfilled by mock-ups and tool description. If proper integration with the Data Protection Impact Assessment tool (DPIAT) is implemented, scenario 15.1.1e will be fulfilled to completion as well.

3.4. Data Subject Access Request Tool (DSART)

According to the description of WP:D-4 (in the Milestone document MS-D4.1) the purpose of the Data Subject Access Request Tool (DSART) is to allow individual cloud subjects to assert their rights to access their personal data held by a data controller (e.g., cloud service provider). This right is based on Article 12 of the EU Data Protection Directive 95/46/EC that grants data subjects with the right of access to their data. This comprises the right to information about the data being processed, the purposes for processing such data, the recipients or categories of recipients of the data, as well as information about the logic involved on any automatic processing of the data (Art. 12 (a)). This data subject rightis also a prerequisite for exercising the data subject rights to correct, erase or block data that are not processed in compliance with the Directive (Art. 12 (b)).

Moreover, the proposed EU General Data Protection Regulation (GPDR) [Eur12], with its Art. 15, also requires data controllers to include information about the data retention periods, the right to lodge a complaint with the supervisory authority, and “the significance and envisaged consequences” of the data processing, at least in the cases of profiling. The data subjects shall also have the right to obtain this information electronically if they have made their requests in an electronic format. Besides, the recently amended text of the proposed GPDR [Eur13] that was passed by the European Parliament even states that “where possible, the data controller may provide remote access to a secure system which would provide the data subject with direct access to their personal data”.

The DSART will hence allow cloud subjects to exercise this right by allowing them to request to see a copy of the information an organization holds about them.

As discussed in A4Cloud MS-D4.1: “In the context of data subject access requests there are two distinctions that need to be made in order to understand the scope of the DSAR tool: role of the user and type of data. The user of the tool may be an individual using the cloud as an end-user (Individual Cloud Customer), or (s)he may be a data subject, whose data are being processed by a data controller who makes use of the cloud (Individual Cloud Subject). In the former case, the individual is an active entity employing cloud services, in the latter (s)he is a passive entity, often lacking knowledge what data exactly are being processed by the cloud customer (who acts as a data controller in DPDP terms). Second, it is useful to distinguish between volunteered, observed, and inferred data. Volunteered data are the personal data disclosed by the individual. In theory, the user is aware of (the contents of) these data. Next to these data, a cloud provider may also observe data about the individual or infer data from other data. The DSAR concerns all three types and hence the result of invoking a data subject access request may entail much more data than just volunteered data.”

The Data Track (Section 3.5) aims at providing cloud subjects direct electronic access to their data that they disclose explicitly or implicitly or that is inferred about them, as well providing information about how their data is being used, and whether these have been transferred to third parties.

The DSART is connected to the Data Track and extends its functionality by granting cloud subjects the option to request their data or further information in regard to the handling of their data offine by helping them to draft a (paper or electronic) mail request.

3.4.1. Work flow for a data subject access request function extending the PRIME Data Track

Within the scope of the EU FP6 project PRIME[3], we have already elaborated the workflow for compiling a data subject request as an extension to the PRIME Data Track. This work flow is displayed in Figure 15 and is discussed in more detail in [FHPB+07]. The DSART tool could basically follow a similar work flow. Nevertheless, whereas the work flow in Figure 15 also includes steps for contacting the supervisory authority in charge in case that a data controller is not answering to the data subject access request in time, the task analysis for DSART that we present below addresses so far only the first steps for contacting the data controller with the data subject access request.

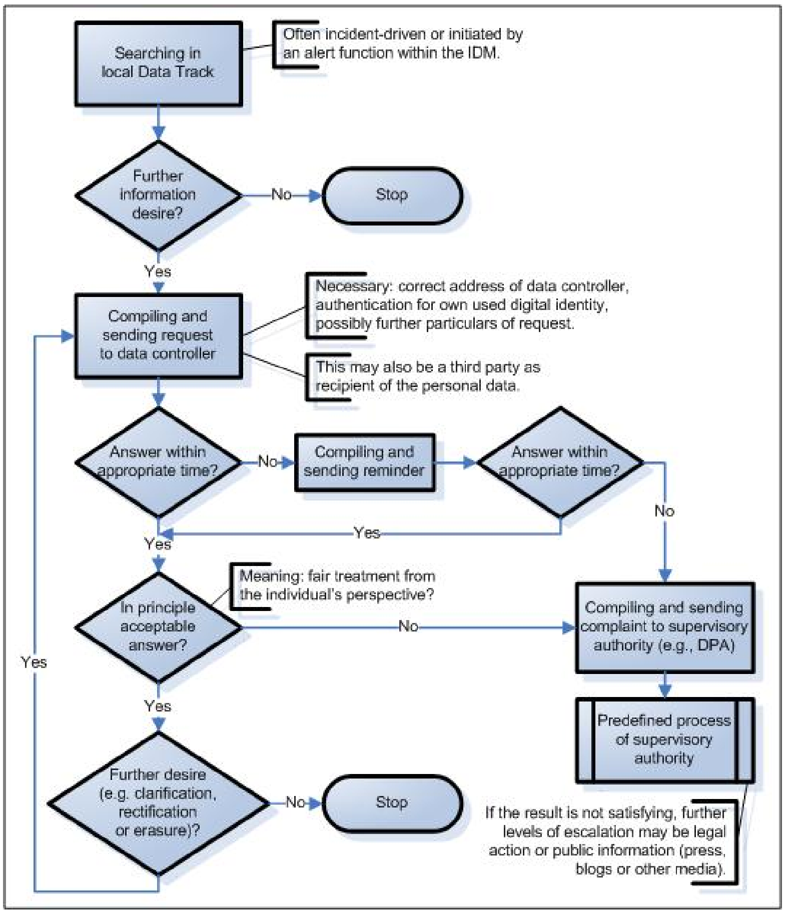

Searching in local Data Track
Often incident-driven or initiated by an alert function within the IDM.
Further information desire?
No
Stop
Yes
Compiling and sending request to data controller
Necessary: correct address of data controller, authentication for own used digital identity, possibly further particulars of request.
This may also be a third party as recipient of the personal data.
Answer within appropriate time?
No
Compiling and sending reminder
Answer within appropriate time?
No
Yes
Yes
Meaning: fair treatment from the individual's perspective?
In principle acceptable answer?
No
Compiling and sending complaint to supervisory authority (e.g., DPA)
Yes
Yes
Predefined process of supervisory authority
Further desire (e.g. clarification, rectification or erasure)?
No
Stop
If the result is not satisfying, further levels of escalation may be legal action or public information (press, blogs or other media).

Figure 15: Flow diagram for a Data Subject Access Request function extending the PRIME Data Track showing the steps to be taken for exercising and supporting user rights, taken from [FHPB+07]

[3] EU FP6 project PRIME, `https://www.prime-project.eu/`

3.4.2. User goals and task analysis

The following paragraphs describe the necessary steps or tasks that a user would have to carry out in order to successfully submit a data access request to a cloud service provider.

Currently, there are two foreseen ways to let cloud subjects submit a request to a cloud provider, one is by actively searching or filtering a given list of providers that have the cloud subjects' data, and the other by selecting a provider when browsing the cloud providers via the Data Track tool which provides an overview of the services to which the cloud subject has made a data disclosure.

Once the correct cloud provider has been identified, the cloud subject can select between different types of requests. Cloud subjects can choose to request all personal data located at a particular cloud service provider, with the possibility to filter out the data requested by the way that data was collected (either explicitly sent by the user, implicitly collected by the provider, or inferred by analysis), as well as by the category of data (e.g., medical, financial, etc.). Moreover, cloud subjects can request to be informed about the motivation behind decisions done by the provider based on the data that they hold. In this scenario, cloud subjects would select the appropriate case from a list of decisions or applications, and fill remaining required information. The tool will then create an automatic request which will be presented to the user. If everything seems in order the user is given the option to confirm or to edit the request. Once the cloud subject has confirmed the request she can choose between printing it for offline submission, send it by email, or submit it electronically via the Data Track. At the end, the cloud subject will be presented with some kind of confirmation of the transaction and possible information on how and when an answer can be expected by the provider.

The UML diagram depicted in Figure 16 provides a high-level view of what the tool should actually do.

3.4.3. Initial UI prototypes

Based on the task analysis (see Appendix A.4) and the information about the functionality of the tool provided by other A4Cloud work packages, we present some initial mock-ups of the possible functionality of the DSART.

The idea depicted in Figure 17 allows a user to filter through service providers that hold her data, which is similar to the functionality that has been envisioned in the Data Track (Section 3.5). The interface allows users to choose the type of data that they want to request access to at a particular point, or request access to all the data at the provider. The "Request" button for every type of data also has the immediate option to submit the request by email or to get a hard printed copy of the request.

In the step shown in the figure, it is be possible for users to make many requests to different service providers in a "shopping cart" fashion, in which the user can see and confirm her selection of the different requests to access her various types of data to the different providers.

If DSART is used as a stand-alone tool not connected with the Data Track, the data subject can refer to specific data types or to all data that a data controller has about the user and that that the user would like to be informed about. Request to access data is also possible through controls in the Data Track interface, which will be described in Section 3.5. In this case, users

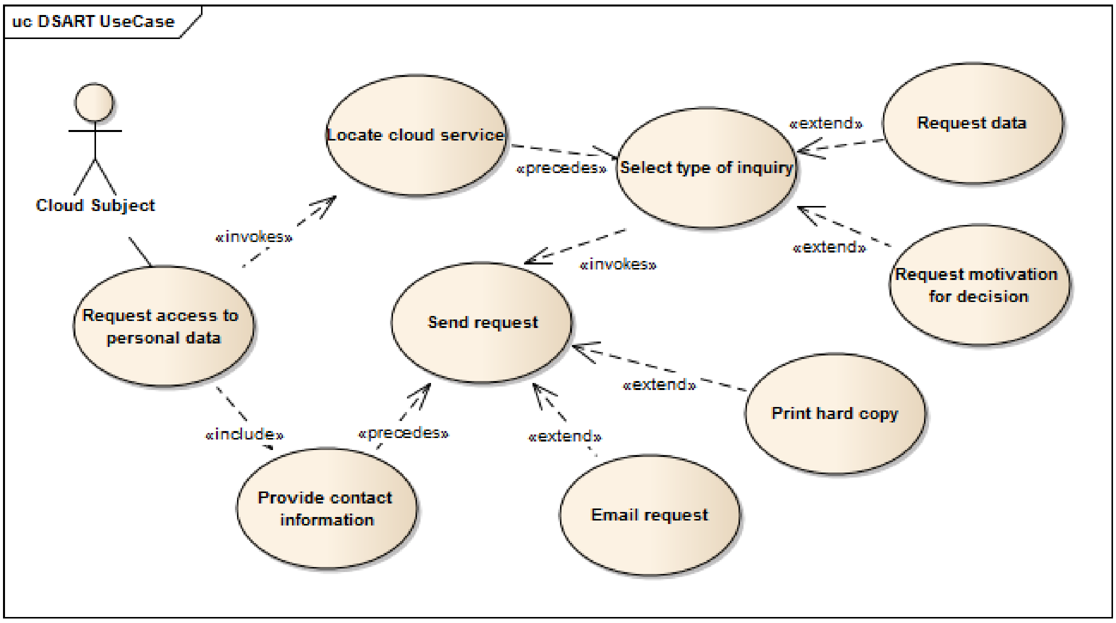


Figure 16: UML use case diagram of the Data Subject Access Request Tool

are able to view first the data or types of data[4] that they disclosed to different data controllers and and then send data subject access request 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 (e.g., in regard to how this data has been processed or whether it has meanwhile been deleted or not).

3.4.4. Verification against use case scenarios

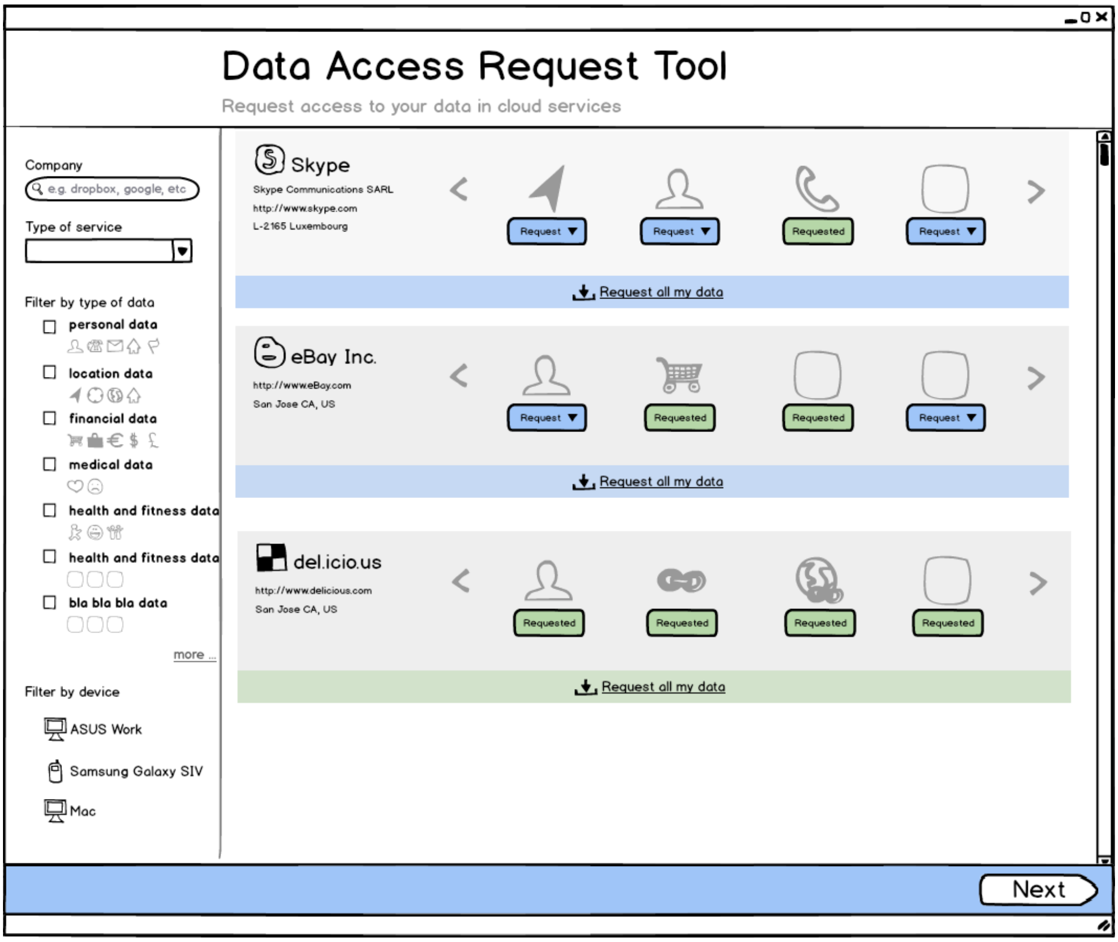
In this subsection, we analyse to what degree the current version of the Data Subject Access Request Tool is able to address the concerns of the personas described in the A4Cloud project deliverable DB3.1 [BFS$^+$13].

Below, we outline the scenarios that describe the activities that happen in relation to an access request:

Scenario 1.1.3a: Kim This scenario describes how Kim, an individual end user, uses a tool to confirm that a cloud service do no longer hold any personal data related to his person. The Data Subject Access Request Tool is one tool that could help him fulfill this task, by allowing him to request what data about him the service holds.

The identified use case scenario is fulfilled by mock-ups and tool description.

[4] The data classification into data types is in this case enabled by ontologies used by the Data Track. These can be ontologies provided by A-PPL or by schema.org



Data Access Request Tool

Request access to your data in cloud services

Skype
Skype Communications SARL
http://www.skype.com
L-2165 Luxembourg

eBay Inc.
http://www.eBay.com
San Jose CA, US

del.icio.us
http://www.delicious.com
San Jose CA, US

Figure 17: Users can user DSART to request access to certain types of data or to all the data located at different cloud service providers.

3.5. Data Track (DT)

As part of the European FP6 and FP7 research projects PRIME[5] and PrimeLife[6], the Data Track tool was developed [PFHB07], [FHHW11]. Initially, the PRIME Data Track comprised of a history function for keeping a log of each transaction in which a user discloses personal data. The log contained a record for the user about which personal data were disclosed to whom, for which purposes, which credentials and/or pseudonyms have been used in the context of the disclosure as well as the details of the agreed-upon privacy policy. These transaction records were stored at the user side in a secure manner (protected by the PRIME core). In the PrimeLife project and in the follow-up A4Cloud project, the Data Tack was extended to allow cloud subjects to exercise their data subjects' rights pursuant to Art. 12 EU Data Protection Directive 95/46/EC to access their data at the remote services sides online and to correct or delete their data online if the service provider allows it.

In its backend the architecture of the Data Track consists of four high-level components. First, the *user interface* component, which displays different visualizations of the data provided by the Data Track's *core*. Second, the *core* component is a backend to the UI with local encrypted storage. Through a RESTful API, the core is able to provide a uniform view to the UI of all users' data obtained from a service provider via *plugins*. Third, the *plugin* component provides the means for acquiring data disclosures from a source and parsing them into the internal format readable by the core. Fourth, the Data Track specifies a generic *API* component that enables a service provider to support the Data Track by providing remote access, correction, and deletion of personal data. Based on the solution proposed by Pulls *et al.* [PPW13], the transfer of data through a service's API can be done in a secure and privacy-friendly manner. By retrieving data from different services through their provided APIs users would be able to import their data immediately into the Data Track and visualize it in different ways. The possibility to immediately import data into the Data Track and visualize it is an important feature that can add instant value to the tool and provide users with immediate gratification.

The Data Track provides two views which allow the cloud subjects to compare disclosures and detect inconsistencies or policy violations. One view shows the user's locally stored Data Track records and another view lists this user's data currently stored at a remote service provider side.

In the following subsection, the user interface designs for the Data Track will be discussed. In contract to all other A4Cloud tools, the Data Track and its user interfaces were developed and evolved over several research projects and were thus not developed from scratch in A4Cloud, but rather re-designed and improved. For this reason, we did not develop a task analysis and use case diagram for the Data Track as we did for all other tools.

3.5.1. Related work

Two commercial well known and publicly available transparency tools include the initiative from Mozilla's Lightbeam[7], which provides users with different playful visual overviews of the trackers

[5] EU FP6 project PRIME, `https://www.prime-project.eu/`

[6] EU FP7 project PrimeLife `http://primelife.ercim.eu/`

[7] `https://www.mozilla.org/en-US/lightbeam/`

embedded in visited websites and their interactions, and the initiative of the Google Dashboard [Goo] which allows its users to manipulate their data that is stored at Google via standard editing and deleting controls. Google[8] and Facebook are also examples of industrial initiatives that try to comply with recent General EU Data Protection Regulation (GDPR) proposal which discusses data subjects' rights to export their data stored at the service provider.

Research efforts have also discuss the need for *Personal Data Services* and usable visualizations or data disclosures [AKLS13, KNP10, KZH12, ZPK$^+$13]. Some of the identified benefits of a PDS included increased transparency and engagement by users, and the allocation of greater "collective power through their access and use of individual and community level data". Nonetheless, challenges were also recognized, like the possible confusion that users might have between the difference of *owning* their data or *accessing* their data remotely, as well as the issue of making sense of large amounts of data through meaningful visualizations, which is a challenge in many other types of big data collection activities [Dum13, KMSH12, LJH13, Wol13].

Data visualizations and personal disclosures For the design of the Data Track tool, we have considered the inclusion of different methods for visualizing data disclosures in a way that is connected to the users' momentary intentions. For instance, a timeline view of personal disclosures, as proposed in the mock-up of Figure 18 can be useful at the moment of searching for data that was released at a particular date, but less useful when trying to find out how much data has been sent to a particular service provider, or what personal data attribute has been sent to which service providers.

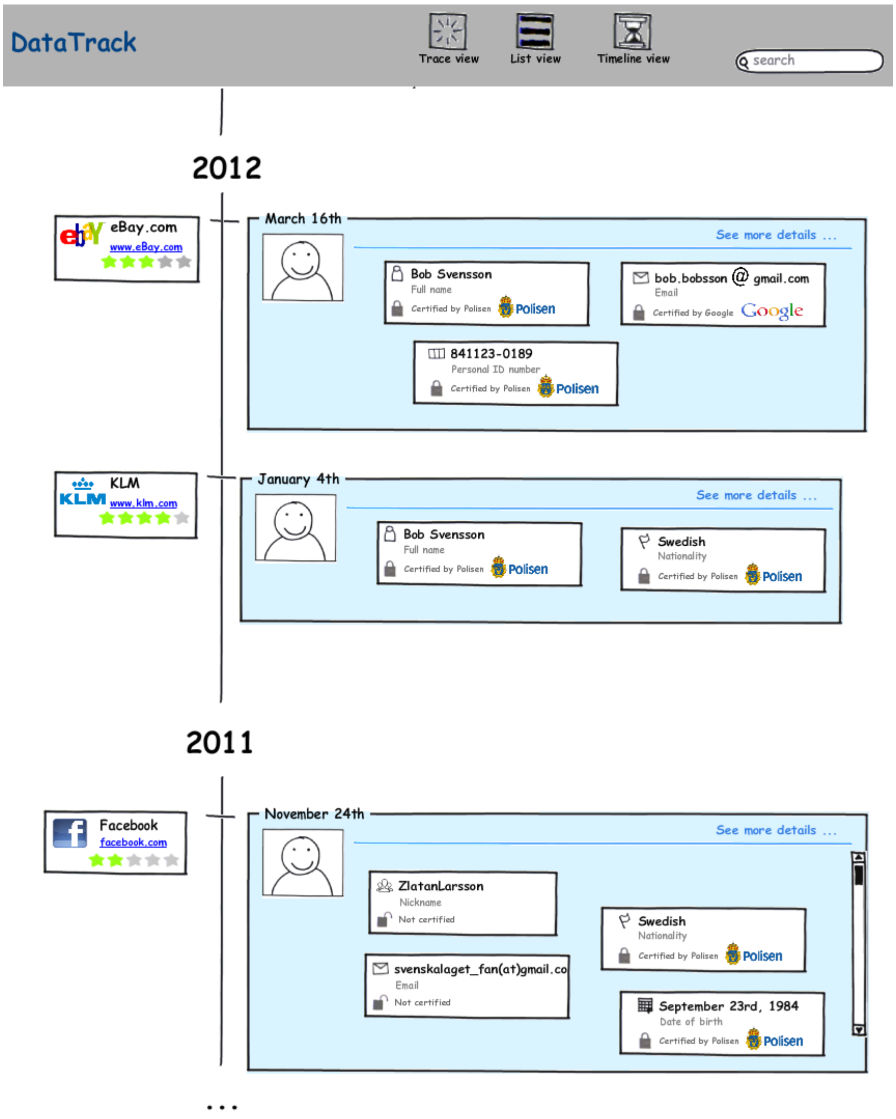
These later questions might be better approached by displaying graphical traces resembling data flows, reflecting how data flows across different entities involved in a data disclosure transaction, as discussed in [Pet08]. In fact, previous research studies suggest that network-like visualizations can provide a simple way to understand the meaning behind some types of data [BNG11, Fre00, KMSH12]. 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 [HL12]. Also, using traces between different online entities in order to visualize data flows and to promote transparency in online commerce has been suggested in [KZH12] and [KNP10]. In [GFC04] diagrams displaying nodes and links have proved to be effective when analysing 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 [PMR$^+$96].

Furthermore, it has been suggested that interfaces for visualizing complex data does not only have to fulfil requirements related to their effectiveness and efficiency, but also to their soundness (i.e., reliability and robustness) and especially their attractiveness [MP11]. Studies have shown close relationships between usability and perceived attractiveness, arguing that users are more forgiving, spend more time and are more likely to want to interact with interfaces that they perceived as attractive [SPSB10, TKI00], but also that good usability can influence the perceive attractiveness of a product [TRH$^+$12]. Similarly, the usability properties of seductivity,

[8] Google Takeout, `https://www.google.com/takeout`

playability, and pliability have also been regarded valuable for the design of digital artifacts [LS07].

During the design work of the Data Track tool we have created various sketches and prototypes for different visualizations of data disclosures that try to fulfil the above mentioned characteristics and adapt to the users' intentions. An example of a lo-fi sketch of a *timeline* view proposed during our design process is shown in Figure 18. However, we have focused our efforts so far on developing and testing a hi-fi prototype for a visualization approach which we call the *trace view*, shown in Figure 20. We started our investigations on various aspects of the users' understanding of their data disclosures with the use of the lo-fidelity mock-ups and interactive prototypes depicted in that figure.



eBay.com
www.eBay.com

March 16th
See more details ...

Bob Svensson
Full name
Certified by Polisen Polisen

bob.bobsson @ gmail.com
Email
Certified by Google Google

841123-0189
Personal ID number
Certified by Polisen Polisen

KLM
www.klm.com

January 4th
See more details ...

Bob Svensson
Full name
Certified by Polisen Polisen

Swedish
Nationality
Certified by Polisen Polisen

Facebook
facebook.com

November 24th
See more details ...

ZlatanLarsson
Nickname
Not certified

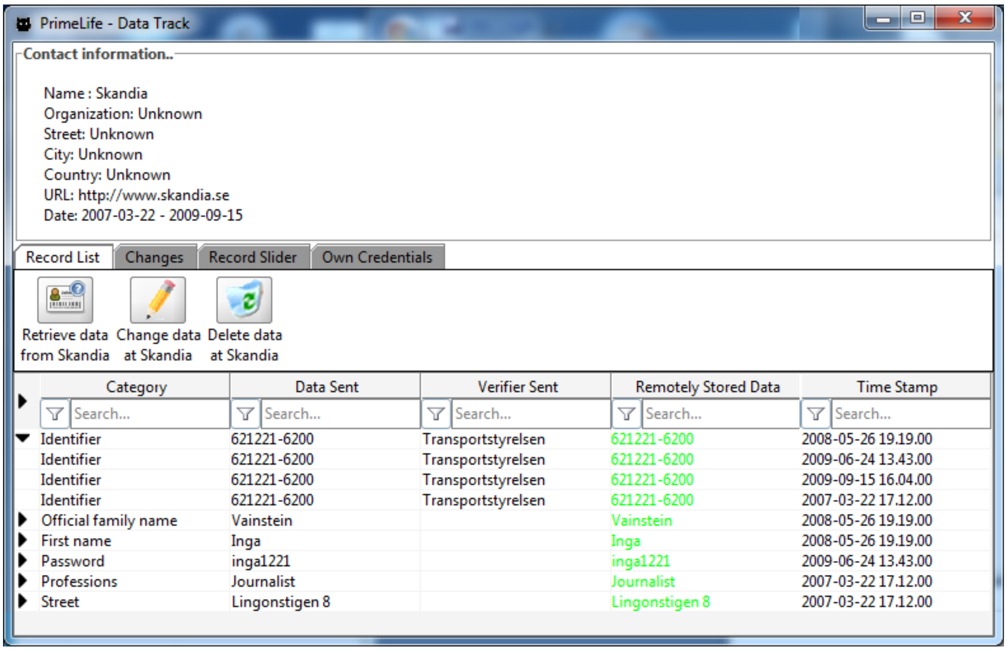
Swedish
Nationality
Certified by Polisen Polisen

svenskalaget_fan(at)gmail.co
Email
Not certified

September 23rd, 1984
Date of birth
Certified by Polisen Polisen

Figure 18: A lo-fi sketch of a timeline visualization of data disclosures

3.5.2. Design iterations



Contact information..

Name : Skandia
Organization: Unknown
Street: Unknown
City: Unknown
Country: Unknown
URL: http://www.skandia.se
Date: 2007-03-22 - 2009-09-15

	Category	Data Sent	Verifier Sent	Remotely Stored Data	Time Stamp
▶	Search...	Search...	Search...	Search...	Search...
▼	Identifier	621221-6200	Transportstyrelsen	621221-6200	2008-05-26 19.19.00
	Identifier	621221-6200	Transportstyrelsen	621221-6200	2009-06-24 13.43.00
	Identifier	621221-6200	Transportstyrelsen	621221-6200	2009-09-15 16.04.00
	Identifier	621221-6200	Transportstyrelsen	621221-6200	2007-03-22 17.12.00
▶	Official family name	Vainstein		Vainstein	2008-05-26 19.19.00
▶	First name	Inga		Inga	2008-05-26 19.19.00
▶	Password	inga1221		inga1221	2009-06-24 13.43.00
▶	Professions	Journalist		Journalist	2007-03-22 17.12.00
▶	Street	Lingonstigen 8		Lingonstigen 8	2007-03-22 17.12.00

Figure 19: The user interface of PrimeLife's Data Track.

Earlier versions. The early versions of the PrimeLife Data Track's user interface [FHHW11] displayed the history of data disclosures as a table (as shown in Figure 19), in which rows could be expanded to show more detailed information about the selected disclosure and its recipient. Clicking on a disclosure would open a second separate window where users could see the specific information attributes sent during that disclosure, and also check if these attributes matched the data stored on the service's side.

Usability evaluations of these earlier versions, presented in [FHHW11], showed that a table visualization was not a very intuitive way of visualizing a summary of data disclosures, and that users often missed out on information that was hidden under the unexpanded rows or elements that were not clicked. Moreover, users had problems to differentiate whether data records were stored locally on the users' side (i.e., under the users' control) or if they were stored remotely in the service providers' sides (and thus not under the users' control). Also, the way in which the interface was structured did not provide a meaningful understanding of the way personal data flows to different entities during an online transaction [FHHW11]. A third-party review of existing transparency enhancing tools even claimed that the Data Track's level of comprehensibility for an average Internet user was questionable [JWV13].

More detailed descriptions of the initial Data Track's proof-of-concept, user interfaces and results of the usability evaluations can be found in [FHHW11]. The security and privacy mechanisms of its software implementation can be seen in [HPHL10, Hed09, PPW13].

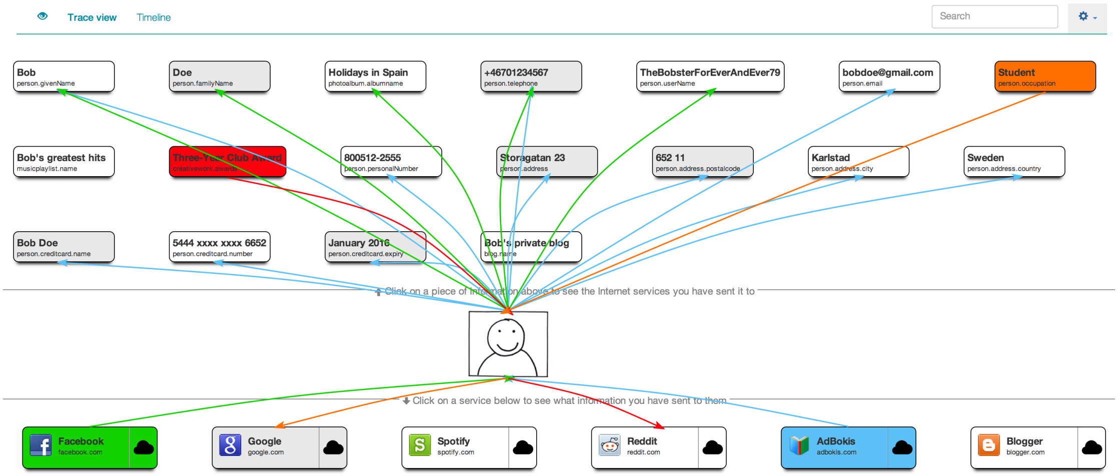


Figure 20: The trace view interface of the Data Track tool

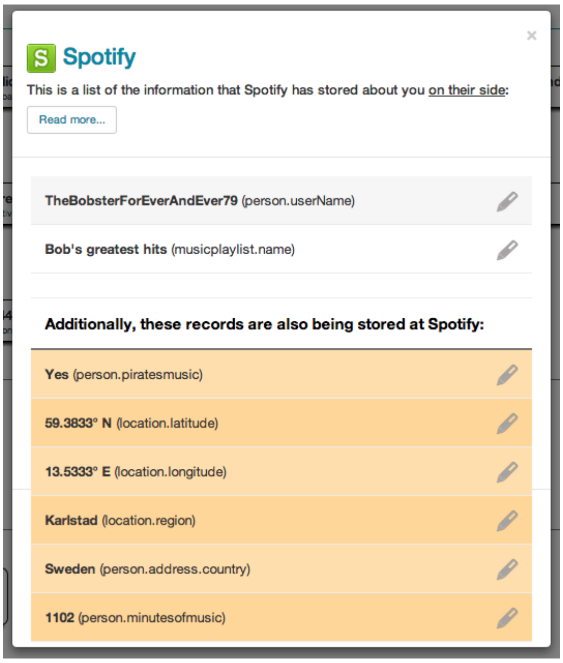
The trace view visualization. After several rounds of paper sketches and lo-fi mockups, which were discussed and refined with the help of domain and HCI experts[9], an interactive prototype of the Data Track's graphical user interface, the trace view, was implemented using HTML5 and jQuery libraries (shown in Figure 20). In the trace view the user is represented by a profile picture in the middle of the screen, motivated by design experts suggesting that users focus most of their attention in the middle of the screen after gazing at the top left corner. In particular, we wanted to give users the feeling that this interface is a *place* that focuses on them (i.e. data about them and services that they have contacted).

The interface is then separated into two main panels, following the design guidelines which advice that clearly separating different regions in the screen diminishes the users' cognitive demands. The services to which the user has released information appear in the bottom panel and the information attributes that have been released by the user to these services appear in the top panel. By clicking in one (or many) of the services at the bottom, the interface shows a *trace* from the service to the user, and then from the user to the data items that she has released to that specific service. If the user clicks instead on a data item at the top, the trace shows which online services have that particular item. The traces are coloured to easily differentiate between them.

Figure 21: A node representing a service provider, from where users can also access their data located at the services' side.

[9] Early versions of lo-fi mockups with a trace view visualization were developed within the scope of a Google Research Award project in discussion with technical and HCI specialists from Google

The services in the bottom panel contain a button with an icon from which users can also access the data about them stored on the services' sides (as seen in Figure 21). Clicking this button opens a modal dialog where users can review the data concerning them that the selected service has stored in their databases (Figure 22). Contrasting colours, an explicit headline and adequate spacing are used to differentiate between data that was explicitly submitted by the user from data that has been implicitly collected or derived by the service provider. In this view users can also exercise their rights to correct or remove data about them.



Spotify

This is a list of the information that Spotify has stored about you on their side:

TheBobsterForEverAndEver79 (person.userName)

Bob's greatest hits (musicplaylist.name)

Additionally, these records are also being stored at Spotify:

Yes (person.piratesmusic)

59.3833° N (location.latitude)

13.5333° E (location.longitude)

Karlstad (location.region)

Sweden (person.address.country)

1102 (person.minutesofmusic)

Figure 22: Information about a user stored at the services' side.

The procedures for evaluating UI prototype with a trace view visualisation with test participants in two iteration cycles and the obtained results can be read in the A4Cloud deliverables DC-7.3 and D-C-7.1.

3.5.3. Further UI work

Noticeable improvements of the usability of the Data Track have been done since its initial iterations. However, there are some aspects that need to be considered before continuing with further design rounds of the Data Track.

For one, the interface of the Data Track presented thus far, does not portray a realistic scenario in which one user discloses large amounts of personal attributes to many different service providers, as it so far mainly served the purpose of testing the basic trace view visualisation concept. This consideration poses a challenge related the visualisation of millions of data records accumulated over time, or big data, which has to consider perceptual and interactive scalability. Some mechanisms for reducing the possible large data sets to smaller comprehen-

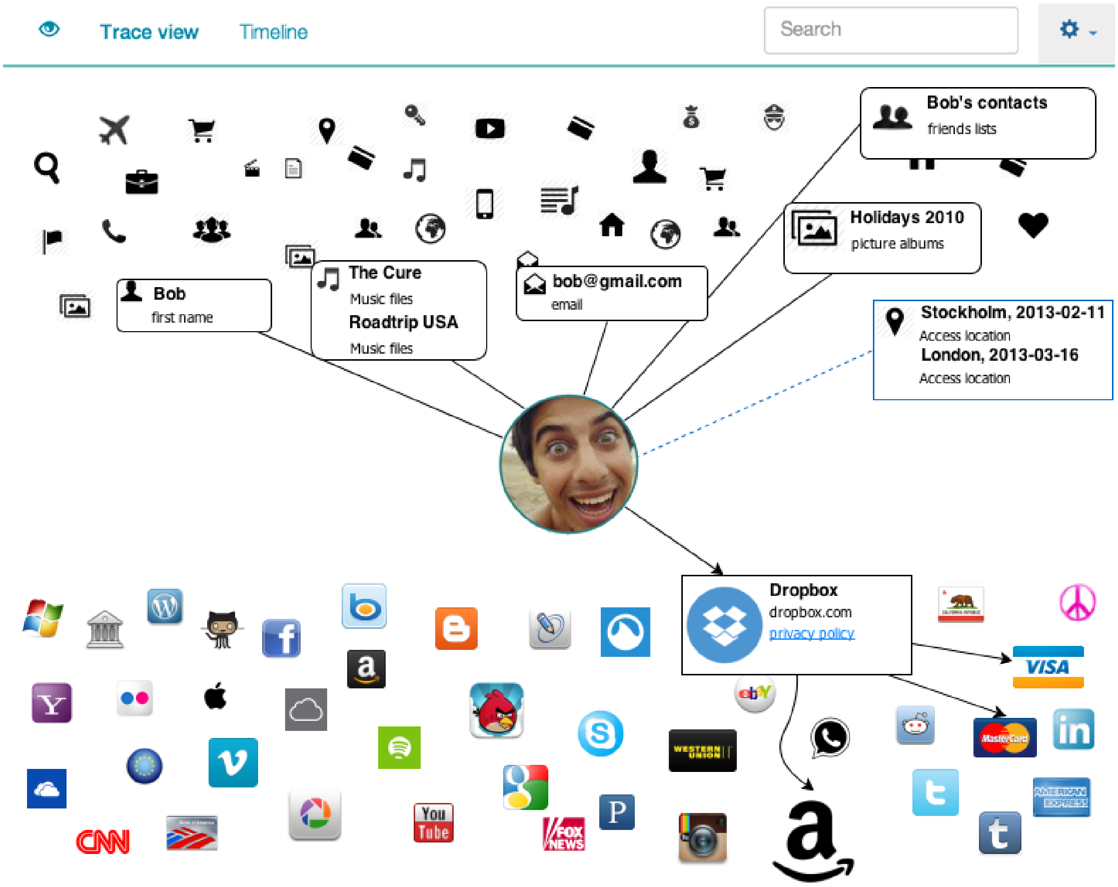


Figure 23: Sketch for the new traceview interface of the Data Track tool

sible subsets that can be handled cognitively by the average viewer are described in [LJH13], including filtering, sampling, binned aggregation, model-fitting, or a combination of these. Decisions for the reduction of data should consider not only the screen real state, but also take into account what users prioritize or find useful to visualise for a particular purpose. For example, conceptually the Data Track could log disclosures of IP addresses, mouse clicks, etc. However, these attributes might not be of relevance to the user in many cases and they could be filtered out initially, only to be revealed if requested.

Based on these observations, along with the feedback from the usability evaluations and further ideas, we have conceived a more realistic design of the Data Track as illustrated in Figure 23. Although the main design paradigm remains the same, the new interface considers displaying many data attributes in form of icons at the top and uses the logotypes of different services at the bottom. When users hover the mouse over one object an in-place container will expand to show some details about that object. If the object is clicked the tracing lines will indicate the object's relationship to the other objects which would also expand to show more detailed information. For example, moving the mouse over the Dropbox icon, could show a box containing this service's contact details, its privacy rating (as set by reputation projects similar to ToS;DR[10]), the date of the last disclosure, and other information of interest. Clicking on the Dropbox expanded box, would show the trace to the users' attributes that have been disclosed to this service, as well as other possible services that might be involved in the flow of data. In this example, Dropbox has a relationship with Amazon's S3 cloud services, and also with some payment providers. This, in turn, forms a network structure, which can then be analysed mathematically in order to present users with, for instance, metrics of clustering or betweenness centrality of the service which can inform users about the probability of their information being spread to other nodes, and other useful information about the consequences of their data dissemination behaviours.

With the help of the popular D^3 (Data-Driven Documents) jQuery library [BOH11] it is possible to quickly prototype and implement the ideas described above. This open source library has the potential of endowing the interface with greater levels of playability, attractiveness, affordance and interactivity, which are properties that we consider valuable for the continuous improvement of the usability and user engagement with a transparency tool. For this next round of design, we also plan to include interactive controls for letting users set particular parameters that dictate how the data is filtered and rearranged, such as grouping or sorting data entries by a certain property, filtering entries depending on a time range, etc. A related challenge, also indicated in [LJH13], is that the filtering and manipulation of big data sets have to be made seamless and quick as to not hinder the user experience, especially in applications where users expect immediate feedback and responsiveness from the tool, as is the case with the Data Track.

Suggestions for further work include the search for better graphical representations of the functionality to access to the data located in the service providers' side. Also, research is needed on mechanisms to assure users that the records displayed by the Data Track are secured, only accessible by the user and only representing attributes that have been disclosed at some point (and not all possible attributes about a user). Once a more robust prototype is in place, it would be interesting and necessary to investigate not only the users' acceptance of the Data Track, but also the users' patterns of interactions with this tool, and find out for what purposes and under which contexts do users interact the Data Track during their routinely online activities. In fact, an expert evaluator commented during a seminar, that he would use the Data Track few times per month, mostly to detect discrepancies or things that fall out of the ordinary in the distribution and usage of his data. Visualising these discrepancies is also something that we will consider.

Besides the trace view visualisation presented in this paper, we are currently developing hi-fi prototypes of other visualisations of data sets related to personal data disclosures, as shown in the timeline sketched in Figure 18.

3.5.4. Plug-in for Assessment of Privacy Violations

As an extension of the Data Track, the Plug-in for Assessment of Policy Violation (PAPV) is developed, which provides an assessment on the relevance of previously detected policy violations. The assessment made is based in various sources, such as machine-readable policies that describes the obligations of the data controller regarding the treatment of private informa-

[10] Terms of Service; Didn't Read `http://tosdr.org/`

tion 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. For each instance of a policy violation, the plug-in produces an ordered measurement of the relevant of the violation event, which can be qualitative or quantitative. This enables the list of violations to be presented to users 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.

The most important thing for the tool to convey is to what extent the user is directly affected and what, if any, options of remediation are available.

WP:C-5 of A4Cloud is responsible for developing the PAPV. A diagram depicting the architecture of this plug-in and the relationship to the Data Track tool is shown in Figure 24. Users could get relevant notifications about policy violations and other incidents through the Incident Response Tool (Section 3.8) and try to respond to these types of incidents through the Response and Remediation Tool (Section 3.9).

3.5.5. Verification against use case scenarios

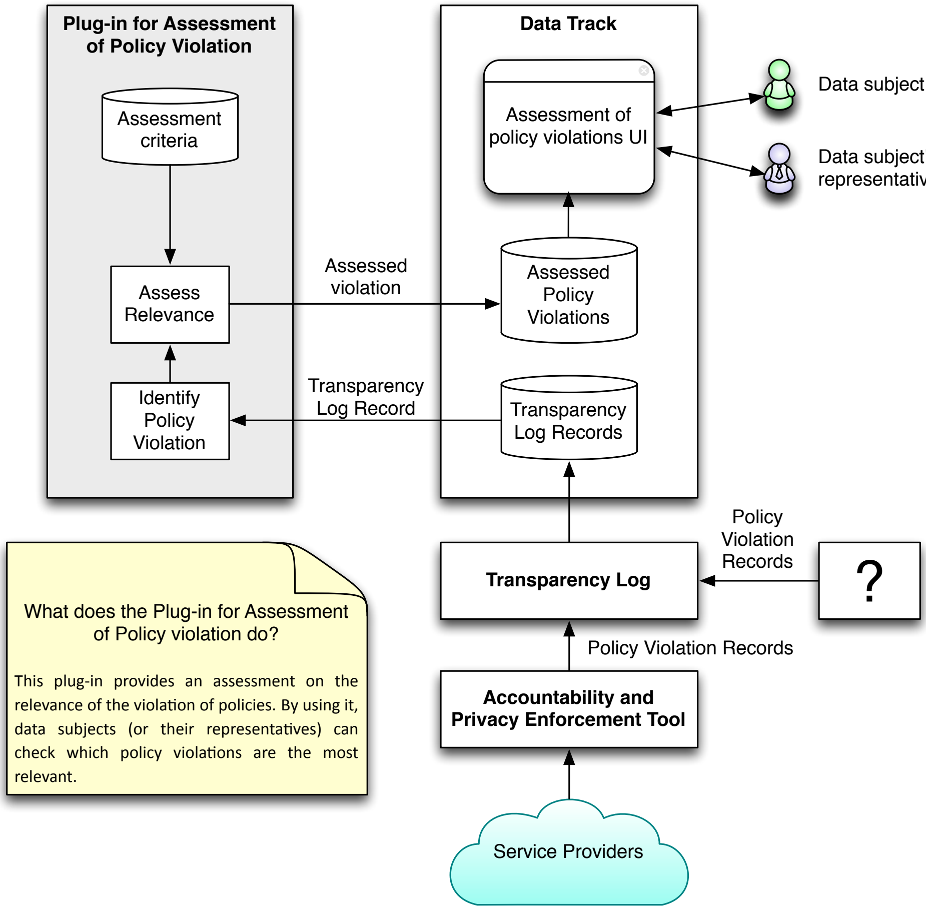
In this subsection we analyse to what degree the current version of the Data Track is able to address the concerns of the personas described in the A4Cloud project deliverable DB3.1 [BFS$^+$13].

First we outline the scenario that describes the activities surrounding data ownership and data access, and then we briefly summarize whether the Data Track will be useful in these scenarios.

Scenario 1.1.3a: Kim This scenario describes how Kim, an individual end user, uses a tool to confirm that all the personal data that has been collected in the research program has been deleted within the time frame stated in the agreement. The Data Track can be of help with this task, provided that the deletion deadline was stated in the policy. Otherwise he can manually confirm that the research project does not have access to the information in question, by examining the visual layout of his personal data.

The mock-ups do not include a view of how policy violations are to be presented to the user in the Data Track tool.

Hence, the identified use case scenario is fulfilled by the Data Track mockups and tool description. However, as mentioned, the mockups do not indicate how policy violations are handled in DataTrack, otherwise scenario 1.1.3a would be fulfilled.



What does the Plug-in for Assessment of Policy violation do?

This plug-in provides an assessment on the relevance of the violation of policies. By using it, data subjects (or their representatives) can check which policy violations are the most relevant.

Figure 24: The architecture for the Plug-in and its integration with the Data Track. Taken from the work of WP:C-5.

3.6. Data Transfer Monitoring Tool (DTMT)

The Data Transfer Monitoring Tool (DTMT) is aimed at making it possible for cloud providers and internal or external auditors to verify that a service provider is fulfilling his obligations specified in the A-PPL policies. It is also supposed to support cloud service providers in demonstrating compliance towards personal data protection and other regulations.

The DTMT uses policies created with the AccLab Tool (Section 3.1) which in turn generates A-PPL policies to be stored in a policy repository. The tool produces events based on the processing of the configuration, Data Transfer Logs, Policy Repository and Data Transfer Queries.

In order to fulfil its purpose, the DTMT relies on the Policy Repository, Data Transfer Logs from the A-PPL engine; configuration of locations of host and legal entities (e.g. computers, data subjects, controllers, processors) as well as user defined Data Transfer Queries.

It must be possible for the users (that be an end users, auditors, service providers, etc.) to present queries to the system and receive the relevant output. The service provider must also be able to configure the systems location.

3.6.1. Users goals and task analysis

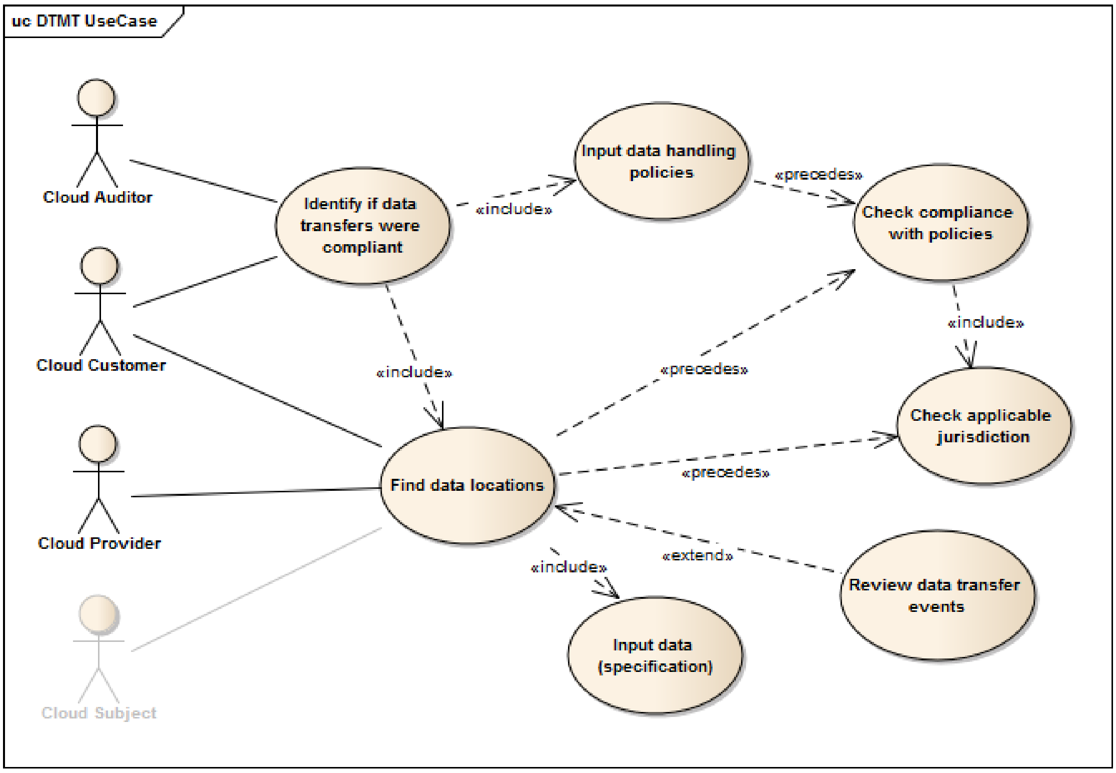

uc DTMT UseCase
Cloud Auditor
Cloud Customer
Cloud Provider
Cloud Subject
Identify if data transfers were compliant
Input data handling policies
Check compliance with policies
Check applicable jurisdiction
Find data locations
Review data transfer events
Input data (specification)
«include»
«precedes»
«include»
«include»
«precedes»
«precedes»
«extend»
«include»

Figure 25: UML use case diagram of the Data Transfer Monitoring Tool

The main purpose of the Data Transfer Monitoring Tool is to allow stakeholders to identify data locations as well as whether data transfers were executed in compliance with the underlying policies.

Both the cloud auditor and the cloud customer should be able to check whether a data transfer was executed in compliance with the underlying policies or not. This also includes checking the applicable jurisdiction of the data and, as such, its location.

The cloud customer, the cloud provider and the cloud subject are all able to identify the location of the data. For the tool to accomplish this task, it needs to know which data to locate and to review the data transfer events to identify its location.

The UML use case diagram depicted in Figure 25 provides a high-level view of what the tool should actually do.

3.6.2. Initial UI prototypes

The mock-ups, reflections and concepts based on the description of the Data Transfer Monitoring Tool, made available in A4Cloud deliverable MS:D-2.2 by WP:D-2, and are created under the following assumptions:

- Audit events are accessible to the users through the AAS
- The data specification are done in AccLab or by the users' own software
- The Service Chain Builder (which is an internal component of DTMT) does not need a GUI
- Inspection of Data Locations is the GUI part to be created within DTMT

List and query view When the users opens the Data Transfer Monitoring Tool, they could be provided with a query interface as the one shown in the left sidebar in figure 26. The interface is similar to that of a filtering interface, as the concepts are mostly the same from a user's point of view. This also reduces the time required to learn using the tool, as no query language is required. If required, the select boxes could be multi select of the same type as the one described in section 3.2.2.

This is to accommodate the requirement stated in A4Cloud deliverable D:C-7.1 [AFHP$^+$13], which states that data sharing and data processing along the cloud should be made transparent and the users provided with means to verify it.

To the right on the screen, a list of data groups (i.e. a list of different categories of data) and their location can be shown. When the users click on a data group, it could open and give a brief summary of its location and data. If there are unhandled violations related to the data group, they could be presented under the summary. The data groups should be sorted in a way placing those with violations on top.

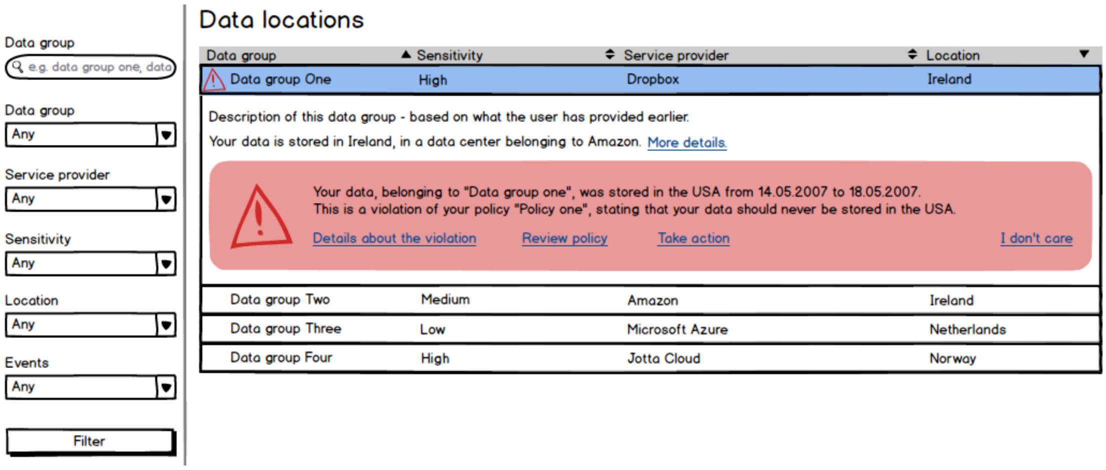
In the overview of the violation, the users could be offered some direct actions.

- **Details about the violation**
  This button could take the users directly to the IRT, where they could get more information about the violation

- **Review policy**
  This button could take the users directly to AccLab, where they could review his preferences and validate them against the providers policy
- **Take action**
  This button could take the users directly to RRT, where they could handle the violation
- **I don’t care**
  This button could simply close the violation without handling it. The somewhat unorthodox wording is used in an attempt to make the users think twice before dismissing the violation. Words like ”Hide” or ”Dismiss” might have a ”I’ll handle it later”-effect, but stating ”I don’t care” might be controversial enough to avoid the users clicking on it other than in valid cases. It might also be helpful in a legal situation, as the users can not argue that they did not have time to handle it or simply postponed it; they have already stated they did not care.
  If this exact wording or a similar one is chosen, studies should be conducted on the effect.

As with all other tools allowing the users to view some more details about an item by opening it inline, the model is not an accordion, but rather a toggle effect. The users open and closes an item by clicking on it. The reason for this, is that accordions removes some of the users’ control when it comes to which items to have open as an accordion auto closes the previous item when the next is activated. It can also cause the users to lose his direction on the page if a long accordion box was open and another one is activated, this would result in the new box being opened closer to the top than where the users opened it.

The users could be offered to get more details about the data group; this is described in the following part.



Data group	▲ Sensitivity	⬍ Service provider	⬍ Location ▼
Data group One	High	Dropbox	Ireland
Data group Two	Medium	Amazon	Ireland
Data group Three	Low	Microsoft Azure	Netherlands
Data group Four	High	Jotta Cloud	Norway

Description of this data group - based on what the user has provided earlier.
Your data is stored in Ireland, in a data center belonging to Amazon. More details.

Your data, belonging to "Data group one", was stored in the USA from 14.05.2007 to 18.05.2007.
This is a violation of your policy "Policy one", stating that your data should never be stored in the USA.

Figure 26: The user can query for data locations and view their details

Detail view When reviewing the details, the users could be presented with a screen like the one in figure 27.

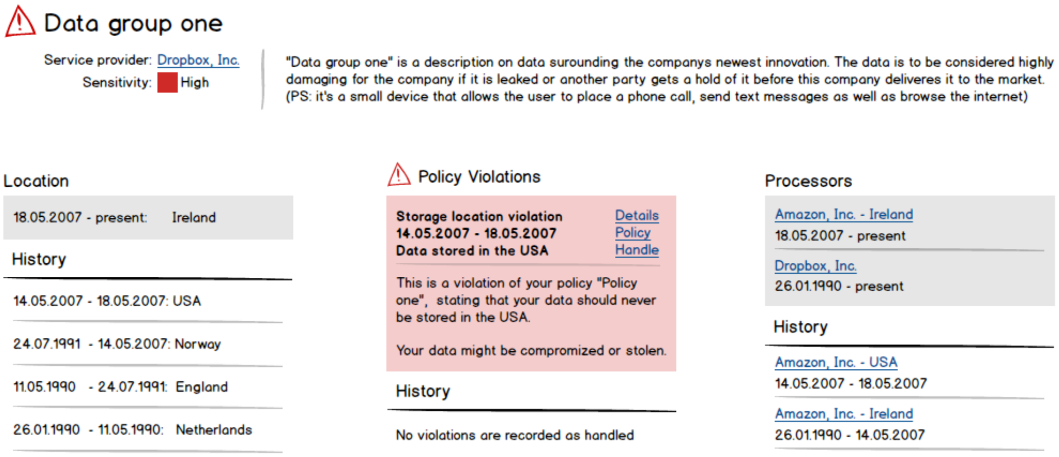
On the top, the data group name should be stated. As could an indicator on whether there are any violations related to this data group. The name of the service provider, preferably linked to a page with more details about the provider, should also be included. The sensitivity of the data in the data group could also be stated, preferably with a visual indicator allowing for the users to effortlessly get an overview. A user provided description of the data group could be displayed, allowing the users to refresh their memory on the content or nature of the data in the current group.

Three types of information are of interest for the users of DTMT: data locations, policy violations and processor locations.

The detail view could present this information in a unified manner, placing the current information on top and the history underneath. This is exemplified in figure 27. The exact placement of the containers should be subject to usability tests.

The violations have the same actions as those described for the violation excerpt in the list view. It could also give a brief statement of possible consequences of the violation. The background colour could be used to give the users an impression of the severity of the violation. In the list of processors, all providers could be linked to pages with more details about the provider. Such a page could also include e.g. track record, terms of services, etc.

This would be part of fulfilling the requirement stated in A4Cloud deliverable D:C-7.1 [AFHP+13], stating that policies need to make the possible consequences of data disclosures in different recurrent situations transparent. It would also contribute to fulfilling the requirement stating that consequences should be explained using wording that is easy to understand for non-technical users. The combination of the background color and the simple sentence “Your data might be compromised or lost.” serves as an example here.



⚠ Data group one

Service provider: Dropbox, Inc.
Sensitivity: 🟥 High

"Data group one" is a description on data surounding the companys newest innovation. The data is to be considered highly damaging for the company if it is leaked or another party gets a hold of it before this company deliveres it to the market. (PS: it's a small device that allows the user to place a phone call, send text messages as well as browse the internet)

Location

18.05.2007 - present: Ireland

History

14.05.2007 - 18.05.2007: USA

24.07.1991 - 14.05.2007: Norway

11.05.1990 - 24.07.1991: England

26.01.1990 - 11.05.1990: Netherlands

⚠ Policy Violations

Storage location violation
14.05.2007 - 18.05.2007
Data stored in the USA

Details
Policy
Handle

This is a violation of your policy "Policy one", stating that your data should never be stored in the USA.

Your data might be compromized or stolen.

History

No violations are recorded as handled

Processors

Amazon, Inc. - Ireland
18.05.2007 - present

Dropbox, Inc.
26.01.1990 - present

History

Amazon, Inc. - USA
14.05.2007 - 18.05.2007

Amazon, Inc. - Ireland
26.01.1990 - 14.05.2007

Figure 27: The user can view details about each data group

3.6.3. Verification against use case scenarios

In this subsection we analyse to what degree the current version of the Data Transfer Monitoring Tool is able to address the concerns of the personas described in the A4Cloud project deliverable DB3.1 [BFS+13].

First we outline the scenarios that describe the activities relates to data transfer monitoring and then we briefly summarize whether the Data Transfer Monitoring Tool will be useful in these scenarios.

Scenario 1.1.1b: Kim This scenario describes how Kim, who is an individual end user, uses a tool that provides him with a report that includes information about where his data is currently being stored. The Data Transfer Monitoring Tool will help with this task.

Scenario 3.1.1b-c: Michael These scenarios describe how Michael, who is a privacy officer at a cloud consumer, uses a tool to track personal data in the cloud. He also uses this tool to compare the track record with the contract terms that his company has with the cloud provider. The Data Transfer Monitoring Tool can be of help with these tasks.

Scenario 5.1.1a: Bruce This scenario describes how Bruce, who is an infrastructure manager at a cloud provider, uses a tool to track customers' data across the cloud and verifying where it has been transferred. The Data Transfer Monitoring Tool can be of help with this task.

Scenario 18.1.1b: Sandra and Scenario 20.1.1a: Peter These scenarios describe how auditors and end users could hold cloud service providers accountable for the handling of personal data. The Data Transfer Monitoring Tool can be of help with this task.

All identified use case scenarios are fulfilled by mock-ups and tool description.

3.7. 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

The way the tool passes this information to the user is by generating a report which includes a risk profile, advice on whether to proceed or not and suggested mitigations. This is both a way of providing the user with the relevant information on the current case, as well as educating the user on risk and threats.

The interaction with the users happens through questions and answers. The users are also informed through a report as mentioned above. In order for the users to provide the correct information, the tool will present them with questions in a questionnaire guiding them to the relevant input.

3.7.1. Users goals and task analysis

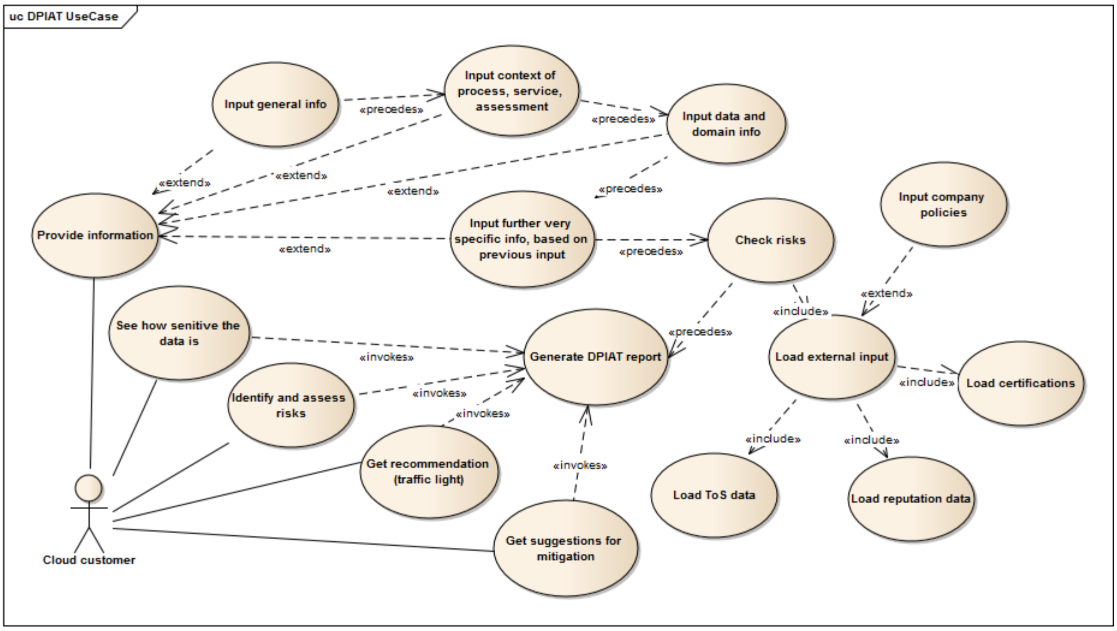


Figure 28: UML use case diagram of the Data Protection Impact Assessment Tool

As can be seen in the task analysis in section A.7, the main purpose of the Data Protection Impact Assessment Tool is to provide the customer with high level advice on the risk of using cloud services in a given context as well as possible mitigations.

In order for the tool to work, the customer needs to provide some information. The tool will present the users with a questionnaire seeking to gain the relevant information about user environment, input data and domain. Based on this input the tool might also construct other relevant questions in order to gain an even better understanding of the situation.

In order for the cloud customer to be able to see how sensitive the data is, identify and assess risks, get recommendations and get suggestions for mitigation, the tool needs to generate a DPIAT report. Generating this report requires the tool to perform a check for risks.

To check the risks the tool utilizes the information provided by the cloud customer as well as external input like company policies, certifications, terms of services and data about reputation.

The UML use case diagram depicted in Figure 28 provides a high-level view of what the tool should actually do.

3.7.2. Initial UI prototypes

The following reflections and mock-ups are based on the description of the Data Protection Impact Assessment Tool, made available in A4Cloud deliverable MS:D-2.2 by WP:D-2.

Questionnaire The main source of interaction between the users and the tool is through a questionnaire. Therefore emphasis is put on making the user experience of interacting with the questionnaire as friction free as possible.

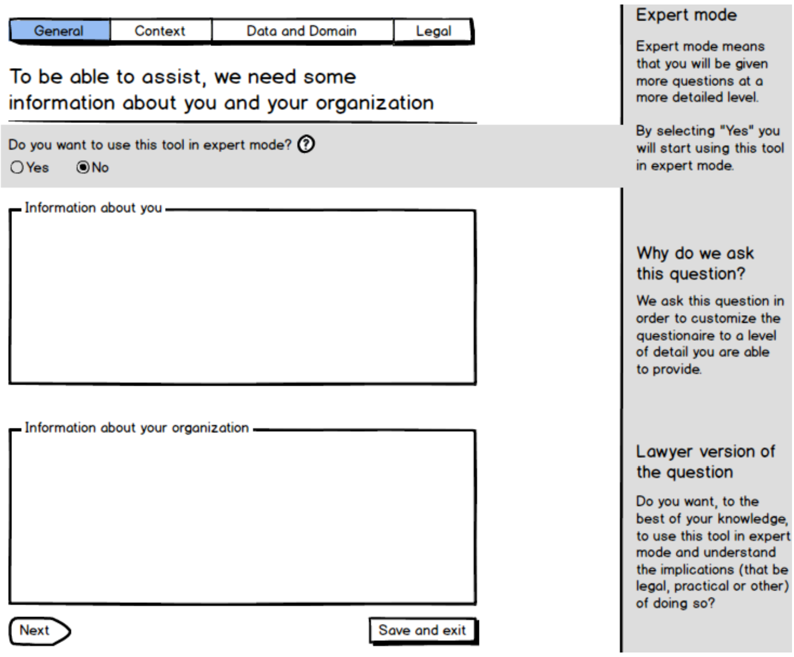
Much of what is discussed here might also apply to other tools as well.

Navigation The questionnaire could have a layout close to the one in Figure 29. Here the users are presented with a horizontal bar acting as a table of contents for the questionnaire, setting the users expectations straight at the very beginning as well as keeping him informed about his progress. The users could be able to use this bar to navigate to pages in the questionnaire they have already completed.

The questionnaire could allow the users to provide answers on their own terms by allowing them to save their answers and exit the questionnaire. At a time of their choosing they could continue the questionnaire and potentially finish it.

As illustrated in Figure 29 and 30, the navigation buttons are placed at the bottom of the questionnaire. In accordance with recommendations derived from an empirical study conducted by the University of Michigan and Market Strategies International [CBM11], the “Next” button (which is the most important button) is aligned to the far left and the “previous” action (which is less important) is placed as an ordinary link next to it.

Text The overall language used could be informal, reassuring and informative. The header in Figure 29 serves as an example.



To be able to assist, we need some information about you and your organization

Do you want to use this tool in expert mode? ?

○ Yes ● No

Information about you

Information about your organization

Expert mode

Expert mode means that you will be given more questions at a more detailed level.

By selecting "Yes" you will start using this tool in expert mode.

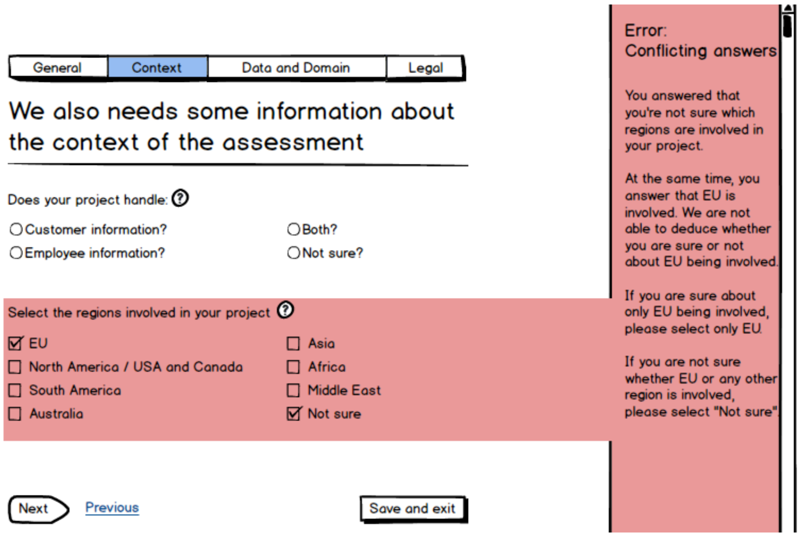
Why do we ask this question?

We ask this question in order to customize the questionaire to a level of detail you are able to provide.

Lawyer version of the question

Do you want, to the best of your knowledge, to use this tool in expert mode and understand the implications (that be legal, practical or other) of doing so?

Figure 29: The user can see a questionnaire with a help pane on the side



We also needs some information about the context of the assessment

Does your project handle: ?

○ Customer information? ○ Both?

○ Employee information? ○ Not sure?

Select the regions involved in your project ?

☑ EU ☐ Asia

☐ North America / USA and Canada ☐ Africa

☐ South America ☐ Middle East

☐ Australia ☑ Not sure

Error: Conflicting answers

You answered that you're not sure which regions are involved in your project.

At the same time, you answer that EU is involved. We are not able to deduce whether you are sure or not about EU being involved.

If you are sure about only EU being involved, please select only EU.

If you not sure whether EU or any other region is involved, please select "Not sure"

Figure 30: The user see a questionnaire with error explanation on the side

Forms When possible, the tool could present the users with sensible defaults such as the one demonstrated in Figure 29 under the question ”Do you want to use this tool in expert mode?”. The default is set to ”No” in order to not overwhelm novice users in a way that might make them uneasy about the questionnaire. To further enhance the user experience on this particular question, the tool could remember the answer and make that the default next time.

Help In data intensive applications it is common to use a designated help system rather than popovers or inline help. The help pane, as shown in figure 29 is activated by the users when clicking on the question mark next to a question. The pane is placed on the right in order to support the natural reading direction of the users. This means that if the tool is to support right-to-left languages, the pane could be placed to the left of the question when such a language is activated.

The help pane could have different modes, one for explaining the question upon the users request and one for offering the users advice on how to correct errors in the form.

When the help pane is explaining A question, as in Figure 29, the users could be offered an explanation of the question as well as a notice about why this question is asked. The explanation on why the question is asked could also include information about which answers made this question relevant if the question is only presented under certain conditions. Doing this would contribute to fulfilling the requirement stated in A4Cloud deliverable D:C-7.1 [AFHP$^+$13], which states that implicit data collections should be made transparent. If applicable, a legal version of the question could also be presented. This might help keep the main questions simple and understandable. There might, however, be unexamined legal implications of doing this.

When the help pane is activated, either for explaining an error or a question, a path could be created for the users to follow all the way to the explanation as exemplified in Figure 30. The path should not only be visual as that would hinder visually impaired users who use screen readers. Therefore the help button should be a link moving the users to the top of the help pane. In the help pane it should also be a link taking the users back to the relevant question.

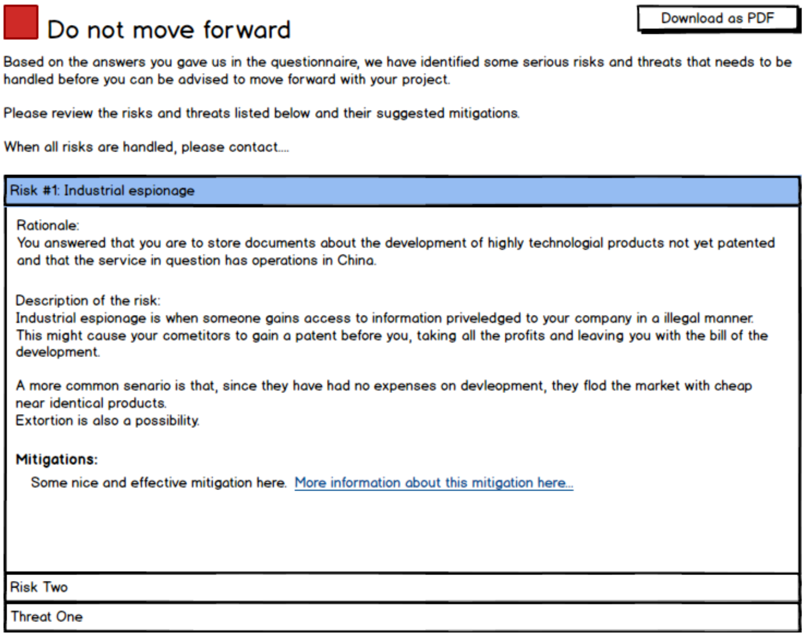
When explaining an error, as in Figure 30, the users could be provided an understandable explanation with concrete advice on what can be done to correct the error. If possible, choices for automatic correction of the error could be included.

Report The generated report, exemplified in Figure 31, could give clear advice at the very beginning whether the users can move forward with his project or not - this sets the users expectations straight. It could then go on to explain how the report was created, provide some simple instructions on how to use the report as well as what to do when all items in the report are handled. The tool could list all the risks and let the users view the detailed version inline, making for a more effective workflow.

For each risk (and threat), the tool could provide an explanation for which answers led to the risk (threat) to be invoked. The risk could be described in a way that makes it easy to understand the ramifications should it become reality – linking it to real world stories could be beneficial. Thus the risks (and threats) could be described from a business or personal point of view, not only from a technical point of view. This would be part of fulfilling requirements stated in A4Cloud deliverable D:C-7.1 [AFHP$^+$13], which says that consequences should be explained in practical terms as well as consequences of data disclosures should be made transparent.

The tool could also provide a structured overview of possible mitigations. Depending on the type of mitigation, the tool could provide a way of gaining deeper knowledge about the mitigation as well as its effects. This could be technical information, information about organizational restructuring, legal information, etc.

The tool could also allow the users to download the report as e.g. PDF. This would allow the users to pass the report on to others in the organization that needs to be involved in the process.



🟥 Do not move forward

Based on the answers you gave us in the questionnaire, we have identified some serious risks and threats that needs to be handled before you can be advised to move forward with your project.

Please review the risks and threats listed below and their suggested mitigations.

When all risks are handled, please contact....

Risk #1: Industrial espionage

Rationale:
You answered that you are to store documents about the development of highly technologial products not yet patented and that the service in question has operations in China.

Description of the risk:
Industrial espionage is when someone gains access to information priveledged to your company in a illegal manner.
This might cause your cometitors to gain a patent before you, taking all the profits and leaving you with the bill of the development.

A more common senario is that, since they have had no expenses on devleopment, they flod the market with cheap near identical products.
Extortion is also a possibility.

Mitigations:

Some nice and effective mitigation here. More information about this mitigation here...

Risk Two

Threat One

Figure 31: The DPIAT shows a report with advices to the users

3.7.3. Verification against use case scenarios

In this subsection we analyse to what degree the current version of the Data Protection Impact Assessment Tool is able to address the concerns of the personas described in the A4Cloud project deliverable DB3.1 [BFS$^+$13].

First we outline the scenarios that describe the activities related to identifying risks and then we briefly summarize whether DPIAT will be useful in these scenarios.

Scenario 3.1.2a: Michael This scenario describes how Michael, who is a privacy officer and cloud service user, uses a tool to identify the risks associated with using a cloud platform in a healthcare program. The Data Protection Impact Assessment Tool can be of help with this task, even though the organization described in the use case is larger than a SME.

Scenario 8.1.1b: Bob This scenario describes how Bob, who is a business analyst on personal data, uses a tool to identify potential new risks based on changes in a service providers terms of service. The Data Protection Impact Assessment Tool can be of help with this task.

Scenario 10.1.1a: David This scenario describes how David, who is a mobile and cloud application developer, uses a tool to identify risks for a new type of personal data to process. The Data Protection Impact Assessment Tool can be of help with this task.

Scenario 15.1.1e: Roger This scenario describes how Roger, who is the Chief Technology Officer of a cloud service provider, uses a tool to assess the risk associated with alternative cloud providers. The Data Protection Impact Assessment Tool can be of help with this task, even though his company might be larger than an SME.

All identified use case scenarios are fulfilled by mock-ups and tool description, even though the companies in some of the scenarios can be characterised a large rather than as SMEs.

3.8. Incident Response (IRT)

The Incident Response Tool (IRT) is a tool aimed for cloud customers as the entry point for handling anomalies and detected violations in cloud environment scenarios, for instance privacy violations or security breaches. In simple terms, the tool receives incident signals (from the work done in WP:C-8) and alerts the user when relevant incident has occurred based on different parameters. The IRT will filter out the incidents that potentially need to be reported to the user. The relevance of the incidents will be partly determined by another A4Cloud tool named the "plug-in for assessment of privacy violations" (Section 3.5.4) which takes into account the users' preferences. When an incident is finally presented to the user, it then allows users to take the initial steps to respond to these incidents in a simple and straightforward manner (through the Remediation and Redress Tool presented in Section 3.9).

The work of WP:D-4 within the A4Cloud project has identified different types of incidents, which are defined within the three categories of confidentiality, integrity and availability incidents. According to the work in this work package, not all incidents can be detected automatically. For example, detecting when a systemadministrator has made a copy of the data to an external drive and sold it to an outsider. Of the incidents that can be reported, some, but not all, may need to be reported to entities outside the cloud service provider (for example to the cloud customer, the data subject and/or to the relevant data protection authority).

During workshops and other elicitation activities a number of considerations have been identified for a tool that notifies users about incidents regarding their data in cloud services:

- Users should not be notified about every possible incident, since this will create annoyance and abandonment. Instead, only notifications about incidents that are relevant for the user should be presented at appropriate times.

  A workshop with 19 individual cloud users was carried out at Karlstad University, as a joint effort between WP:B-2 and WP:C-7, where participants were asked to specify which incidents would they like to be notified about from a list of predefined incidents. Table 1 shows the responses of participants, which indicates that data subjects would like to be notified if hackers managed to obtain copies of their personal data, or if a service that they were using was attacked by a hacker, while they would care less about notifications regarding data transfers (see DTMT in Section 3.6) or news about services that have their data. Even though these results are not representative for the general population, they still provide some indications of the cloud subject's preferences.

- The participants of the same workshop expressed that they would preferred to be notified about violations to their personal data only if they were able to do something about it. Participants mentioned that obtaining information about something bad that happened without being able to take action, might just cause stress and alert, and that in such cases they might not even want to know what happened.

- Experiments done as part of WP:C-7 suggested that people would care more about controlling who is able to see the data that they place in the cloud. Thus, the IRT should also consider prioritizing notifications when the access control or sharing has been violated.

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

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

- Given that people are biased towards immediate gratification and would rather postpone long term gratifying activities the interface should provide an easy and comprehensible way to react to important events and instigate the process of remediation.

  For instance, if the IRT has reported that hackers have obtained passwords and credit cards information from a service, the tool should provide users with the mechanisms to change their password immediately and lock any transactions with the use of their credit card and ask for a replacement.

- While it is important informing users about the occurring incidents in the cloud, it is also important that the interface provides at times feeling of calmness and safety, while sparing the evoking reactive and fear emotions only for really dangerous or important incidents, where users should take actions immediately. It is better not to jade the users with unimportant notifications or notifications where they cannot react immediately.

Similarly, the Open Security Foundation hosts a website under the name of DataLossDB [11] documenting many known and reported incidents related to data breaches and leaks of personal information. This services maintains a database of incidents with the help of volunteers who actively search and report data breaches as they become publicly known through websites, blogs, news, and other communication channels. This service provides a list of the types of reported data breaches, providing for a general topology of this bridges. A listing the five more common categories of incidents according to the DataLossDB service is provided in Table 2.

One type of incident which is detectable by other A4Cloud Tools, such as the Audit Agent System AAS, are privacy policy violations. The Plug-in for Assessment of Policy Violation (PAPV), which is further described in section 3.5.4 provides an assessment on the relevance of previously detected policy violations.

[11] DataLossDB `http://datalossdb.org/`, accessed 2014-06-03

Type	Description	Frequency
Hack	Computer-based intrusion, data may or may not be publically exposed	30%
Stolen Laptop	Stolen desktop (or unspecified computer type in media reports)	11%
Fraud	Fraud or scam (usually insider-related), social engineering	11%
Web related	Data typically available to the general public via search engines, public pages, etc.	9%
Document disposal	Discovery of documents not disposed of properly	6%

Table 2: Top 5 categories of data breach incidents according to DataLossDB.

3.8.1. Users goals and task analysis

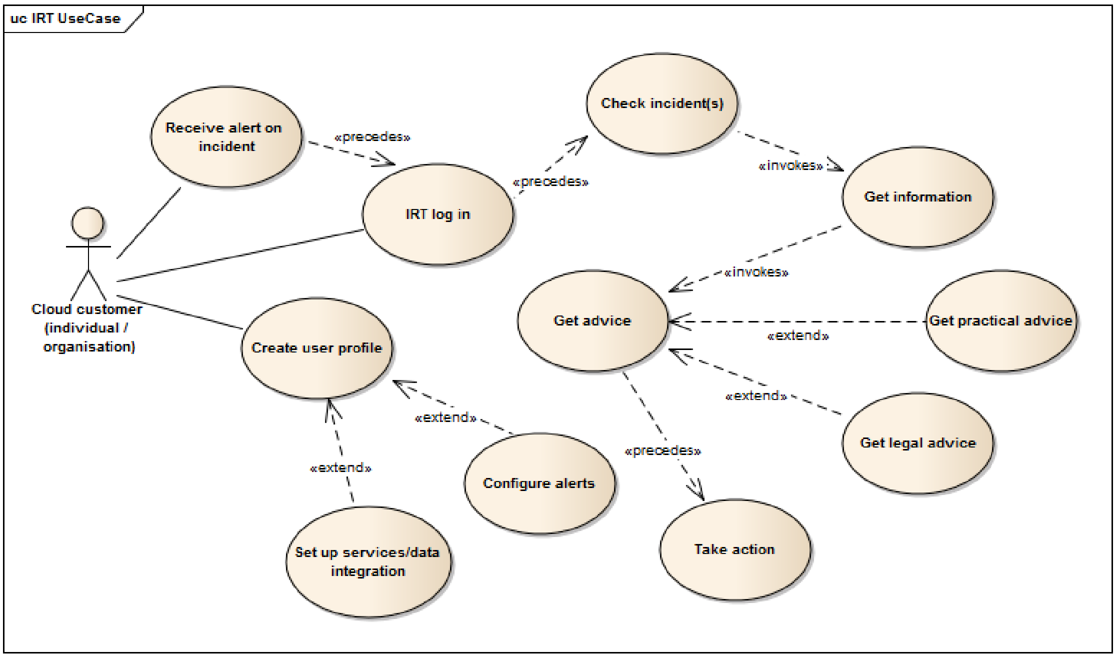


Figure 32: UML use case diagram of the Incident Response Tool

As can be seen in the UML use case diagram in Figure 32 and the task analysis in section A.7, the main purpose of the Incident Response Tool is to alert cloud customers of incidents and provide them with relevant information relating to the incident.

The cloud customer might create a user profile in which he configures how often, for which severity level and for which incident types he wishes to receive alerts as well as which services he utilizes.

When the cloud customer has configured an account, he is able to receive alerts on incidents. Upon receiving an alert, he might log in to the Incident Response Tool to check the incidents. In order for the cloud customer to make an informed check of the incident, the tool presents the user with the ability to get more information like advice. The advice could be practical or legal in nature.

Upon having received advice, the cloud customer might choose to take action based on the advice provided.

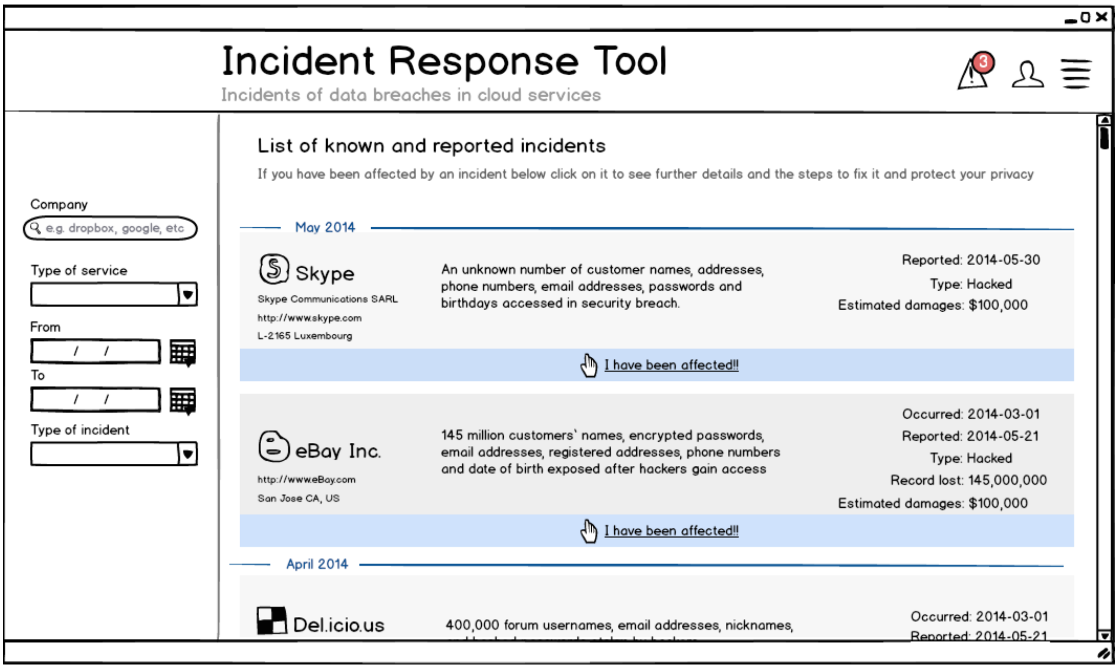
3.8.2. Initial UI prototypes for individual cloud subjects

Based on the findings from the different elicitation activities, discussions with project partners, development of use-case scenarios and the task analysis presented in Section 3.8.1, we present initial suggestions for the design of the user interface for the IRT which caters for individual cloud subjects.

Displaying all detected incidents. The general view of the IRT could display all incidents detected by the tool, as shown in Figure 33. In this view users could have a preview of all possible incidents that have been detected or reported. Users could either browse through the list of incidents or search for a specific incident with the use of various filtering options (e.g., looking for the services' name, the data of the breach, the type of data involved, the place where she heard about the breach, etc.). If the IRT knows that the user has been affected by some incidents, those incidents could be highlighted with using different colours when browsing through the list of incidents. If the user finds or identifies an incident that might be relevant to her, she could have the opportunity to take action when appropriate, for instance, by clicking in a button that says 'I have been affected!' This will in turn launch the Redress and Remediation Tool (RRT), described in Section 3.9.

As an example scenario, consider that a cloud subject has heard news or rumours about a data breach in a service where she has an account. In this case, she might be interested to look for information about this breach and have the possibility to do something about it (through the RRT).

Notifying users of important incidents. We envision a system where cloud subjects can have the possibility to be notified through different channels of important incidents to which they might want to take quick action in order to resolve an issue. Sending notifications to users via, for example, their mobile devices could be the starting point to alert users about a crucial incident to which they might want to pay attention to (rather than waiting to open the IRT in their desktop computer). Information about the nature of incidents in regard to services that a user was using, or even in regard to her data that was affected, can present rather sensitive personal information that should be kept confidential (as also discussed in the A4Cloud deliverable D:C-7.2 on "Privacy Design Guidelines for Accountability Tools"). Sending such information via push notifications to the users concerned would thus raise many privacy and security issues. Addressing these issues with suitable privacy enhancing technologies, as discussed and suggested in D:C-7.2, will however not be easily feasible in the mobile case. Therefore, mobile



Incident Response Tool

Incidents of data breaches in cloud services

List of known and reported incidents

If you have been affected by an incident below click on it to see further details and the steps to fix it and protect your privacy

May 2014

Skype

Skype Communications SARL
http://www.skype.com
L-2165 Luxembourg

An unknown number of customer names, addresses, phone numbers, email addresses, passwords and birthdays accessed in security breach.

Reported: 2014-05-30
Type: Hacked
Estimated damages: $100,000

eBay Inc.

http://www.eBay.com
San Jose CA, US

145 million customers` names, encrypted passwords, email addresses, registered addresses, phone numbers and date of birth exposed after hackers gain access

Occurred: 2014-03-01
Reported: 2014-05-21
Type: Hacked
Record lost: 145,000,000
Estimated damages: $100,000

April 2014

Del.icio.us

400,000 forum usernames, email addresses, nicknames,

Occurred: 2014-03-01
Reported: 2014-05-21

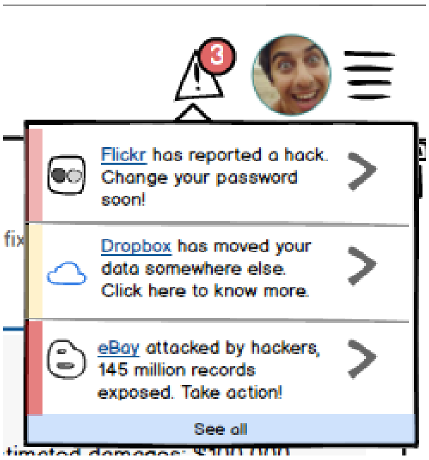
Figure 33: The IRT could show a list of all detected incidents.

incident notifications should by default not contain any personal information, but rather inform user only about the pure fact that an incident occurred. It may be possible for users to configure that the notification will also inform about the service in relation to which the incident occurred, even though in this case the user should be well informed by the configuration UI that this may already leak sensitive information about services that a user is using (e.g. specific health care services). Notification should encourage users to go to a desktop computer to get more details about the incident and take steps to address the incident if needed.

Similarly, the incident response system could set up email notifications for incidents that are important but perhaps not as crucial, where the cloud subject does not have to take immediate actions. Email notifications can contain a link that redirects the user to the IRT, opening the detail view for the specific notification. Again, appropriate security measures (e.g., mail encryption) should be taken to address privacy risks.

Displaying incidents relevant to the user. The IRT is responsible for notifying cloud subjects of incidents pertaining their data in the cloud. When users authenticate into the IRT[12] they can be presented with a list of incidents that have a connection to the services that hold their data. The presentation of the list of services would be similar to the mock-up presented in Figure 33, but with added information that is more relevant to the user and her preferences.

[12] We assume that cloud subjects are going set up a user name and password to sign in to their IRT environment



Flickr has reported a hack. Change your password soon!

Dropbox has moved your data somewhere else. Click here to know more.

eBay attacked by hackers, 145 million records exposed. Take action!

See all

Figure 34: A simple overview of the incidents relevant for the user.

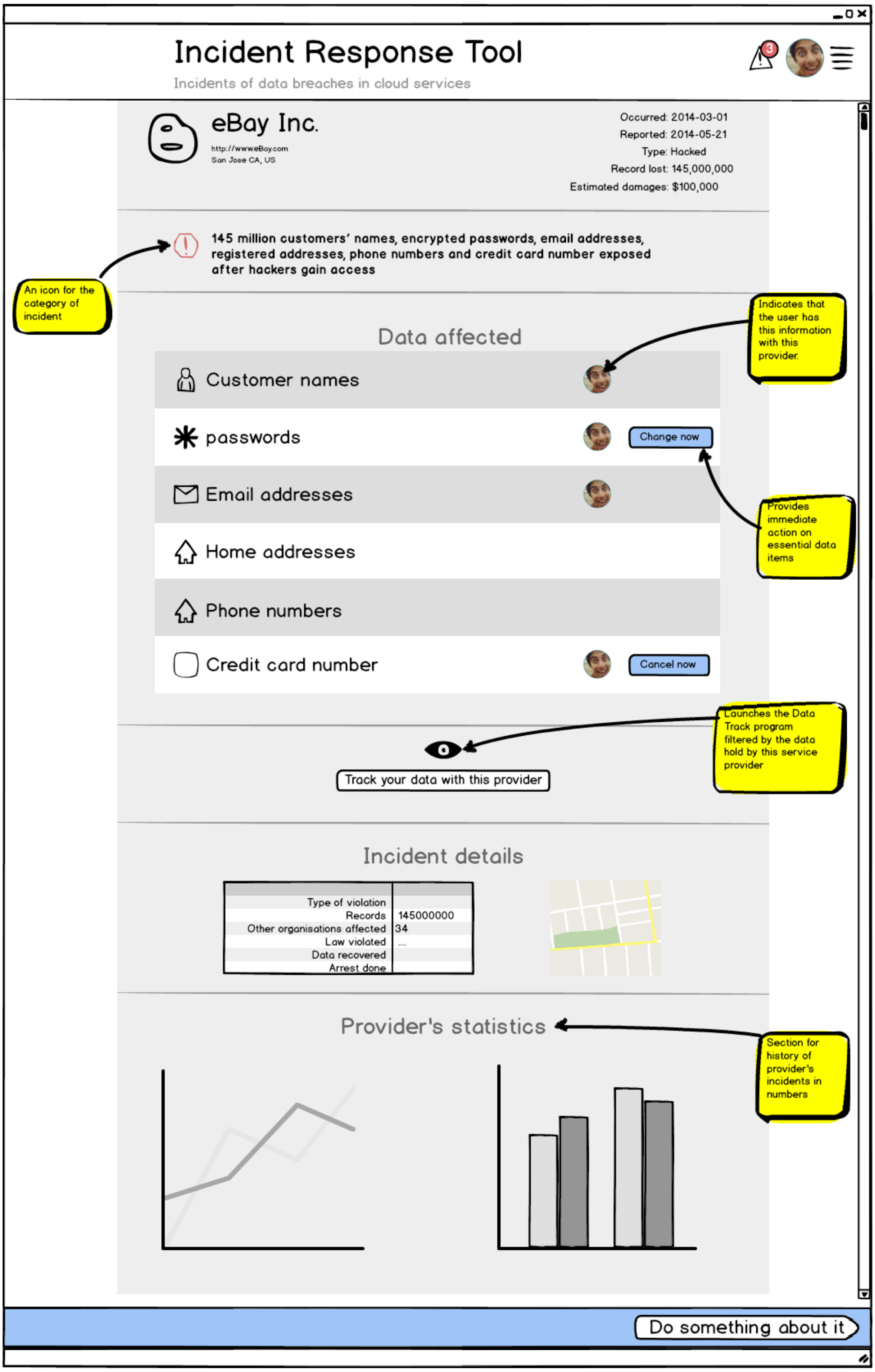
For instance, for indicating the importance of an incident, the incidents could be grouped, sorted and coloured coded according to the assessment done by the PAPV. Also, icons representing the user's personal data that might be affected by the incident can be listed at the bottom.

New incoming notifications could be shown in a standard way by placing a coloured circle with a number in the navigation bar at the top of the interface, thus becoming unobtrusive but always accessible when the user wants to navigate to a particular incident and take action. A very short summary of the incident can be presented, and placing the service provider's icon can make the user recognize the provider that have their personal data. The assessment done by the PAPV can also indicate the importance of the incident by placing a subtle colour bar on the side, or colouring the whole row to invoke a feeling of a more important incident. These design ideas are portrayed in the mock-up of Figure 34.

Detail view for a particular incident. When the user has identified and selected an incident that is of interest, a detailed view of that incident will be shown. At this point of the A4Cloud project the type of information that an incident might contain has not yet been specified. Nevertheless the sample mock-up shown in Figure 35 presents one design idea based on the information contained by a data breach incident in the DataLossDB service[13].

In this view, the cloud subject can see clearly at the top the service provider from where the incident originated and its contact information. Brief factual information, such as the date the incident occurred, date it was reported, the type of incident and others are also presented. A brief description of the incident is highlighted, and an icon representing the type of incident according to a defined typology is also shown so that the viewer recognizes. Then, a list of the type of personal data affected is shown, and the user can see if she had these affected data items stored at this service provider. At this point the user is also given the possibility to look at all the data about herself that is stored at the service provider affected by the incident. This might launch an appropriate visualization of the Data Track tool (Section 3.5) filtered to only show the data at this particular provider. The interface can also show more information about the incident and statistics about the incidents in which the service provider might have been involved.

[13] Most of the information about the incident presented in the mock-up comes from an actual incident involving eBay reported in DataLossDB - http://datalossdb.org/incidents/12625-145-million-customers-names-encrypted-passwords-email-addresses-registered\-addresses-phone-numbers-and-date-of-birth-exposed-after-hackers-gain-access.



Incident Response Tool

Incidents of data breaches in cloud services

eBay Inc.

http://www.eBay.com
San Jose CA, US

Occurred: 2014-03-01
Reported: 2014-05-21
Type: Hacked
Record lost: 145,000,000
Estimated damages: $100,000

145 million customers' names, encrypted passwords, email addresses, registered addresses, phone numbers and credit card number exposed after hackers gain access

An icon for the category of incident

Data affected

Indicates that the user has this information with this provider.

- Customer names
- passwords — Change now
- Email addresses
- Home addresses
- Phone numbers
- Credit card number — Cancel now

Provides immediate action on essential data items

Track your data with this provider

Launches the Data Track program filtered by the data hold by this service provider

Incident details

Type of violation	
Records	145000000
Other organisations affected	34
Law violated	....
Data recovered	
Arrest done	

Provider's statistics

Section for history of provider's incidents in numbers

Do something about it

Figure 35: The detailed view about a particular incident.

3.8.3. Initial UI prototypes for cloud customers and providers

The characteristics of the incidents that will occur in a cloud ecosystem is independent of who owns the data. Moreover, the main purpose of the IRT is to provide information about the incidents. The IRT could thereforeuse similar user interfaces for individual cloud subjects and businesses. This would reduce the learning curvefor business users who also may use the IRT to receive alert regarding their personal data.

Some differences would be present, due to the different nature of incidents, depending on the type of services the business utilizes. Apart from that, only the button named ”Track your data with this provider” in Figure 35 would need to have a change in behaviour. When the business user clicks this button, he could be taken to the data locator of DTMT instead of Data Track.

It is important to note that even though the user interface might mostly look and behave the same, there needs to be clear indications of whether the users are logged in to their personal account or the business account.

3.8.4. Verification against use case scenarios

In this subsection we analyse to what degree the current version of the Incident Response Tool is able to address the concerns of the personas described in the A4Cloud project deliverable DB3.1 [BFS+13].

First we outline the scenarios that describe the activities that happen after an incident has been detected and then we briefly summarize whether IRT will be useful in these scenarios.

Scenario 3.1.3a: Michael This scenario describes how Michael, who is a privacy officer and cloud service user, is notified about policy violations that occur. The Incident Response Tool can be of help with this as its task is to inform the user about violations that have occurred.

Scenario 11.1.1a: Edgar This scenario describes how Edgar, who is a cloud infrastructure administrator, opens a plugin to assess the significance of a policy violation. The Plug-in for Assessment of Privacy Violations, which is a part of the Incident Response Tool, can be of help with this task.

Scenario 12.1.1b: Frank This scenario describes how Frank, who is a data protection officer and auditor, provides proper notification to the different stakeholders involved in the cloud service ecosystem. The Incident Response Tool can be of help bringing the notifications to the user.

Scenario 13.1.1c-e: Sandra These scenarios describe how Sandra, who is an individual employee and end user of cloud services, will be able to access policy violation information about the cloud services she is using. She will have access the moment the violation occurs. The Incident Response Tool can be of help with this task, notifying her about the violation and offering easy access to more information.

Scenario 13.1.1f: Sandra This scenario describes how Sandra, who is an individual employee and end user of cloud services, is to be able to report any policy violation she is experiencing to the service provider. The Incident Response Tool is supposed to support this, but the current version of the mock-ups do not include this feature.

Scenario 13.1.1g: Sandra This scenario describes how Sandra, who is an individual employee and end user of cloud services, will be notified about any policy violation occurring throughout the cloud supply chain. The Incident Response Tool can be of help with this task, allowing for notifications to be sent to Sandra and her to review them.

Scenario 14.1.1c-d: Paul These scenarios describe how Paul, who is the Chief Privacy Officer of a SME moving most of its services to the cloud, is notified about policy violations in the cloud supply chain. The Incident Response Tool can be of help with this task.

Scenario 14.1.1e: Paul This scenario describes how Paul, who is the Chief Privacy Officer of a SME moving most of its services to the cloud, needs to be able to notify customers and employees about any incident occurring throughout the cloud supply chain. The Incident Response Tool can be of help with this task, allowing the employees and clients to register a connection to his service.

Scenario 15.1.1d: Roger This scenario describes how Roger, who is the Chief Technology Officer of a cloud service provider, needs to be able to notify cloud users about any incidents occurring throughout the cloud supply chains. The Incident Response Tool can be of help with this task, allowing users to register a connection to his service and receiving notification upon incidents occurring.

Most identified use case scenarios are fulfilled by mock-ups and tool description. Scenario 13.1.1f would be fulfilled if the user is allowed to report any policy violation to the service provider.

3.8.5. Early feedback by tool owners

This section describes the feedback given by the tool owner as a response to the chapter presented above and will be used for guidance for future work on the Incident Response Tool. The main feedback concerned the areas of architecture and what information to display. In short the tool owner envisions IRT to be primarily a tool used on mobile devices with a minimized amount of information to be displayed; the rationale behind these points will be elaborated bellow.

People are increasingly spending more and more time using mobiles, phablets, and tablets on the expense of desktops and laptops. Additionally, while laptop and desktop users will also use mobile devices the opposite is not necessarily true. Hence by making the ITR a mobile based system it will automatically reach a larger user group. As people are more often close to the mobiles than to desktop devices the ITR will be able to disseminate information regarding incidents instantaneously and users to react as soon as their data has been compromised.

Furthermore, by minimizing alerts to in-app push messages instead of using for instance emails or text messages users will not have to worry about phishing attacks or other types of fraudulent scams.

As already shown there is a great amount of information regarding incidents that could be shown to the user of the IRT. However, in order to make it easier to comprehend the severity of the incidents and to what extent the user needs to take active steps to remedy the situation the tool owner suggests that incidents should be divided into two categories only: those that directly affect the user and those that pertain to a cloud service registered in the app but not directly affecting the user. Incidents that directly affect the user should be pushed to the app directly whereas incidents that pertain to the service should be shown when the user' opens the app on their own violation. The main focus of the top level of the push information should be: This incident is happening and these are the possible options to remedy the issue (such as depicted in Figure 34). As a response to this tool owner's response, we however

want to emphasise that developing a desktop-based tool and interfaces has advantages in comparision to a mobile solution for the following reasons: (1)it enables users to view and react on notifications in a more user-friendly manner, (2) we may not assume that all users are also in possession of a mobile device, (3) within the project, the decision was made at an early stage to use web-based technologies for the tool development. The integration of a mobile ITR with the Data Track based on web technologies will not be straightforward, (4) push notification with sensitive information about used services and incidents would cause many privacy and security risks that will not be easy to address. Having said this, it may still be possible to include functions in Data Track or IRT that allow to send notifications to the users' mobile device if configured accordingly (informing just about the fact that an incidence occurred or was reported with no further information), as discussed above in the section on "Notifying users of important incidents".

3.9. Remediation and Redress (RRT)

Key elements for accountability within the A4Cloud project include the possibility of data subjects' right to remedy occurring incidents and to obtain redress in case a breach of policy and obligations have occurred and when some kind of compensation need to be given to the data subject (cf. Art 22, 23 EU Data Protection Directive 95/46/EC).

Therefore, in A4Cloud an interactive tool for supporting the concepts of remediation and redress has been envisioned. This "Remediation and redress" tool (RRT) will respond to (perceived) incidents in the arrangement of the corresponding users. Possible users of this tool include individual cloud subjects or cloud customers looking for remediation or redress after becoming aware of an incident regarding their data in the cloud. Interaction with this tool can be triggered in different ways:

1. When an incident has been reported by the Incident Response Tool (IRT) (Section 3.8), the RRT can be triggered. In this case, the tool will know what type of incident has occurred and what possible actions can be taken. It will guide the user through these actions, which may involve composing request or asking questions to the cloud service provider, or possibly contacting a Data Protection authority to take some kind of action (file a complaint or take legal action).

2. Users might consult the RRT without being triggered by the IRT. In this case, the tool will engage in a dialogue with the user to establish their concern and guide them through appropriate possible actions.

3. When appropriate the tool will take automatic action for communicating the request for remediation or redress through the possible APIs provided by the Cloud service provider and/or by the Data Protection Authority.

The output of the tool can be a set of potential actions that the user can take to obtain redress or carry out a remedy. It is important to note that the purpose of the tool is not to guarantee that users will obtain remediation or request to users, but rather to help users create and send a remediation or redress request to the appropriate authority (either the CSP, Data Protection Authority, or similar). The tool has also the purpose of educating the stakeholders on possible incidents and their potential actions and procedures for remediation of these incidents.

Requirements for exercising data subjects' rights were elicited through various user centred design activities. One of such requirements identified in A4Cloud's deliverable D:C-7.1 [AFHP$^+$13] include making users aware of their rights and supporting them to exercising these rights, as well as providing clear statements of the rights that apply to a user given his or her context.

3.9.1. User's goals and task analysis

Based on the description for the RRT made available by WP:D-4 and on the identified requirements presented above, in this section (as with the many of the tools described in this document) we again present an UML use case diagram (Figure 36) and carry out a task analysis for the first iterations of the design of this tool (presented in Appendix A.9). This analysis has the purpose of specifying some of the concrete tasks that users will need to perform with this tool in order to succeed in sending a remediation or redress request.

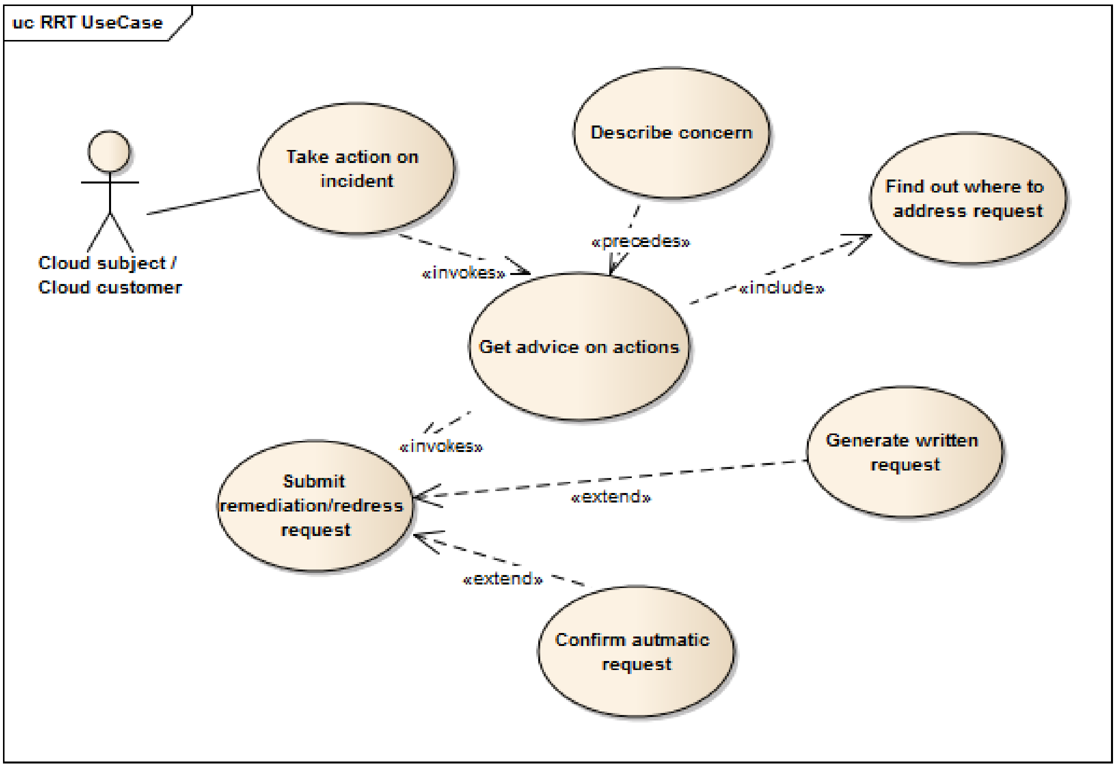


Figure 36: UML use case diagram of the Remediation and Redress Tool

The UML use case diagram starts by describing the cloud subjects' (or users') ultimate goal when using this tool, namely to take an action on an existing incident. If the incident is detected by the IRT (Section 3.8) the RRT tool will *know* most of the necessary information needed to complete a remediation or redress request, such as the type of incident, the best approach to request remediation, the contact details of the involved services or corresponding authorities, and others. This information can then be presented to the users, giving them the possibility to modify some parameters, and providing them with an simple way of submitting a remediation request by, for instance, pressing a button to confirm the shown information and send the request (as mocked-up in Section 3.9.2).

If the user initiates the request for remediation herself, then she could be given different alternatives to choose from, with the purpose of making the process of filling the request easier. In one alternative the interface will give her the option of choosing the type of help she needs, either seek direct remediation with the cloud service provider, obtain legal help or practical advice, or contact an authority (e.g., the data protection authority or consumer agency in her region).

Another alternative could be that she starts by describing her concern about a known incident. To make the process simple for the user, the tool could present a list of major recognized incidents and allow users to select the option "I have been affected!" and enter a description of the incident and information needed for the remediation. If the incident is not recognized by the RRT, then the user will engage in a more robust dialogue, where she would need to complete more details about the incident and justify the remediation requests. Section 3.9.3).

3.9.2. UI mock-up - Remediation triggered via the IRT

The first case, the RRT would be triggered when the user wants to take an action on an incident described by the IRT. In this case, most of the information about the incident will be known to the tool, which intelligently will automatically fill in the necessary information to create an electronic remediation request to the cloud service provider.

In this scenario, we envision three main steps. In the first, users would just confirm the information presented about the incident and their contact information necessary for the service provider to get in touch with them (Figure 37).

In the second step, users will be shown a preview of the remediation request in a similar format in which it will be seen by the recipient (Figure 38). At this point users could choose the appropriate authority to submit the request to according to the nature of the incident. For instance, in some situations users might be encouraged to send the request directly to the cloud service provider, while in others it would be more appropriate to contact a consumer agency or data protection authority depending on the user's jurisdiction, the type of service, etc. Once everything is in order, users can click a button that will sign and submit the request.

In the final step, users will be given a kind of receipt of their transaction with the opportunity to save this record in a printed or digital format.

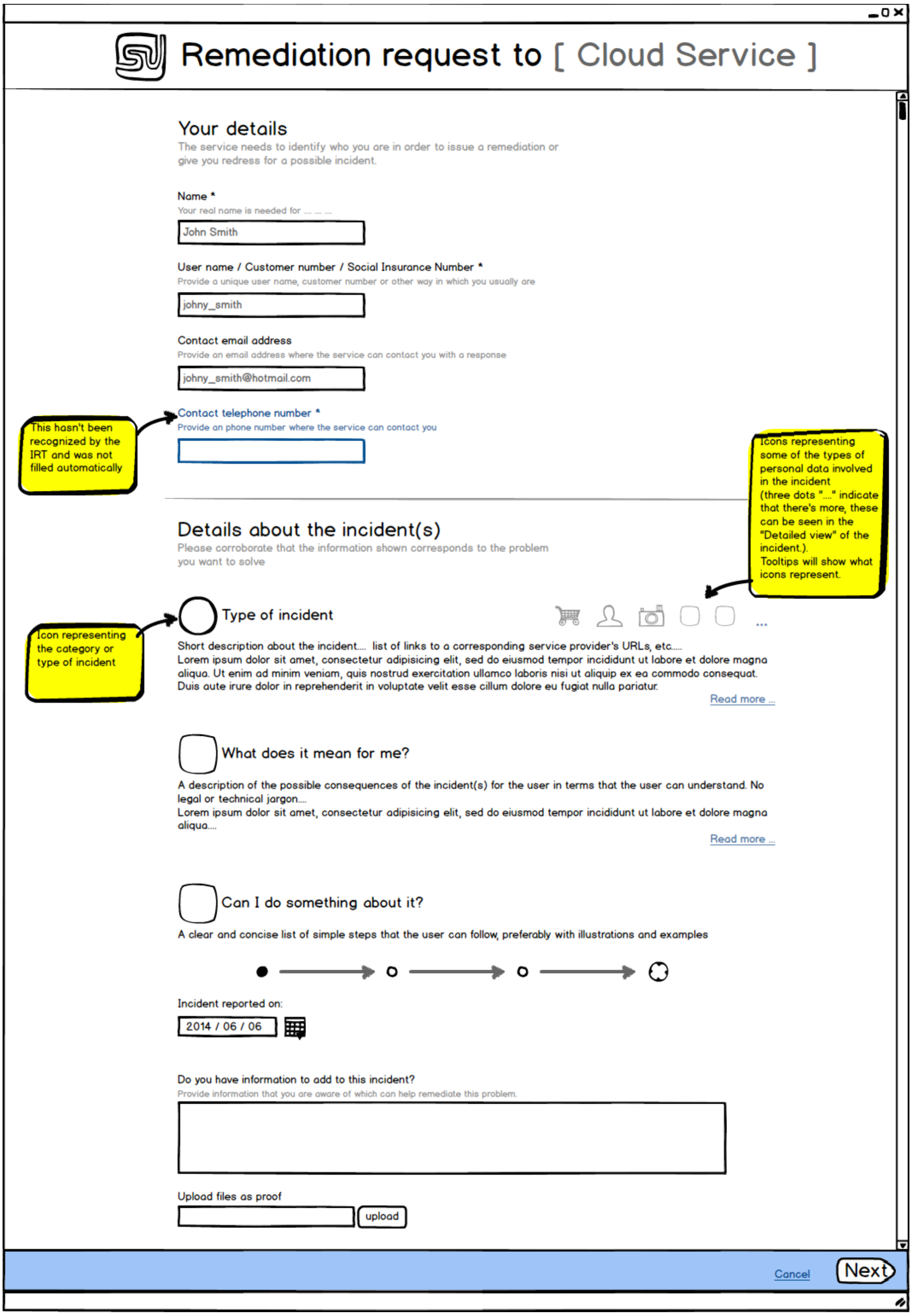
3.9.3. UI mock-up - Remediation trigged by user's initiative

In the second case, the request for remediation would be initiated by the user herself. Scenarios of this case include, for example, the user finding out about an incident in the news about a cloud service where she has an account; or the user realizing that content concerning her has been uploaded to a cloud service by a third person or party, and she wants to request this content to be removed or corrected. Similarly, a recent example that has recently been set in practice due to the new European regulations is shown by the recently launched service by Google, which allows people in Europe to request for personal data to be removed from online search results[14].

In this case, the user could be presented with three simple options to initiate a request for remediation (Figure 39). As a first approach, users should be nudged into trying to resolve any dispute by contacting the service provider directly. If an agreement cannot be reached this way, users could be given the option of contacting an authority within their jurisdiction. Users could also be given advice on what to do in order to achieve remediation, which in turn, educates them on possible breaches and the protection of their personal data.

When choosing the option of obtaining remediation directly from the service provider, the users could be presented with a list of known service providers who have recently reported

[14] `https://support.google.com/legal/contact/lr_eudpa`, accessed 2014-06-02.



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 ....

John Smith

User name / Customer number / Social Insurance Number *

Provide a unique user name, customer number or other way in which you usually are

johny_smith

Contact email address

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

johny_smith@hotmail.com

Contact telephone number *

Provide an 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

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

Type of incident

Short description about the incident.... list of links to a corresponding service provider's URLs, etc.....
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

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....
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua....

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:

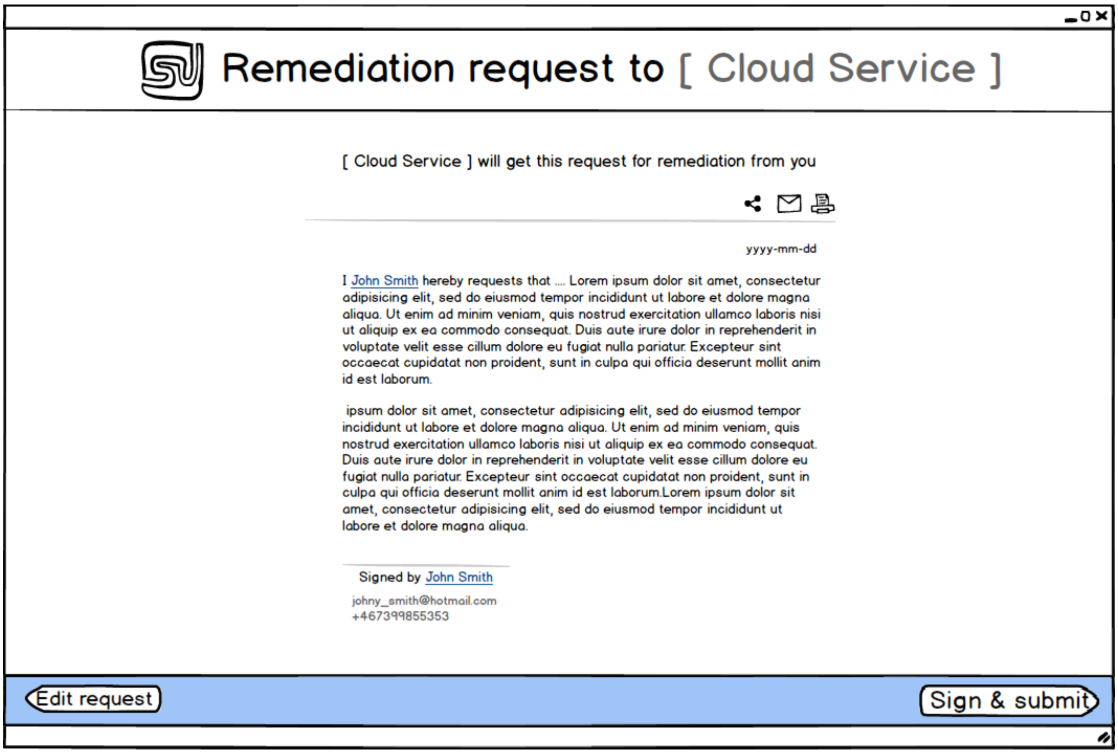
2014 / 06 / 06

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

Figure 37: When the RRT is triggered by the IRT, users can review and complete the remediations request.



Remediation request to [Cloud Service]

[Cloud Service] will get this request for remediation from you

yyyy-mm-dd

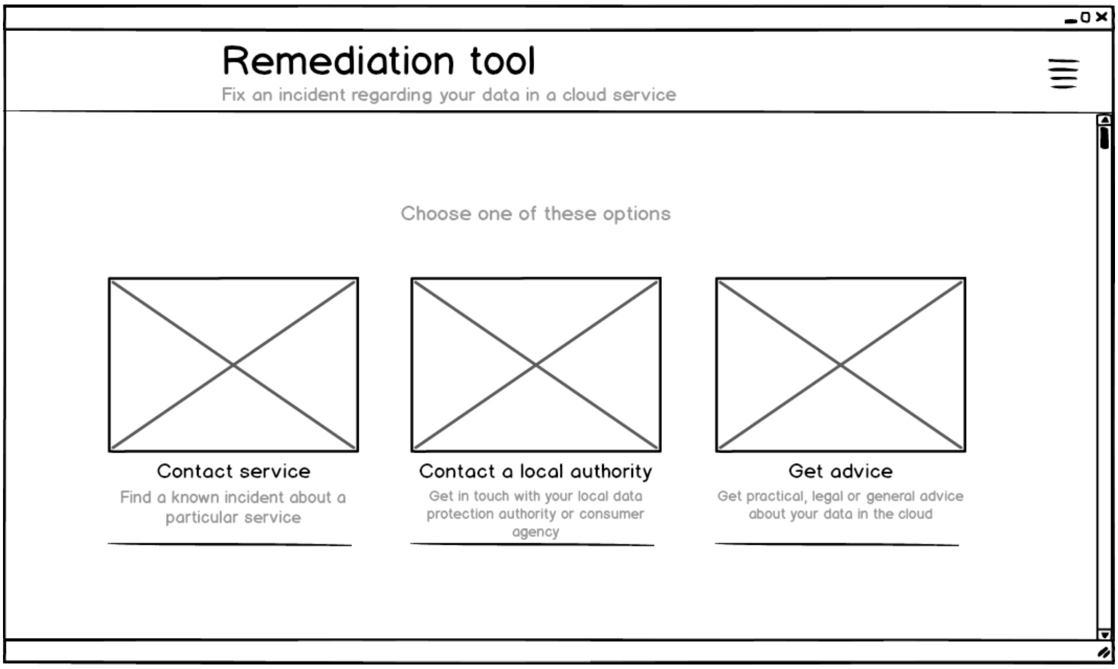
I John Smith hereby requests that .... Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Signed by John Smith

johny_smith@hotmail.com
+467399855353

Figure 38: Users then can get a preview of the request and submit it to the service provider.



Remediation tool

Fix an incident regarding your data in a cloud service

Choose one of these options

Contact service
Find a known incident about a particular service
Contact a local authority
Get in touch with your local data protection authority or consumer agency
Get advice
Get practical, legal or general advice about your data in the cloud

Figure 39: Users can choose the action to take to initiate a remediation request.

an incident or which incident was severe. Users could then choose the service that they are subscribed to and at a later step fill in their personal details and other information that can help the assessment of the remediation request, similar to the form shown in Figure 37.

3.9.4. Verification against use case scenarios

In this subsection we analyse to what degree the current version of the RR tool is able to address the concerns of the personas described in the A4Cloud project deliverable DB3.1 [BFS+13]. First we outline the scenarios that describe the activities that happen after an incident has been detected and then we briefly summarize whether the RR tool will be useful in these scenarios.

Scenario 3.1.3b: Michael This scenario describes how Michael, who is a privacy officer at a hospital needs to investigate what actions that needs to be taken redress the affected parties after an incident has happened. The hospital is a cloud customer and data controller in the healthcare use case and Michael is therefore one of the intended users of the RR tool. The RR tool can help Michel in this scenario.

Scenario 6.1.1b: Leslie This scenario described how an adviser at a DPA makes a person (a data subject) aware of the RR tool and how she provides him with legal guidance when he is using the tool to fill out the compensation request form. This scenario emphasizes the need for the RR tool, even though employees at a DPA are not the intended users of the tool.

Scenario 12.1.1a-b: Frank These scenarios described how a DPA can use tools to support the handling of a large number of complaints concerning cloud services. The RR tool can be of these tools that the scenarios refer to. (Note that, similar to scenario 6.1.1b, employees at a DPA are not the intended users of the tool.)

Scenario 17.1.1b: John This scenario assumes that some data protection infringements have happened and it describes how an adviser at a DPA initiates a process that may lead to sanctions to cloud services providers. The RR tool cannot be directly applied in this scenario.

To summarize, the scenarios described in DB3.1 are mostly concerned with the role of the DPA when it comes to remediation and redress activities. Since the main target user group of the RR tool are cloud subjects and cloud customers, it is difficult to verify whether the tool is able to address the concerns of its intended users. However, our brief analysis above indicates that the tool may be of use in some settings, in particular since it provides affected parties with a way to submit remediation and redress requests without involving the DPAs, hence preventing the DPAs from becoming overloaded with large amounts of inquiries that otherwise have to handled manually.

4. Toolset Integration

The HCI task within A4Cloud work package D-5 aims at developing usable UI prototypes for various combinations of tools assembled to address stakeholder-specific needs. User interface prototypes for toolsets will be developed for the following stakeholder groups that integrate the consistently designed UIs for A4Cloud tools for these respective groups of users:

- **Individual cloud subjects:** The toolset for cloud subjects should combine different transparency and control tools for individuals, namely the Data Track, Incidence Response tool, Remediation and Redress tool, Plugin for Policy Violations, Transparency Log (TL), Data Subject Access Request tool, and Data Protection Impact Assessment tool into a coherent tool dashboard.

- **Cloud customers:** Cloud customers who want to adapt cloud computing will have an interest to use the DPIAT and the COAT tools. Moreover, organisation cloud customers whose data are already being processed in the cloud also need to use different transparency and control tools, which can be integrated into another toolset. These tools are the Data Transfer Monitoring tool, Incidence Response tool, Remediation and Redress tool, Plugin for Policy Violations, Transparency Log, as well as the Audit Agent System.

Proposals and concepts for tool integration and first mock-ups for toolsets for cloud subjects and for cloud customers will be presented and discussed below.

For **cloud providers and their data protection officers (DPOs)** the Accountability Lab tool is developed in A4Cloud that allows writing policy obligations and generating machine readable policies. At a later stage they may also use other tools, such as the A-PPL Engine and AAS. However, since these tools are used more or less independently of each other we have not designed any integrated tool set for them.

4.1. Toolsets for individual cloud subjects

As part of the A4Cloud project we are considering to integrate features related to transparency and accountability in cloud services into a single service. We envision some type of cloud subject dashboard from where individual cloud subjects can access different mechanisms to visualize their disclosures and control their data using the Data Track tool (Section 3.5). They can be notified about possible incidents regarding their data stored at cloud services with the Incident Response Tool (Section 3.8), which assesses incidents related to policy violations according to the Plugin for Assessment of Policy Violations (Section 3.5.4). Whenever possible, cloud subjects would also be able to request compensation or to take appropriate action in order to rectify an incident using the Remediation and Redress Tool (Section 3.9) from within the dashboard. Moreover, functionality for the Data Subject Access Request Tool (Section 3.4) in the dashboard would allow cloud subjects to obtain an offline written request to the cloud service provider to access the data stored on their servers.

The diagram in Figure 40 taken from the work done by Task 2 of WP:D-5, shows the big pictures on how the Data Track and other A4Cloud tools are related to each other. For a detailed description of this diagram, the reader is referred to the Overview chapter in the Deliverable D:D-5.2 on “User-Centric Transparency Tools V.1”.

Figure 41 shows a mock-up of a toolset for cloud subjects showing the traceview visualisation as well as icons on the right side of the menu bar with icons and status information for other cloud subject tools that can be enabled by mouse clicks.

Figure 42 shows a mock-up of the interface that appears if the Incidence Response tool icon has been clicked showing an overview of current incidents.

Figure 43 shows a mock-up for user interfaces visualising details of incidents. The user interfaces of the Incidents Response Tool also contains links for activating the Remediation and Redress tool, and are thus addressing the HCI requirement that we elicited for the Deliverable D:C-7.1 [AFHP+13] stating that control options that are relevant in a certain context should be made available and obvious in that context.

Figure 44 provides a hi-fi prototype for a dashboard named “GenomSynlig”combining different tools for cloud subjects. The Swedish words “GenomSynlig”and “Synlig” mean “transparent” and “visible”. The dashboard provides so far at its top layer access to the Data Track tool functions and to the IRT. When clicking on the box with the eye-icon on the left-side, the user could for instance filter and track the services to that the users disclosed data. The box on the right side with the person-icon will allow users to filter and track the personal data attributes that were disclosed to different services. The middle box with the bell-icon informs about the number of incident alerts and will activate the IRT if clicked. The DataTrack with the trace view visualisation or the IRT can also be activated via clicking the eye- or the bell-icon on the right side of the menu bar.

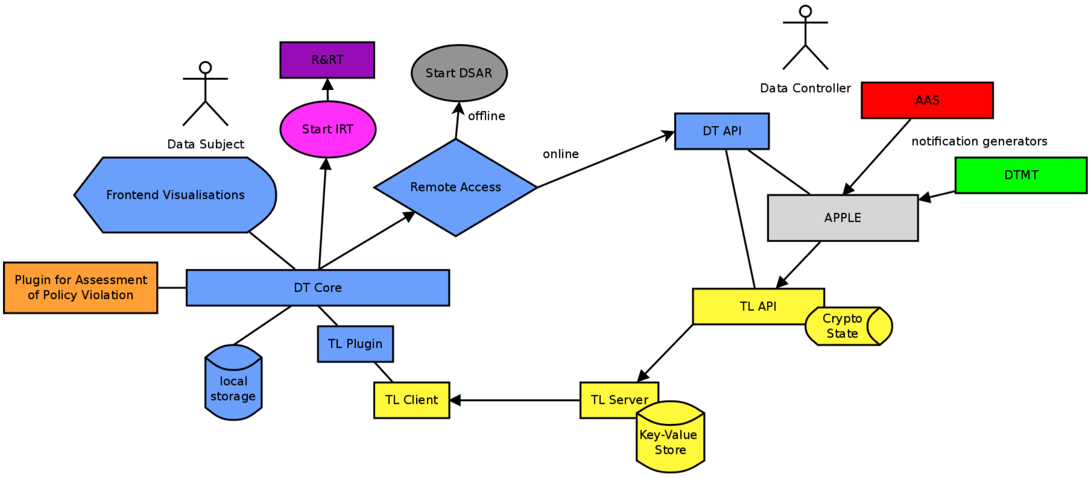


Figure 40: Diagram showing the relationships between the Data Track and other A4Cloud tools for individual cloud subjects.

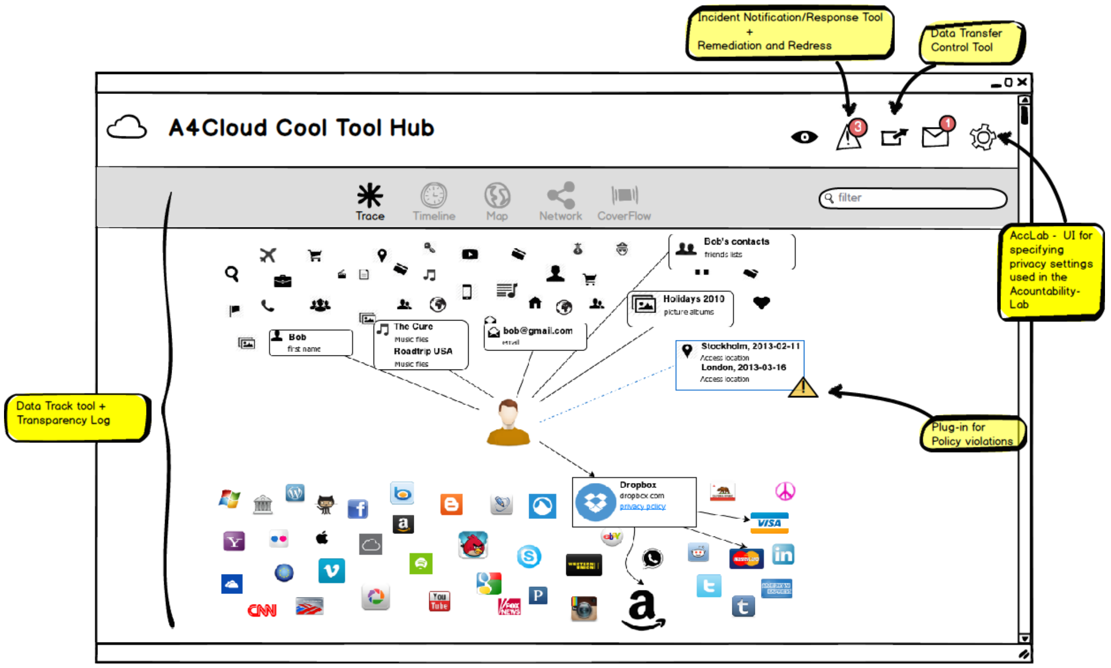
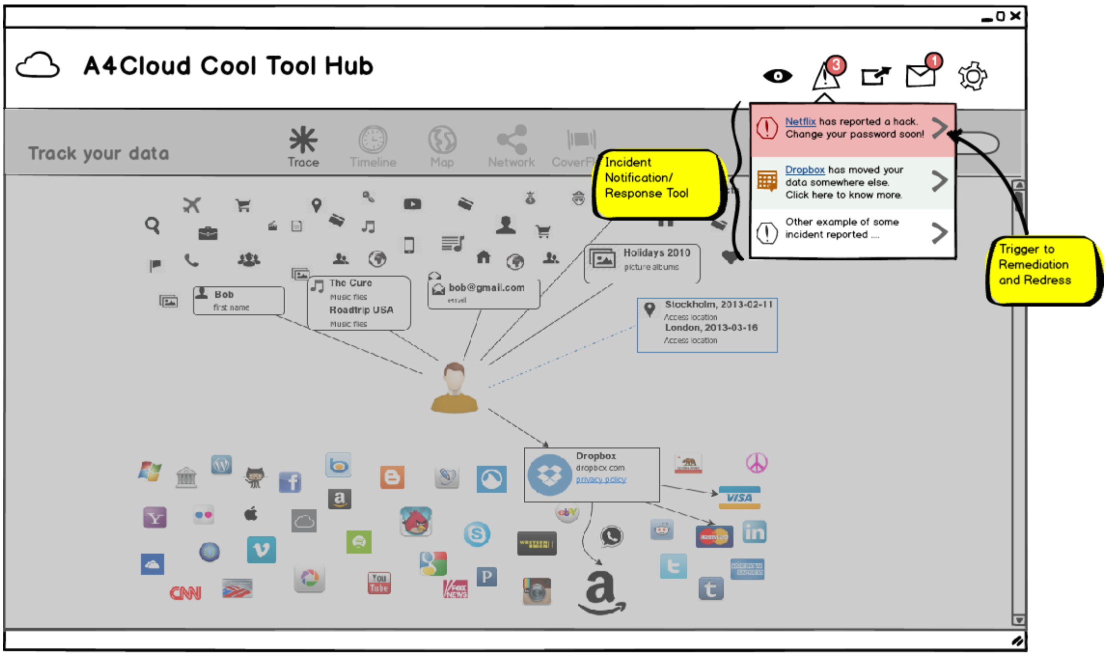


Figure 41: Mock-up of toolset for cloud subjects showing the traceview visualization.

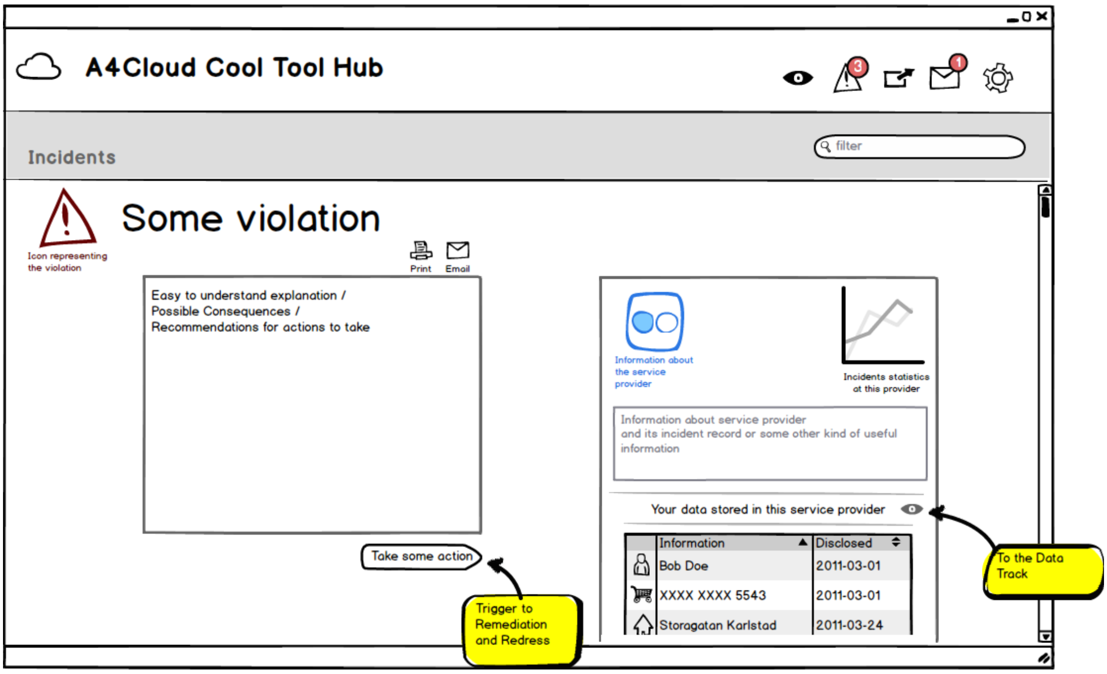


Netflix has reported a hack.
Change your password soon!

Dropbox has moved your
data somewhere else.
Click here to know more.

Other example of some
incident reported ....

Figure 42: Mock-up of toolset for cloud subjects showing the overview of the current incidents.


A4Cloud Cool Tool Hub
Incidents
filter
Some violation
Icon representing the violation
Print
Email
Easy to understand explanation / Possible Consequences / Recommendations for actions to take
Take some action
Trigger to Remediation and Redress
Information about the service provider
Incidents statistics at this provider
Information about service provider and its incident record or some other kind of useful information
Your data stored in this service provider
To the Data Track

Information	Disclosed
Bob Doe	2011-03-01
XXXX XXXX 5543	2011-03-01
Storagatan Karlstad	2011-03-24

Figure 43: Mock-up of toolset for cloud subjects showing a detail view for one possible incident.

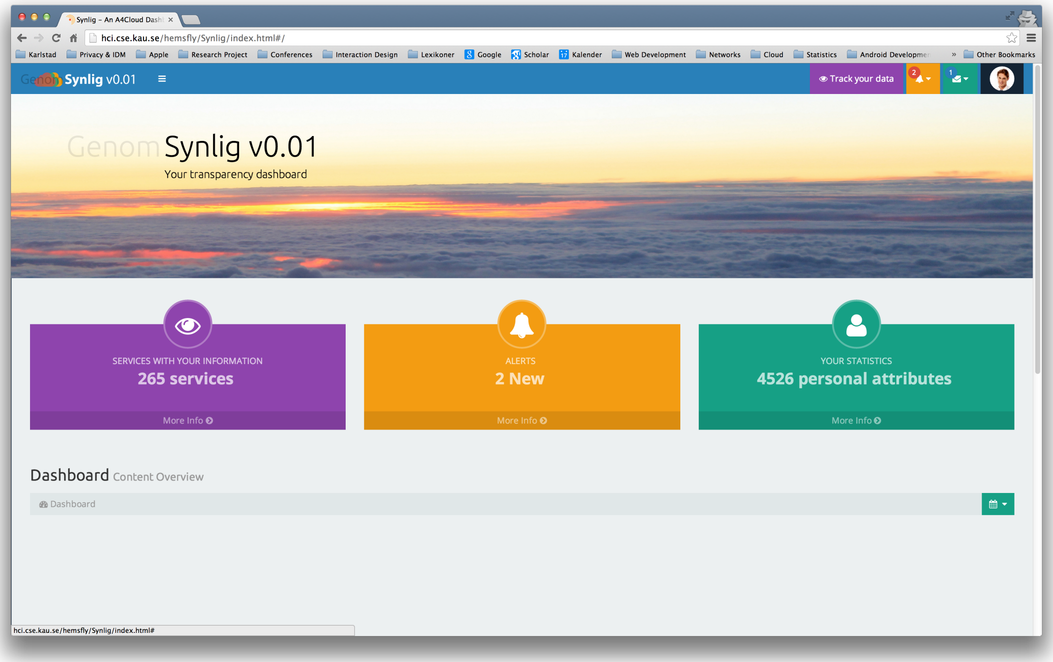


Figure 44: Hi-fi prototype of toolset for cloud subjects.

4.2. Toolset for cloud customers

Within the stakeholder group of cloud customers, which comprises SMEs as well as individual and business cloud users, we have identified two possible toolsets. One of the toolsets will appeal to those cloud costumers who are looking to adopt cloud computing solutions, while the other toolset will be directed at costumers who are already using cloud computing and are looking for transparency tools for controlling and monitoring the data that they place in the cloud, similar to the toolset described in Section 4.1.

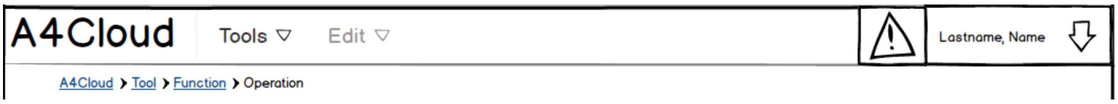


Figure 45: Menu for toolset, with breadcrumbs

To integrate all the tools in a usable manner, the system could have a simple menu bar on the top as shown in Figure 45. The menu bar could hold a tools element, giving the users access to all the available tools, an edit menu, notifications and profile access. The users could also be informed about their position in the tool at any given time by having breadcrumbs under the menu.

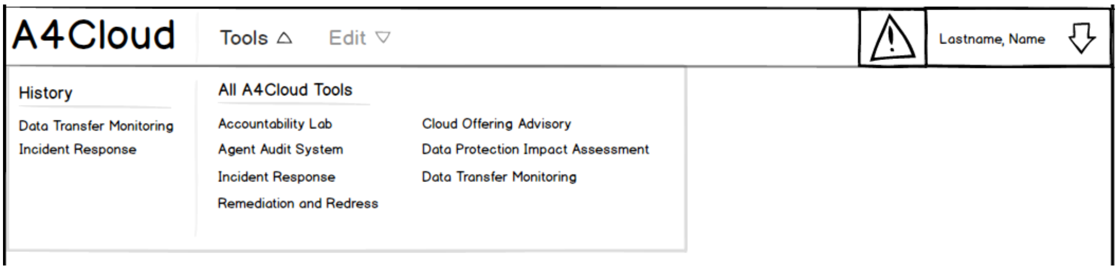


Figure 46: Open menu for selecting among all tools in toolset

When the users clicks on the “Tools” element, a menu opens and gives them access to all available tools, as can be seen in figure 46.

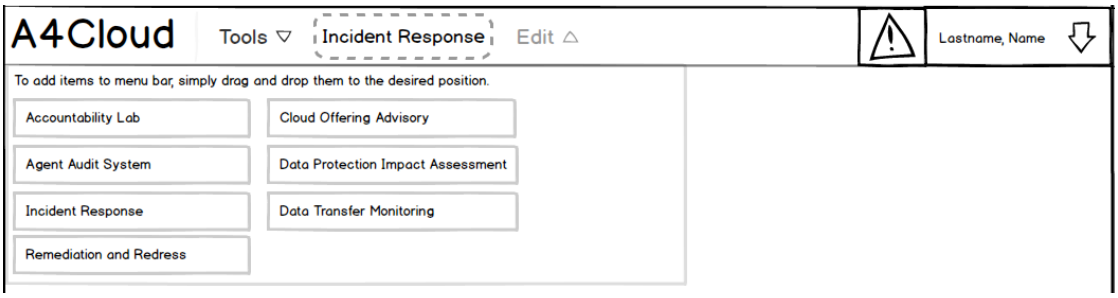

To add items to menu bar, simply drag and drop them to the desired position.

Figure 47: Open edit menu to customize the main menu bar

By clicking on the “Edit” element, the users could get access to customizing the main menu bar, as can be seen in Figure 47. This could allow the users to adapt the toolset to their preferences way of working.

The menu elements could be rearranged by dragging and dropping them in place where the users want them placed.

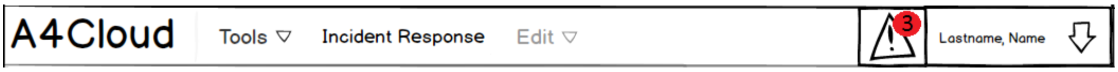


Figure 48: Updated menu after adding Incident Response

When the users close the “Edit” element, the new menu elements are docked in place where the user put it. This can be seen in Figure 48 which also shows three policy violation notifications.

This solution is based on the AWS Management Console [Ohlb] from Amazon.

4.2.1. Toolsets for cloud customers for evaluating Cloud Computing implications and options

Both DPIAT (section 3.7) and COAT (section 3.3) are intended for SMEs, while COAT is also intended to be used by cloud subjects.

Both these tools will most likely only be used during the procurement phase. Cloud subjects will not switch services very often, and only occasionally subscribe to new cloud services. SMEs will not switch services very often, but in some cases it might be more frequently than the cloud subject due to a larger focus on cost. The DPIAT tool might be used more frequently as the SME would need to do a new risk analysis when storing new types of data or laws change. Both tools might be used once or up to a few times a year by SMEs. Cloud subjects would probably not use COAT more than once a year[15].

Both tools have a logging component for logging the user’s choice for accountability purposes. For the logging to be of value, it would be necessary to be able to identify who used the tool. One way of knowing who is using the tool, is by having the user log in. This is a method the user is familiar with, would accept and to some degree understand. However, COAT can still be used anonymously without logging in if the user choose to do so.

It would be preferable, but not mandatory, if the user could reuse information he has entered into DPIAT when using COAT and the other way around. This would reduce the work load on the user when it comes to assessing risk and acting on them in a responsible manner.

Assessing risks with DPIAT and receiving recommendations for cloud services from COAT are focused tasks, requiring extensive interaction with the user through questions and answers. Such focused tasks, requiring extensive input from users are most efficiently done on an ordinary computer. Given that most individuals are busy and time used is money spent for businesses, all mock-ups of the interfaces aimed at professionals and business users are desktop based.

[15] Note that these are only assumptions; we do not have any emphirical results to back up these claims.

4.2.2. Toolsets for cloud customers for enhancing transparency and control

DTMT DTMT (Section 3.6) is intended to be used by the privacy officers of data controllers as well as internal and external auditors.

The tool will probably be used rarely, as the information is only of interest when a policy is breached. When that occurs the user is notified. Auditors might execute audits at any given time, when tasked to do so.

Due to getting access to potentially sensitive information about where certain data is stored, the tool will require the user to log in or in other ways verify his identity.

IRT, RRT and PAPV IRT (Section 3.8) and RRT (Section 3.9) are intended for SMEs and individual cloud consumers. PAPV (Section 3.5.4) is intended for individual consumers in the role of data subjects and Data Protection Commissioners as the data subject's representative.

The tools are likely to be used only when the user is notified about an incident. Therefore the frequency of use depends entirely on how often and how many incidents occur. The use might vary from multiple times a day to a few times a year.

There might be a difference in the context of use, between the individual cloud subject and businesses. While the individual cloud subject might prefer to receive a notification on his phone, this might not be desirable in a business context for reasons such as work time and security. The individual cloud subject might primarily be interested a quick fix for the incident, the business might also be interested in a full report allowing them to investigate and learn from the incident. The business might also be interested in the systems communicating directly, so that their systems might take automatic action upon incidents.

Preferably all events, from all the tools that will generate notifications that might be classified as incidents, show up in the IRT and not in the tool itself. This would make the tools feel more tightly integrated even while staying modular in nature.

In order for the user to receive only relevant incident and for the tool to send requests on the user's behalf, the tool needs to know who the user is. One way of solving this, which is familiar to the user, is with login.

AAS AAS (Section 3.2) is intended for auditors.

The tool will probably be used upon request, but given that the auditors likely are professional auditors, the tool might be used daily.

The tool allows the auditor to assess the security controls put in place in cloud ecosystems. In order for this not to become a way of harvesting information before an attack, some authentication is probably needed. Login is a method well known to the user.

5. Concluding Remarks

In this deliverable, we have presented the initial UI prototypes for A4Cloud tools and integrated toolsets for the different stakeholders, namely cloud subjects, cloud consumers and data protection officers of cloud providers, that we have developed following user centred design processes.

Even though these mockups are mostly preliminary and will need further refinements and tests, they have already been helpful in discussions with the tool owners and other project partners, the A4Cloud advisory board and end user focus groups for getting helpful first feedback. Such feedback as well as further user tests to be performed, will be input for the next round of mockup iterations.

The final final user interface prototypes for toolsets for the different stakeholders will be implemented and presented in the upcoming deliverable D:D-5.3 "*User Interface prototypes V2*" at project month 36.

References

[AFHP$^+$13] Julio Angulo, Simone Fischer-Hübner, John Sören Pettersson, Erik Wästlund, and Leonardo Martucci. D:C-7.1 General HCI principles and guidelines for accountability and transparency in the cloud. Project deliverable D:C-7.1, A4Cloud Project, September 2013.

[AKLS13] Alessandro Acquisti, Ioannis Krontiris, Marc Langheinrich, and Martina Angela Sasse. 'My Life, Shared' - Trust and Privacy in the Age of Ubiquitous Experience Sharing (Dagstuhl Seminar 13312). *Dagstuhl Reports*, 3(7):74–107, 2013.

[BFS$^+$13] Karin Bernsmed, Massimo Felici, Anderson Santana De Oliveira, Nils Brede Moe Jakub Sendor, Thomas Rübsamen, Vasilis Tountopoulos, and Bushra Hasnain. D:b-3.1 use case descriptions. Technical report, A4Cloud Project, June 2013.

[BNG11] 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.

[BOH11] Michael Bostock, Vadim Ogievetsky, and Jeffrey Heer. D^3 data-driven documents. *IEEE Transactions on Visualization and Computer Graphics*, 17(12):2301–2309, 2011.

[CBM11] Mick P. Couper, Reg Baker, and Joanne Mechling. Placement and design of navigation buttons in web surveys. *Survey Practice*, 4(1), 2011.

[CRC03] Alan Cooper, Robert Reimann, and David Cronin. *About Face 3: The Essentials of Interaction Design*. Wiley Publishing, Inc., New York, NY, USA, 3 edition, 2003.

[Dum13] Edd Dumbill. Making sense of big data. *Big Data*, 1(1):1–2, 2013.

[Eur12] European Commission. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final 2012/0011 (COD). Available at `http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf`, January 2012.

[Eur13] European Commission. Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Available at `http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf`, October 2013.

[Fal03] Daniel Fallman. Design-oriented human-computer interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, pages 225–232, New York, NY, USA, 2003. ACM.

[FHHW11] Simone Fischer-Hübner, Hans Hedbom, and Erik Wästlund. Trust and assurance HCI. In Jan Camenisch, Simone Fischer-Hübner, and Kai Rannenberg, editors, *PrimeLife - Privacy and Identity Management for Life in Europe*, chapter 13, page 261. Springer, June 2011.

[FHPB$^+$07] Simone Fischer-Hübner, JS Pettersson, Mike Bergmann, Marit Hansen, Siani Pearson, and Marco Casassa Mont. Hci designs for privacy-enhancing identity management. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati, editors, *Digital Privacy: Theory, Technologies, and Practices*. Taylor & Francis, 2007.

[Fre00] Linton C. Freeman. Visualizing social networks. *Journal of social structure*, 1(1):4, 2000.

[GFC04] 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.

[Goo] Google. Google dashboard. `https://www.google.com/settings/dashboard`.

[Hed09] Hans Hedbom. A survey on transparency tools for enhancing privacy. In *The future of identity in the information society*, pages 67–82. Springer, 2009.

[Her03] Morten Hertzum. Making use of scenarios: a field study of conceptual design. *International Journal of Human-Computer Studies*, 58(2):215–239, February 2003.

[HL12] Lane Harrison and Aidong Lu. The future of security visualization: Lessons from network visualization. *Network, IEEE*, 26(6):6–11, 2012.

[HPHL10] Hans Hedbom, Tobias Pulls, Peter Hjärtquist, and Andreas Laven. Adding secure transparency logging to the prime core. In *Post-Proceedings of the Fifth International Summer School: Privacy and Identity Management for Life, Nice, France, 7th - 11th September 2009*. in press, 2010.

[JWV13] Milena Janic, Jan Pieter Wijbenga, and Thijs Veugen. Transparency enhancing tools (tets): an overview. In *Third Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pages 18–25. IEEE, 2013.

[KMSH12] 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.

[KNP10] 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.

[KZH12] 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.

[LJH13] Zhicheng Liu, Biye Jiang, and Jeffrey Heer. imMens: Real-time Visual Querying of Big Data. In *Computer Graphics Forum*, volume 32, pages 421–430. Wiley Online Library, 2013.

[LS07] Jonas Löwgren and Erik Stolterman. *Thoughtful Interaction Design: A Design Perspective on Information Technology*. MIT Press, 2007.

[MP11] Andrew Vande Moere and Helen Purchase. On the role of design in information visualization. *Information Visualization*, 10(4):356–371, 2011.

[ND86] 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.

[Ohla] Ohloh. Apache openoffice. `https://www.ohloh.net/p/openoffice`.

[Ohlb] Ohloh. Getting started with the aws management console. `http://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/getting-started.html`.

[Pet08] John Sören Pettersson. HCI Guidelines. PRIME deliverable D6.1.f, February 2008.

[PFHB07] John Sören Pettersson, Simone Fischer-Hübner, and Mike Bergmann. Outlining "Data Track": Privacy-friendly data maintenance for end-users. In *Advances in Information Systems Development*, pages 215–226. Springer, 2007.

[PMR+96] Catherine Plaisant, Brett Milash, Anne Rose, Seth Widoff, and Ben Shneiderman. Lifelines: visualizing personal histories. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 221–227. ACM, 1996.

[PPW13] Tobias Pulls, Roel Peeters, and Karel Wouters. Distributed privacy-preserving transparency logging. In *Workshop on Privacy in the Electronic Society (WPES)*, pages 83–94, Berlin, Heidelberg, Germany, November 2013.

[PTC+12] Siani Pearson, Vasilis 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 *CloudCom*, pages 629–632. IEEE, 2012.

[RC02] Mary Beth Rosson and John M. Carroll. Scenario-based design. In Julie A. Jacko and Andrew Sears, editors, *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications*, chapter 53, pages 1032–1050. Lawrence Erlbaum Associates, 2002.

[SN93] Douglas Schuler and Aki Namioka, editors. *Participatory Design: Principles and Practices*. L. Erlbaum Associates Inc., Hillsdale, NJ, USA, 1993.

[SPSB10] Carolyn Salimun, Helen C Purchase, David R Simmons, and Stephen Brewster. The effect of aesthetically pleasing composition on visual search performance. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries*, pages 422–431. ACM, 2010.

[TKI00] Noam Tractinsky, AS Katz, and Dror Ikar. What is beautiful is usable. *Interacting with computers*, 13(2):127–145, 2000.

[TRH+12] Alexandre N Tuch, Sandra P Roth, Kasper Hornbæk, Klaus Opwis, and Javier A Bargas-Avila. Is beautiful really usable? toward understanding the relation between usability, aesthetics, and affect in hci. *Computers in Human Behavior*, 28(5):1596–1607, 2012.

[Wol13] Patrick J Wolfe. Making sense of big data. *Proceedings of the National Academy of Sciences*, 110(45):18031–18032, 2013.

[ZPK+13] Angeliki Zavou, Vasilis Pappas, Vasileios P. Kemerlis, Michalis Polychronakis, Georgios Portokalidis, and AngelosD. Keromytis. Cloudopsy: An autopsy of data flows in the cloud. In Louis Marinos and Ioannis Askoxylakis, editors, *Human Aspects of Information Security, Privacy, and Trust*, volume 8030 of *Lecture Notes in Computer Science*, chapter Part IV, pages 366–375. Springer Berlin Heidelberg, Las Vegas, NV, USA, July 2013.

A. Task analyses

A.1. Accountability Lab

A. Write policy

User goal: The user wants to create a machine-readable accountability policy.

Desired outcome: An AAL policy is created..

Plan: Do 1; 2; 3 (optional); 4 (repeatable)

1. Visually declare system resources

   Plan: Do 1.1 (repeatable); 1.2 (repeatable); 1.3 (repeatable)

   1.1. Declare agents

   1.2. Declare services

   1.3. Declare data

2. Visually define obligations for resources
3. View/modify AAL code
4. Click to check consistency

   Plan: Do 4.1 (if relevant); 4.2

   4.1. Review errors

   4.2. Select error for suggested fix

B. Check compliances

User goal: The user wants to check compliance between two policies.

Desired outcome: An automated check reveals compliance issues.

Plan: Do 1; 2; 3

1. Open an existing policy
2. Click to initiate compliance check

   Plan: Do 2.1; 2.2 (optional)

   2.1. Select a policy for comparison

   2.2. Get warning for any consistency errors in second file

3. Review compliance results

A.2. Audit Agent System

A. Perform audit

User goal: The user wants to perform an audit of a cloud service. This may also be an internal audit, where the cloud auditor is supplied the cloud provider itself.

Desired outcome: An audit is performed and the results are made accessible for the cloud provider and/or its customers.

Plan: Do 1; 2 (optional); 3; 4 (optional, repeatable); 5 (optional); 6; 7

1. Specify audit scope

   Plan: Do 1.1; 1.2

   1.1. Specify service

   1.2. Specify agents
2. Generate audit tasks from existing policy

   Plan: Do 2.1; 2.2

   2.1. Click to start with audit policy generation

   2.2. Upload A-PPL policy file(s)
3. Add audit tasks to be performed

   Plan: Do 3.1; 3.2

   3.1. Specify task

   3.2. Set compliance thresholds
4. Modify audit tasks

   Plan: Do 3.1; 3.2

   4.1. Modify task attributes

   4.2. Modify compliance thresholds
5. Delete audit task(s)
6. Review list of audit tasks
7. Approve audit policy

B. Access audit results

User goal: The user wants to access the results of an audit.

Desired outcome: The user is shown evidences that the data have been processed accordingly to policies, and any discrepancies.

Plan: Do 1

1. User login for dashboard?
2. Review results

   Plan: Do 2.1; 2.2

   2.1. Click on task result

   2.2. Review evidences/discrepancies

A.3. Cloud Offering Advisory Tool

A. Specify usage context for session

User goal: The user wants to experience a tailored service when using COAT.

Desired outcome: The terminology and layout of the tool is adapted to the user's knowledge of cloud technology.

Plan: Do 1; 2 (repeatable with several possible paths); 3 (optional)

1. Choose if you are a business or individual

   Plan: Do 1.1; 1.2 OR 1.3; 1.4

   1.1. Click business

   1.2. Choose type of cloud service

   Plan: Do one (or more?) of 1.2.1; 1.2.2; 1.2.3

   1.2.1. Click storage service

   1.2.2. Click processing service

   1.2.3. Click database service

   1.3. Click individual

   1.4. Choose type of cloud service

   Plan: Do one (or more?) of 1.4.1; 1.4.2

   1.4.1. Click general files service

   1.4.2. Click photos backup service

2. Perform main scenario (B or C, etc.)
3. Change usage context

B. Find service offers based on accountability requirements

User goal: The user wants to list service offers that meet a set of specific requirements.

Desired outcome: The user is provided with a set of options that allows him/her to specify requirements.

Plan: Do 0 (if not done before); 1; 2 (optional), 3 (repeatable); 4; 5;

0. *Specify usage context for session (A)*
1. Click to choose between a number of different requirements
2. Click to let the tool suggest a set of suitable requirements

   2.1. Adjust ”levels” of needs (on high level, for example ”high/medium/basic” security))

   2.1.1. Review definition of what high/medium/basic levels mean

3. Modify the requirements

4. Search for service offers that fulfil the requirements
5. *View accountability of service offers (C)*

C. View accountability properties of service offer(s)

User goal: The user wants to list service offers in order to inspect the accountability properties for one or more of these.

Desired outcome: COAT informs the user about the accountability properties of one or more services, and allows the user to compare them each other.

Plan: Do 0 (if not done before); 1 (optional); 2; 3; 4 (optional, repeatable); 5 (optional, repeatable); 6 (requires 5)

0. *Specify usage context for session (A)*
1. *Find service offers based on accountability requirements (B)*
2. View the list of service offers

   Plan: Do 2.1 (optional, repeatable)

   2.1. Adjust sorting criteria

   Plan: Do 2.1.1 and/or 2.1.2 (optional, repeatable)

   2.1.1. Select the sorting criteria

   2.1.2. Choose option/range for criteria (if available)
3. View the accountability properties of a service offer

   Plan: Do 3.1 (repeatable starting from 2); 3.2

   3.1. Click to view the details of a service offer

   3.2. Go back to the search result
4. Learn more about accountability properties

   Plan: Do 4.1; 4.2 (optional)

   4.1. Click the help-icon next to any property

   4.2. Click on a link to be redirected to external sources (if available)

   4.3. Review threats
5. Add service offer for comparison (”shopping cart”)
6. Compare selected service offers

   Plan: Do 6.1 (repeatable, optional); 6.2 (repeatable, optional); 6.3 (repeatable, optional)

   6.1. Add accountability properties for comparison matrix

   6.2. Remove accountability properties for comparison matrix

   6.3. Remove service offer from comparison

A.4. Data Subject Access Request Tool

A. Produce or submit a data access request

User goal: The user wants to submit a request to the cloud service provider for getting access to her data held by the provider.

Desired outcome: The user successfully submits a request, and eventually gets a copy of the data concerning her which is stored at the provider.

Plan: Do 1

1. The user locates a cloud service from where she wants to access her data

   Plan: Do 1.1 OR 1.2

   1.1. Uses standard controls to search or filter to a catalogue of service providers (data controllers) that hold the user's data

   1.2. Selects (through the Data Track tool) a service provider that hold the user's data

2. Select the type of request

   Plan: Do 2.1 OR 2.2

   2.1. Request data sets / data attributes (request all by default)

   2.1.1. Select the type(s) of data to request access to (explicit, implicit, inferred)

   2.1.2. Filter the category(ies) of data to request access to

   2.1.3. Select the (group of) data attributes to request access to

   2.2. Request motivation for decisions

   2.2.1. Select case from list of decisions (e.g., denied credit at a bank, or status of performance at work)

3. Continue to confirm request

4. Submit request

   Plan: Do 4.1 OR 4.2 OR 4.3

   4.1. Print offline request (service provider's address and all other necessary information filled in automatically in a printable paper)

   4.2. 4.2. Click to send request as email (service providers email and all other necessary information filled in automatically)

   4.3. Click ‘Submit’ to send request electronically

5. Obtain a receipt of the submission

6. (Get personal data)

A.5. Data Track

No task analysis

A.6. Data Transfer Monitoring Tool

No task analysis

A.7. Data Protection Impact Assessment Tool

A. Provide information and context about personal data processing

User goal: The user wants to provide information about the personal data that an organisation wants to process in a cloud.

Desired outcome: The tool has access to all information that is necessary to do a data protection impact assessment.

Plan: Do 1; 2 (optional)

1. The user inputs information about the data that will be processed

   Plan: Do 1.1; 1.2 (if requested by 1.1); 1.3 (if requested by 1.2); 1.4(if requested by 1.3)

   1.1. The user inputs general information

   1.2. The user input contextual information

   1.3. The user inputs information about the data and domain specific information

   1.4. The user inputs additional specific information

2. The user specifies a company policy

   Plan: Do 2.1 OR 2.2

   2.1. The user configures the tools settings to reflect the company policy

   2.2. The user uploads a file that contains the (machine-readable?) company policy

B. Generate DPIA report

User goal: The user wants to do a privacy impact assessment of the personal data processing

Desired outcome: The tool provides the user with a DPIA report, including a recommendation of whether to proceed with the outsourcing of personal data processing in a cloud

Plan: Do 0 (if not done before); 1 (optional, repeatable); 2; 3; 4;

0. *Provide information and context (A)*
1. The user specifies what service that will be used

   Plan: Do 1.1 OR 1.2

   1.1. The user chooses a service from a list of possible services

   1.2. The user creates a new service with input

   1.2.1. The user specifies certifications for the service

1.2.2. The user loads the ToS for the service

2. Generate risk assessment report

   Plan: Do 2.1 (optional); 2.2

   2.1. The user chooses to include/exclude reputation data in the assessment

   2.2. Click ”Get report”

3. Review DPIA report

   Plan: Do 3.1; 3.2 (optional)

   3.1. Check final result (proceed/seek assistance/don’t proceed)

   3.1.1. Click to read reasons for advice

   3.2. Review risks and threats

   3.2.1. Click risk/threat to learn more

   3.2.2. Click to get suggested mitigations

A.8. Incident Response Tool

A. User defines incident notification preferences

User goal: The user sets her preferences in the frequency and relevance of the notifications that she will receive (at the moment, users can just define a threshold level of the severity of the incidents defined by the plug-in for the assessment of privacy violations).

Desired outcome: User will receive only those notifications that are relevant to her.

Plan: Do 1 (if needed) ELSE 2;

1. Login

   1.1. Access tool by entering password

2. Click on the profile icon to open the preferences panel

3. Configure alerts (Adjust notification preferences)

   3.1. Select level of incident severity to be notified about

   3.2. Select type of incidents to be notified about

   3.3. Select frequency (how often) for notifications

4. Save changes

B. Receive a notification

User goal: The user is notified when an incident regarding her data in the cloud has occurred.

Desired outcome: The user is aware of an incident and is given the possibility to take action when appropriate.

Plan: Do 1

1. Get a notification (via mail, via a phones push service, via a dashboard, or other)
   - 1.1. 1.1. Click on the notification overview
   - 1.2. 1.2. Select one incident
2. See more details of one particular incident

   Plan: Do 2.1 OR/AND 2.2 OR/AND 2.3

   - 2.1. Check details about the incident
     - 2.1.1. Check the type personal data affected
     - 2.1.2. Check the service responsible
     - 2.1.3. Check contact details of service
     - 2.1.4. Check other organizations involved
   - 2.2. Select the type of advice to obtain
     - 2.2.1. Click to legal advice
     - 2.2.2. Click to get practical advice
   - 2.3. Take action (Remediation and Redress Tool)
     - 2.3.1. Click to contact cloud service provider
3. Interactively manipulate parameters of the incident to see other interesting facts (e.g. total incidents reported by same provider, number of incidents in general by month or category, etc.)

A.9. Remediation and Redress Tool

A. Produce remediation/redress request

User goal: The user wants to take action when concerned about an incident regarding their data.

Desired outcome: The user has succeeded in submitting a request for remediation/redress.

Plan: Do 1 OR 2; 3;

1. The user click how he would prefer to be helped
   - 1.1. Seek direct remediation with Cloud Service Provider
   - 1.2. Choose to get general, legal, practical advice
   - 1.3. Contact an authority
2. Describe the user’s concern (point **B**)
3. Review suggested advice or available actions or information from the tool

   Plan: Do 3.1; 3.2; 3.3 OR 3.4

   - 3.1. Confirm proposed automatic request for remediation/redress

3.2. Click to generate a written request

Plan: Do 3.2.1; 3.2.2

3.2.1. Input recipient(s)

Plan: Do 3.2.1.1

3.2.1.1. Select from a list of suggestions

3.2.1.2. Add custom based on knowledge about the service

- Get help to find out who are responsible

3.2.2. Input your own contact information

3.3. Download the generated written document

3.3.1. Print the document

3.3.2. Sign the document

3.3.3. Send the document

3.4. Send the request electronically

3.4.1. Verify your identity / eID (?)

B. Describe the user's concerns

User goal: The user wants to take action when concerned about an incident regarding their data.

Desired outcome: The user has succeeded in submitting a request for remediation/redress.

Plan: Do 1 OR 2; 3 OR 4;

1. Select the service in question

1.1. Click ”I have been affected!” by a known major incident with this provider

1.2. Click to describe a custom concern for this CSP

2. Specify the service in question **Plan:** Do 2.1; 2.2; 2.3

2.1. Enter service provider info

2.2. Enter link to machine-readable privacy policy

2.3. Answer questions about service policy in human language

3. Describe the incident **Plan:** Do 3.1 (optional, if available)

3.1. Select incident category: Service, privacy, security

3.2. Select specific incident type

3.3. Describe the data involved

3.3.1. Data type/sensitivity/origin

3.4. Specify time

3.5. Input additional information in free text

4. Click to complete survey