CLOUD ACCOUNTABILITY PROJECT

D:D-7.3: Evaluation report

Deliverable Number	D47.3
Work Package	WP 47
Version	1.0
Deliverable Lead Organisation	ATC
Dissemination Level	PU
Contractual Date of Delivery (release)	29/02/2016
Date of Delivery	31/03/2016

Editor

Vasilis Tountopoulos (ATC)

Contributors

Giorgos Giotis (ATC), Michela D' Errico (HPE), Siani Pearson (HPE), Rehab Alnemr (HPE), Tobias Pulls (KaU), Anderson Santana de Oliveira (SAP)

Reviewers

Carmen Fernandez-Gago (UMA)

Executive Summary

This deliverable is the final document of WP47, which aims to depict the feedback received from the different stakeholders involved in the evaluation of the project development activities and, especially, on the delivery of the A4Cloud tools. More specifically, the activities described here ran in parallel to the project dissemination activities and aimed to engage actual end users from the target communities in order to provide their feedback on how the project presents the implementation of the accountability framework.

The evaluation ran in various sessions organised in the context of a number of dissemination events. It has been performed in two iterations, namely the intermediate and the final evaluation phases. For each of them, the evaluation teams had the chance to provide their assessment as potential adopters of the A4Cloud tools through the demonstration of the first and the final project use case prototype, respectively.

Subsequently, this document report on the results of these two evaluation phases, trying to structure the feedback collected in three dimensions: i) the perception of the evaluation teams on the use of the A4Cloud prototype to implement the wearables use case, ii) the level of acceptance provided by the evaluation teams on the scope and the coverage of the A4Cloud tools to address accountability requirements, and iii) the assessment of the A4Cloud impact in the cloud security market and the practices currently adopted by the various stakeholders' groups to address privacy and data protection requirements.

Overall, the feedback received from the involved evaluators was good enough to draw the plan for the sustainability of the tools beyond the end of the project. Of particular importance is the fact that, although the participants in the evaluation process understand that there are a lot of challenges to be addressed prior to the commercialisation of the A4Cloud results, they do see benefits for the cloud security market from the introduction of the tools in order to run a cloud business.

Table of Contents

Executive Summary 2
1 Introduction 4
1.1 The Scope of the evaluation process 4
1.2 Structure of the Deliverable 4
1.3 Glossary of Acronyms / Abbreviations 4
2 Intermediate Evaluation 6
2.1 Demonstration at the CSP EU Forum 2015 6
2.1.1 Objectives of the evaluation 6
2.1.2 How we set up the demo 6
2.1.3 Profile of the audience 9
2.1.4 Presentation of results 9
2.2 IFIP Summer School 2015 10
2.2.1 Objectives of the evaluation 10
2.2.2 How we set up the demo 10
2.2.3 Profile of the audience 10
2.2.4 Presentation of results 10
3 Final Evaluation 13
3.1 Final Advisory Board Meeting 13
3.1.1 Objectives of the evaluation 13
3.1.2 How we set up the demo 13
3.1.3 Profile of the audience 17
3.1.4 Presentation of results 17
3.2 Workshop and Demo at CSA Congress 2015 18
3.2.1 Objectives of the evaluation 18
3.2.2 How we set up the demo 18
3.2.3 Profile of the audience 21
3.2.4 Presentation of results 21
3.3 CloudScape 2016 22
3.3.1 Objectives of the evaluation 22
3.3.2 How we set up the demo 22
3.3.3 Profile of the audience 25
3.3.4 Presentation of results 25
4 Conclusions 30
5 References 31
6 Appendices 32
6.1 The evaluation questionnaire 32
7 List of Figures 36

1 Introduction

1.1 The Scope of the evaluation process

As part of the work performed in WP47, a task for evaluating the demonstration of the first and the final A4Cloud use case instantiation was defined. The scope of this task is to reinforce the project dissemination activities, reported in [3], and engage actual end users from the target communities in order to provide their feedback on how the project presents the implementation of the accountability framework. The scope of this deliverable is to present the feedback collected from the target stakeholders involved in the evaluation sessions (evaluation team), by using the evaluation process that was introduced in Deliverable D47.1 [1], and specifically to understand the following:

- The perception of the evaluation team on the use of the A4Cloud prototype for the implementation of the wearables use case. The evaluation result should reflect the level of awareness of the evaluation team on the accountability problems of the actors involved in the wearable use case and how demonstration allows them realise the involvement of the A4Cloud offering in addressing these problems.
- The level of acceptance provided by the evaluation team on the scope and the coverage of the A4Cloud tools to address accountability requirements. The evaluation result should reflect the confidence of the evaluation team to execute the tasks defined in the evaluation process and whether the performed actions are aligned with the current problems of the cloud security market.
- The assessment of the A4Cloud impact in the cloud security market and the practices currently adopted by the various stakeholders' groups to address privacy and data protection requirements. The evaluation result should offer insight on the potentials of the A4Cloud work to raise benefits for the cloud actors and be sustainable in the future.

1.2 Structure of the Deliverable

This deliverable is structured as follows:

- Section 2 presents the results from the intermediate evaluation phase, in which we demonstrated the first A4Cloud use case prototype to the communities of target stakeholders. Specifically, the evaluation took place as part of the project activities in the CSP EU Forum 2015 and the IFIP Summer School 2015.
- Section 3 presents the results from the final evaluation phase, in which we demonstrated the final A4Cloud use case prototype to the communities of target stakeholders. Specifically, the evaluation took place as part of the project activities in the final project advisory board meeting, the CSA EMEA Congress 2015 and the CloudScape 2016 event.
- Finally, Section 4 concludes this document.

1.3 Glossary of Acronyms / Abbreviations

Acronym / Abbreviation	Description
AAS	Audit Agent System
AccLab	Accountability Lab
A-PPLE	Accountable Primelife Policy Engine
CARA	Cloud Accountability Reference Architecture
COAT	Cloud Offerings Advisory Tool
CSP	Cloud Service Provider
DPIAT	Data Protection Impact Assessment Tool
DPPT	Data Protection Policies Tool

Acronym / Abbreviation	Description
DT	Data Track
DTMT	Data Transfer Monitoring Tool
IMT	Incident Management Tool
PLA	Privacy Level Agreement
RRT	Remediation and Redress Tool
TL	Transparency Log
UI	User Interface

2 Intermediate Evaluation

This section presents the results of the demonstration activities for the evaluation of the first A4Cloud use case instantiated prototype. This period spans from April 2015 up to July 2015.

2.1 Demonstration at the CSP EU Forum 2015

The first A4Cloud use case prototype was demonstrated in the context of the CSP EU Forum 2015[1]. The event was organised in Brussels, on April 28th and 29th, 2015.

2.1.1 Objectives of the evaluation

Through our participation in the CSP EU Forum 2015, we aimed to demonstrate the capability of the A4Cloud tools to support the definition and enforcement of accountability policies for the wearables use case. More specifically, the evaluation process for this event should concentrate on the demonstration of:

- Preventive accountability mechanisms, through the specification and enforcement of accountability policies in the cloud environment.
- Detective accountability mechanisms, through the tool support for the detection of incidents, with respect to data access, data retention and data transfers.

2.1.2 How we set up the demo

In order to evaluate A4Cloud in this session, we set up the demonstration that provided the perspective of the different cloud actors, namely, the Wearable Co customer, the Wearable Co and Kardio-Mon.

The demonstration was held through two different activities. They are explained below.

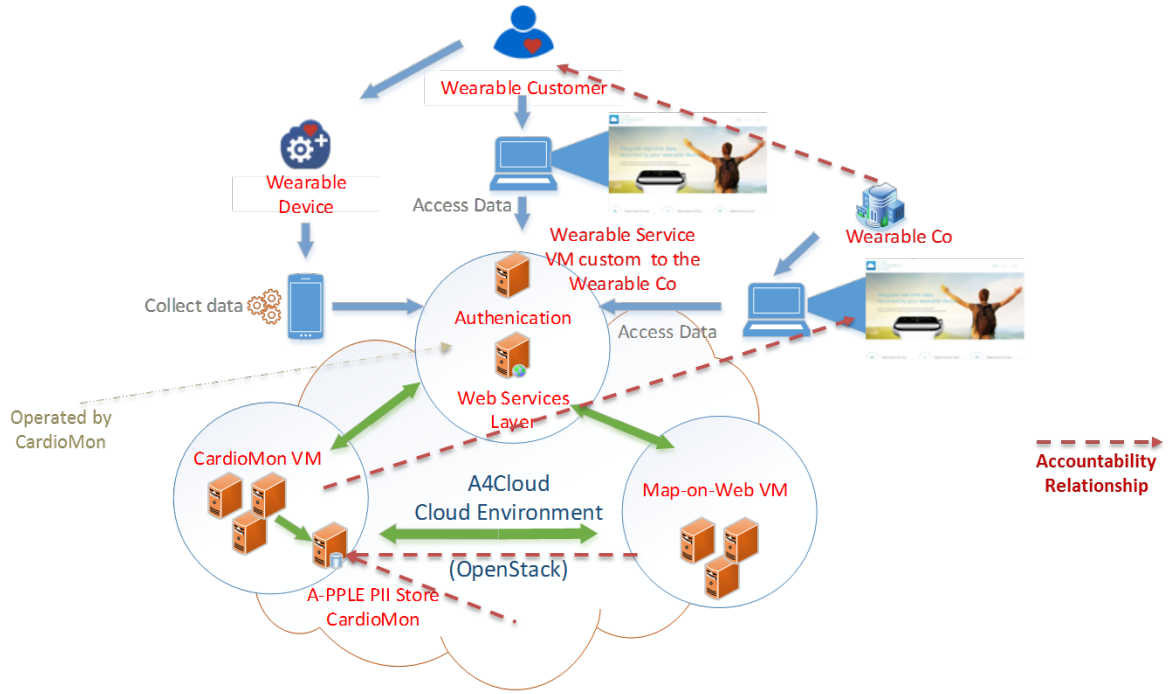

Figure 1: The execution environment used for the demonstration of the A4Cloud project at the CSP EU Forum 2015.

Holding an exhibition booth

[1] http://www.cspforum.eu/2015.

We had a booth at the exhibition area of the CSP EU Forum 2015[2], in which we run the first A4Cloud use case prototype, as it is depicted in Figure 1.

Thus, for this demonstration, the evaluation assets were the policy definition and enforcement tools and the incident detection tools for unauthorised data transfers. More specifically:

- We presented the manual compilation of high level policy rules for data access, data retention and data transfer situations into machine readable policies in A-PPL format. The policy specification engaged the business actors involved in the wearables use case and the personal data collected from the Wearable Co customers.
- We presented the enforcement of the policies when operating the application level functionalities of the wearable cloud service. Specifically, we emphasised on the enforcement of the data access and data retention rules through A-PPLE. The scenario involved the Wearable Co employee browsing the list of registered wearable customers and requesting to access the complete record of the personal information of a customer, which is not allowed by the specified policy.
- We presented the detection of incidents on unauthorised data transfers. The scenario involved the Wearable Co having agreed with Kardio-Mon that only data centres in EEA are used for storing the personal data of the customers. A sudden hardware failure in DataSpacer results in the Kardio-Mon storage area being moved to a third country location (i.e. USA).

The demonstration was performed through a laptop machine accessing the execution environment. Two A4Cloud representatives recruited the booth (see Figure 2).

Figure 2: The booth for demonstrating A4Cloud at the CSP EU Forum 2015.

Organising a workshop

[2] https://www.cspforum.eu/2015/Exhibitions.

A4Cloud collaborated with the CoCoCloud[3] project in the organisation of Track 12 of the main conference programme. The objective of this workshop was about the implementation of privacy policies in the cloud. A power point presentation was given, detailing the approach of A4Cloud for the specification and enforcement of privacy policies.

The panel of the workshop was as follows (see Figure 3):

- Chair: Nick Wainwright HP Labs
- "EU DP legal framework review and its impact on cloud architectures", Demosthenes Ikonomou,Head of Information Security & Data Protection Unit, ENISA
- "Specification and Enforcement of Privacy Policies", Michela D'Errico , A4Cloud project, HP, UK
- Claudio Caimi, Coco Cloud project, HP Italy

Figure 3: Screenshots from the A4Cloud-CocoCloud workshop at the CSP EU Forum 2015.

[3] www.coco-cloud.eu/

2.1.3 Profile of the audience

During this demonstration event, A4Cloud work was presented to around 80 researchers in the field of security and privacy, coming from both the industry and academia, and the EC services as well. Most of them attended the event as representatives of EC-funded research projects.

Figure 4: Screenshot from the exhibition hall of the CSP EU Forum 2015.

Figure 5: Screenshot from the audience attending the A4Cloud presentation on implementing privacy policies in the context of the CSP EU Forum 2015.

2.1.4 Presentation of results

Overall, both the attendees of the workshop and the visitors of the A4Cloud booth at the exhibition area were satisfied with the results presented to them.

During the workshop, the attendees expressed an interest in the policy definition and implementation tools of the project and they asked for the difference between the tools being implemented in A4Cloud and the CocoCloud project. They highlighted the need for tool support in translating policy rules into machine readable formats that can be enforced automatically.

In the booth, the interest was mainly on the use of the tools to compile and enforce the accountability policies and how these policies can cover the data protection and privacy requirements in a real cloud problem. All the visitors realised that the scenarios presented to them were interesting from an accountability point of view. We did understand that the tools are in a research prototype form and they were curious on how the tools can be applied in real business cases. They realised the need for the accountability framework and they expressed their perception that the project results can have an impact in the future landscape of the cloud environment.

Overall, an important point from the evaluation of A4Cloud in the CSP EU Forum 2015 was the fact that we validated our initial thought that the A4Cloud tools should provide a graphical user friendly interface for the policy experts to be able to define the accountability policies in an easy way and the tool to translate it to machine readable formats so that the policies are enforced in the cloud runtime environment.

2.2 IFIP Summer School 2015

The IFIP Summer School 2015[4] took place in Edinburgh, UK, from the 16th to 21st of August, 2015. The IFIP Summer Schools take a holistic approach to society and technology and support interdisciplinary exchange through keynote and plenary lectures, tutorials, workshops, and research paper presentations. The IFIP Summer Schools welcome interdisciplinary contributions. To this end, this event was considered challenging in order to demonstrate the first A4Cloud prototype.

2.2.1 Objectives of the evaluation

At this IFIP Summer School, A4Cloud held a workshop to discuss the problem of accountability in the cloud and how the toolkit being developed within the A4Cloud project could help enhancing accountability. Specifically the objective of the workshop were the following:

- To introduce the project objectives and what tools have been developed for addressing the problem of accountability;
- To increase awareness of what it is possible to achieve from the accountability point of view;
- To obtain feedback from the attendees that will help us to enhance the tools.

The following tools were demonstrated: COAT, DPIAT, DT, DPPT and A-PPLE.

2.2.2 How we set up the demo

At the beginning of the session, the workshop organisers gave a general overview of the A4Cloud project to the audience. Then, the group of participants was split into four different subgroups of four or five people each. Each of these subgroups approached specific booths set up to show demos of the tools (there was a shared booth for DPIAT and COAT). At each booth, a member of A4Cloud was in charge of presenting and demoing a specific tool. Each demo session was interactive and participants asked questions and gave feedback.

2.2.3 Profile of the audience

The summer school was attended by around 50 people from very multidisciplinary fields like Computer Science, Social Sciences or Law. In the A4Cloud workshop, we attracted PhD students, legal experts, and Computer Science experts, who had the chance to join the subgroups and follow the demonstrations of each tool.

2.2.4 Presentation of results

At the time of the workshop, the tool prototypes were in a state mature enough to be demonstrated. Therefore, the attendees could have a very good idea of how they could be used by end users, cloud customers or cloud providers. The participants provided their feedback from this workshop, which has

[4] http://www.ifip-summerschool.org/previous-schools/.

been taken into account, and, as far as possible based on the development stage for the tool, addressed within the improved versions of the tools involved in this evaluation. More specifically, we highlight the following points for the tools involved in the evaluation:

- For the Data Track tool: the evaluation team raised some concerns on how data is stored or visualised, and whether the information fed into the tool for visualisation would be valid, as it is coming from a cloud provider. They also expressed their concerns about the resolution of conflicts or the evaluation of this tool as well as about monitoring aspects. These aspects led to the question of how this tool improves the accountability of the service provider. In general, attendees viewed the tool as being interesting for allowing end users auditing their cloud providers. They also pointed out that security aspects should be considered in order to move forward. For the sake of usability, it was mentioned that it would be interesting if the DT tool worked in a mobile environment.
- For the Data Protection Impact Assessment Tool: the evaluation team raised questions about the selection of cloud providers, how risk is considered and how the rating and the evaluation are performed. More specifically:
    - Concerning the selection of the providers, the main question is whether the algorithm needs tweaking. It was suggested that it would be convenient for the user of the tool to be able to select more than one CSP at the beginning (perhaps, up to three?). Then, on the final output screen it would be a good idea to have the different options selected shown up in the second band of output. This way the user does not have to go through the whole questionnaire each time if they were not quite sure about which CSPs to use but had a good idea.
    - It would be nice to highlight the differences between CSPs when running a DPIAT. This functionality could indeed be added fairly easily to allow comparison of several providers at once, but there was a difference of opinion amongst the attendees as to whether this would be a good idea, or appropriate for typical contexts in which the tool might be used.
    - Attendees' concerns about risk were related to how it is presented for users to understand it. The distinction between the risks to data subjects (the core of a DPIA), and those related to a more classic organisational risk assessment (on the proposed service provider) should be clear. Also, the attendees suggested that the colour code and used signs for the DPIAT overall output, e.g. a high risk should show up as red, not green (this seemed due to a glitch with the system on the day). It was noted that risk mitigation is missing and also other factors that might be relevant for assessing risk, e.g. who owns the key?
    - There was a difference in opinion about how helpful an overall rating would be for the first section. Perhaps, the consensus was that it would be helpful indeed for decision making, but one would have to be very careful how that was done. It is important that there would be some explanation about what this overall rating would mean, and what the implications would be.
    - It was highly stressed by the more mature researchers and experts that it should be clear how the user should interpret the findings, and what it meant for them in terms of what they should do next, etc. It was advised to check whether or not the very high and extremely high, etc. of the second part were indeed the same bands (and associated meaning) as those used in the first part - it seemed that there might be a mismatch with different terms being used. Perhaps it needed to be clearer how DPIAT should be used in the context of an overall DPIA process, and how things like consultation of stakeholders fit in. We do have some information on this, but it still seems not so clear about what else must be done, and when and how often the DPIAT tool could be used.
    - An important issue is also time consuming for running the tools. It would be very interesting to run all the tools at once. The major concern that attendees had was that there was no justification of why the results were given, or explanation of how the results were obtained, or way of the user or a third party to check the verification of the process used to obtain these results. One aspect of dealing with this is that an explanation of how the results were obtained should be added within the tool in a way that it could be accessed by a user exactly, even if the particular chain of processing leading to that particular result might not be exposable in other words, to be able to click to see how it was done, and provide more evidence about that. Which results from the system can be relied on, and why?

  - There should be more explanation about how the risk was obtained, to what extent probability and impact are taken into account, etc., and whether that differs across the different sections of output. In what way is the output to be regarded as a proof for interpretation and used by the user, and in what way could it be provided as a proof for a data protection authority? The legal implications are different. What is the outcome of the result (single answer, guidelines, etc.)? What is it useful for?

- For the Cloud Offerings Advisory Tool: Some options in the answers given seem very odd, e.g. in the encryption options there should be a distinction made between data at rest and during transit, and also the types of weaker and stronger encryption should be brought out more accurately. We had already realised this and updated the questionnaire offline, although that was not yet reflected within the demo version. There were also issues relating to what we have been showing for some time in this same demo versus our proposed improvements that were not yet reflected within it, such as more sophisticated ordering of results, display of certification/seals, etc. Questions from the audience were related to the use of standards, in the sense of how everything related to the tool would be documented. Concerning legal regulations it was pointed out that different regulations depending on the countries should be taken into account.
- For the policy definition part: One of the first questions that arose from the audience was why the A-PPL language was chosen. If the reason is a question of scalability this seems to be a good reason. The way requirements are dealt with is also another of the questions: are all the requirements translated into the policy? And what is happening with the role undertaking the task to define the policies, which might not be a privacy officer, as this is the case for example of SMEs.

3 Final Evaluation

This section presents the results of the demonstration activities for the evaluation of the first A4Cloud use case instantiated prototype. This period spans from August 2015 up to March 2016.

3.1 Final Advisory Board Meeting

The final A4Cloud advisory board meeting was held in London UK, on October 5th and 6th, 2015. Although this event aimed to inform the members of the advisory board on the project evolution in Year 3, the event was also exploited to deliver an end-to-end demonstration of the accountability tools in the context of the wearables use case.

3.1.1 Objectives of the evaluation

Through the demonstration of A4Cloud in the advisory board meeting, the project aimed to understand how the multidisciplinary synthesis of the advisory group perceives the results of the final A4Cloud use case prototype, how the target community stakeholders can better realise the usefulness of the tools to support accountability and which are the potentials for the implementation of the cloud accountability reference architecture in the cloud security market.

3.1.2 How we set up the demo

The demonstration of the final A4Cloud use case prototype was split into five sub scenarios, each of which presented the perspective of the actors shown in Figure 6.

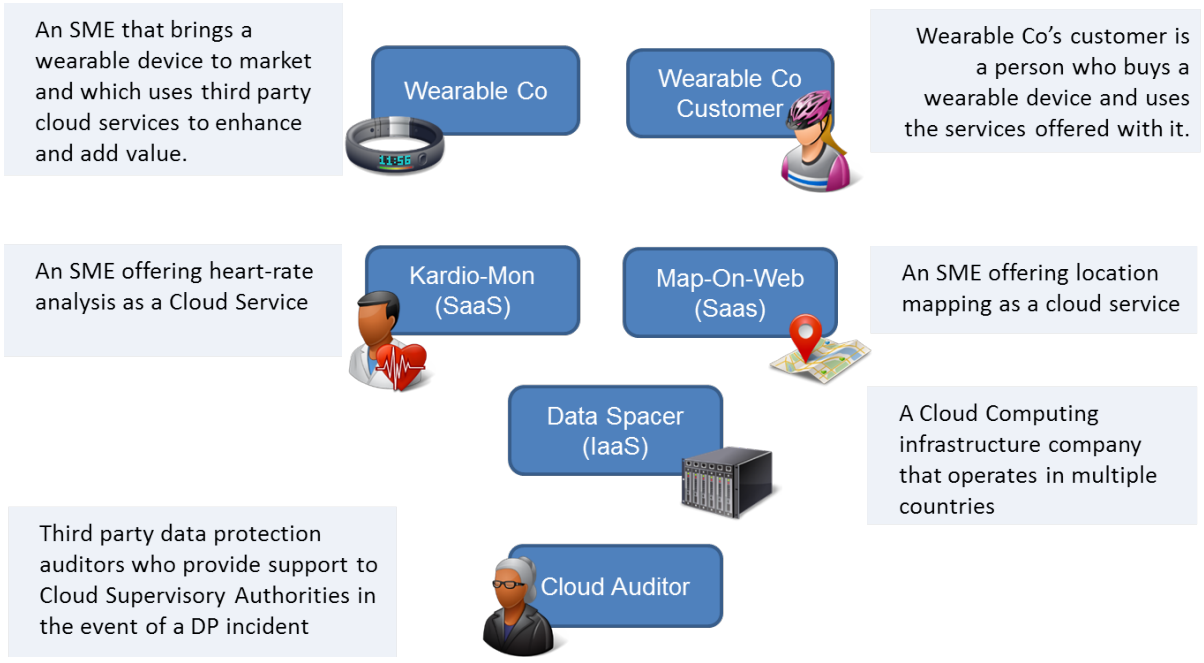

Figure 6: Demonstrating A4Cloud from the perspective of the business actors in the final Advisory Board meeting.

More specifically, due to the complexity of the demonstration process from an end-to-end approach, we decided to set boundaries in the presentation of the whole story from the development of the cloud service supply chain to the operational phase of the wearable service. Thus, we demonstrated the final prototype of the A4Cloud use case implementation from the perspective of the cloud actors and emphasised on the tool usage for the different phases of the wearables use case implementation. Through the following five scenarios, which are summarised in Figure 7 , we planned to touch the needs of each role in the provision of the wearable service and showcase the integration of the accountability tools with the business process operations of the wearables use case.

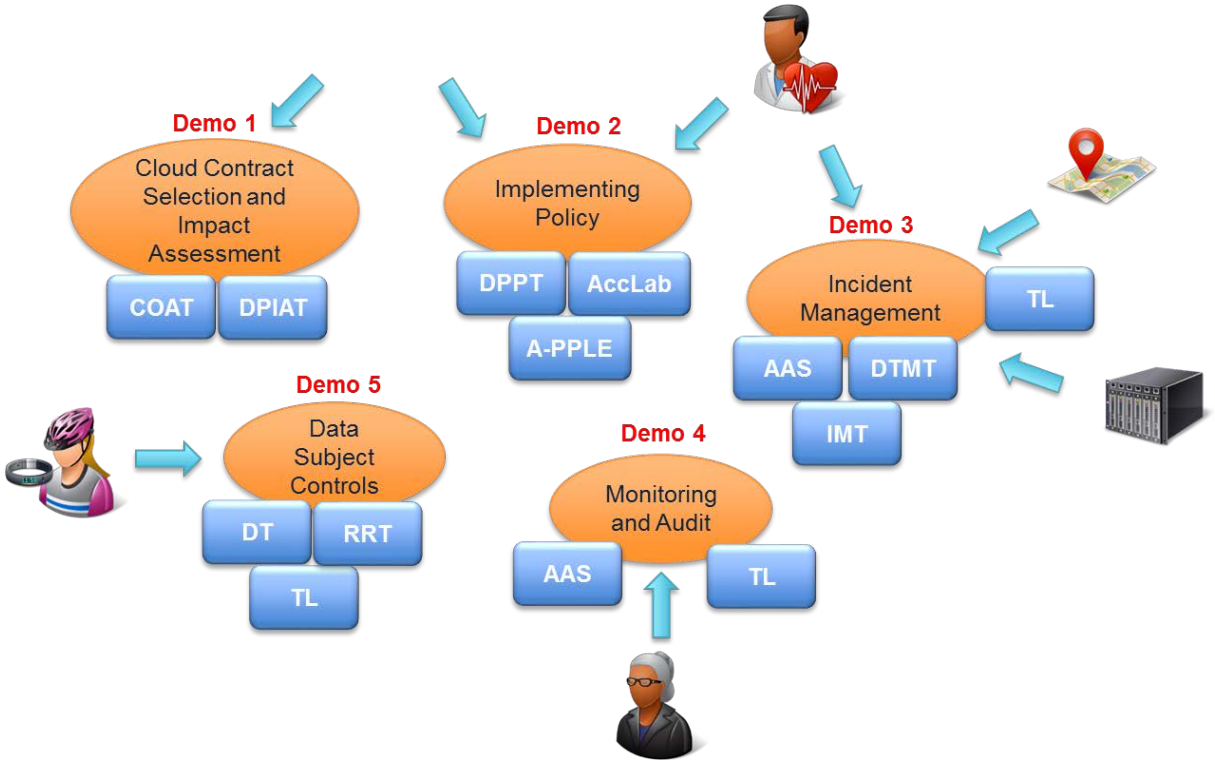

Figure 7: The demonstration scenarios of the final A4Cloud use case prototype.

The five scenarios we demonstrated in this event are:

- Selection of the cloud service supply chain (see Figure 8): This scenario presents the perspective of the Wearable Co as a cloud customer to demonstrate accountability in the policy definition and validation support service.
- Implementation of policies (see Figure 9): This scenario presents the perspective of Kardio-Mon to demonstrate accountability in the policy definition and validation support service and the policy management and enforcement service as well.
- Incident Management (see Figure 10): This scenario emphasizes on the perspective of the different actors in the cloud environment, namely Kardio-Mon, Map-on-Web and DataSpacer, to demonstrate their activities towards the collection of logs and the provision of evidence for the accountable execution of their processes.
- Monitoring and Audit (see Figure 11): This scenario presents the perspective of the Cloud Auditor and the Cloud Supervisory Authority to perform audits on the data handling procedures of the cloud providers.
- Data Subject Controls (see Figure 12): This scenario presents the perspective of the Wearable Co customer as the cloud subject in the wearables use case.

The details of the scenarios and how they are executed are presented in Deliverable D47.2 [2].

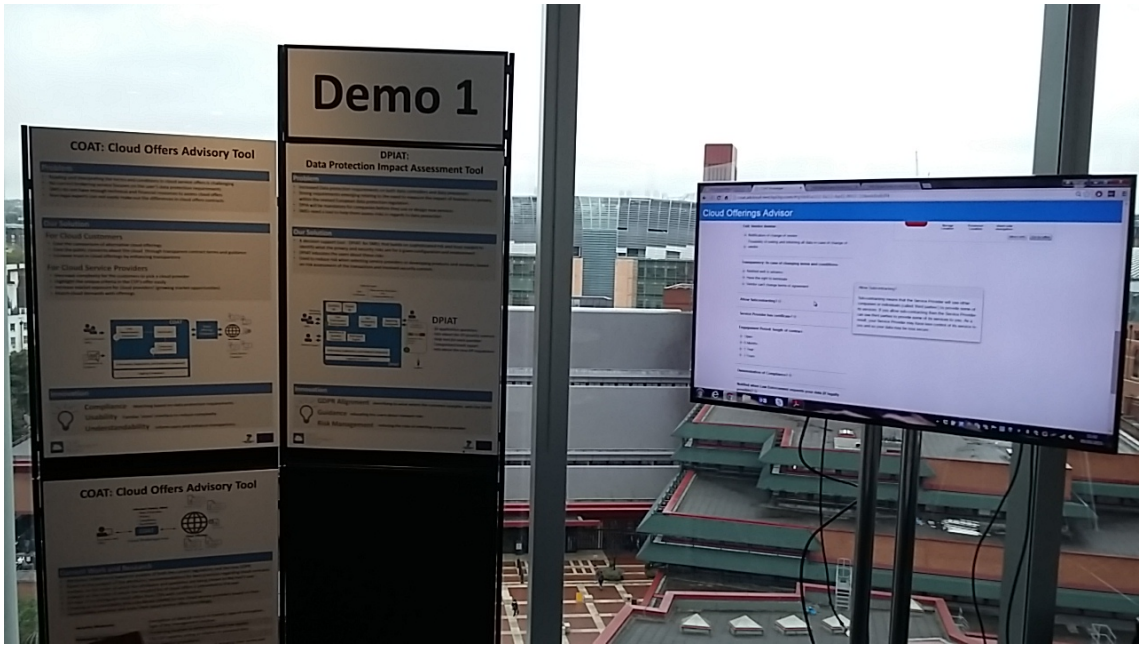

Figure 8: The setup of demonstration scenario 1 in the final advisory board meeting.

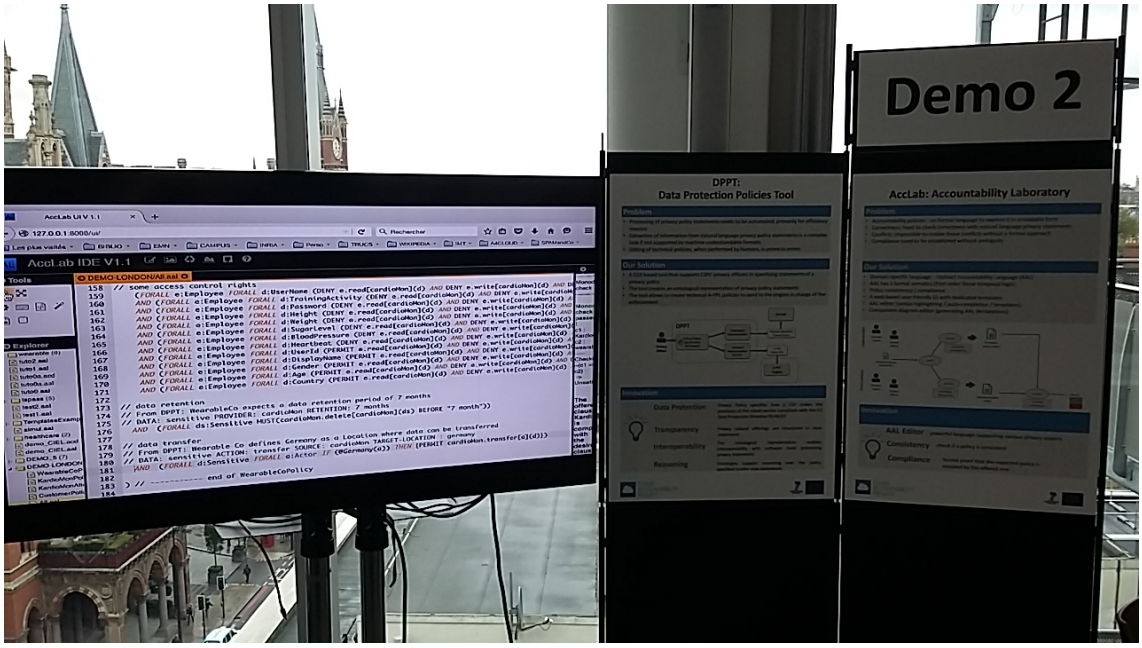

Figure 9: The setup of demonstration scenario 2 in the final advisory board meeting.

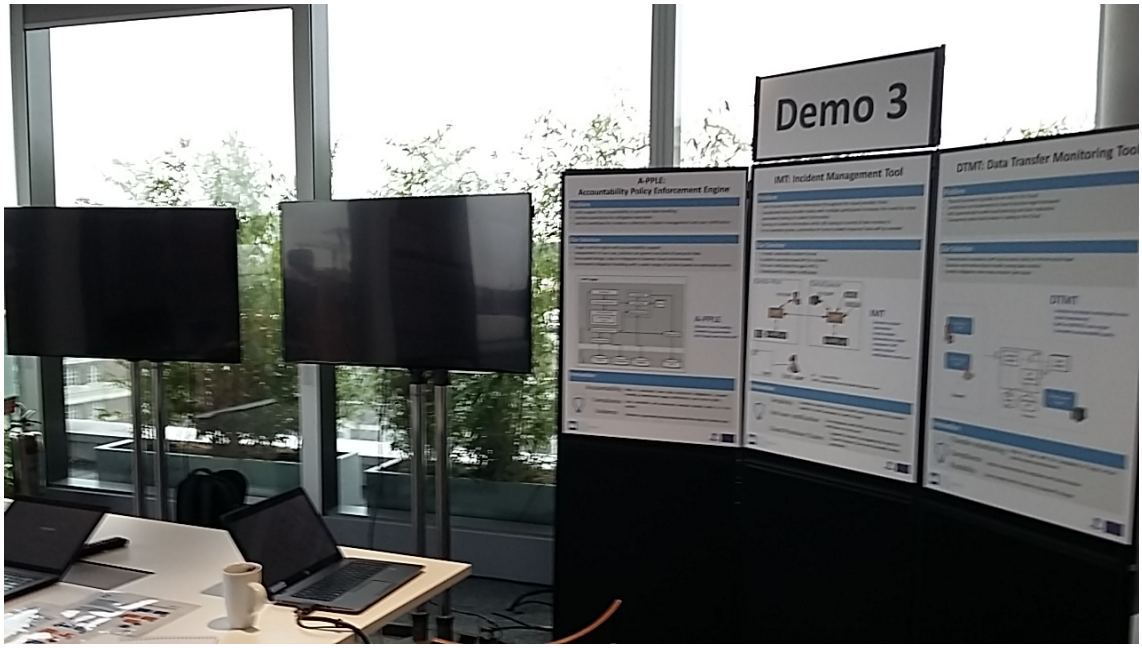

Figure 10: The setup of demonstration scenario 3 in the final advisory board meeting.

Figure 11: The setup of demonstration scenario 4 in the final advisory board meeting.

Figure 12: The setup of demonstration scenario 5 in the final advisory board meeting.

3.1.3 Profile of the audience

A multidisciplinary group of 18 people attended the evaluation session in the context of the final advisory board meeting, from the following groups (see a screenshot in Figure 13):

- The Business Community Group, representing the cloud service providers market, cloud brokers and carriers, as well as cloud customers
- The IT Technical Community, such as IT Managers, Security Experts, cloud service and application developers, as well as members of Standardisation Bodies.
- The Business Compliance Community Group, such as representatives from Data Protection Authorities and Compliance Managers.
- The Regulatory Community, representing Regulatory Experts and Policy Makers.
- The Research Community, representing cloud computing and IT security research teams, legal researchers on data protection and privacy, social scientists and academic economists.

Figure 13: Screenshot of the audience being engaged in the demonstration of the five scenarios in the final advisory board meeting.

3.1.4 Presentation of results

This evaluation event was a great opportunity to understand what the audience feels about A4Cloud. By allowing the groups of people to go through the five demonstration scenarios, we managed to get their valuable feedback putting them in the position of the various roles. Thus, here we presented the synthesised comments received from all the groups per scenario.

- Scenario 1: Use of COAT and DPIAT tools

In this scenario, the audience asked about the commitment of the cloud service providers to offer their capabilities in order to allow COAT and DPIAT functionalities, their incentives to provide a description of these capabilities in a way that this is not vague and how they would be laced in a process to maintain their capability offerings up-to-dated in the tools. An important aspect towards the impact of the tools has to do with the operational model and who is running these tools and whether the assessment offered is complete enough. Overall, the attendees felt that the demonstration of the way that the tools align with actual policies and follow standardised practices for this is a strong asset.

- Scenario 2: Use of DPPT and AccLab

As part of the evaluation for this scenario, the audience raised the issues of security for accessing the tools and the incentives for the adoption of such tools, both from the perspective of whether it is easy to use them and the wider acceptance of the background technologies. For example, the ontologies behind DPPT require the engagement of standardisation bodies to come up with a valid and widely acceptable definition, while the use of Privacy Level Agreement (PLA) templates is critical to demonstrate that privacy policies can work.

- Scenario 3: Use of A-PPLE, DTMT and IMT

In this scenario, the attendees expressed an interest in realising a semi- automated approach for the policy enforcement and incident management practices. They do understand the role of human interaction in this process, but they feel that the involvement of digital SLAs is required. The incident response must be aligned to data protection issues and should provide justification on the type of the notifications raised (i.e. legal, data breach, etc.).

- Scenario 4:Use of AAS

For the use of AAS as a monitoring and auditing tool, the audience emphasised the importance of collaboration between the target users. They raised some security and trust concerns about the use of the tool and the management of evidence and they were curious about the potentials for interfacing with existing monitoring systems that CSPs already use.

- Scenario 5: Use of DT and RRT

The data subject control tools were considered by the audience as useful as they advance the current capabilities of the cloud subjects in controlling their data. However, they thought that a lot of risks arise from the use of such tools on insecure end user devices, but they do see potentials by allowing these tools to be locally installed, instead of being provided as services. A major concern for the attendees was the willingness of cloud providers to cooperate with the tools by providing access to the collected information. This is especially crucial for big players in the cloud market. Nevertheless, the audience felt that these tools can empower individuals in exercising their rights as per the data protection directives and by allowing the tools to be part of the business models of the cloud providers would maximise the potentials for both the acceptance and the use of the tools.

3.2 Workshop and Demo at CSA Congress 2015

The final A4Cloud use case prototype was presented at the CSA Congress, which was held in Berlin, Germany on November 16th - 18th, 2015.

3.2.1 Objectives of the evaluation

The objective of this evaluation activity was to gather the opinion from the cloud market representatives on how A4Cloud addresses the problem of accountability for the cloud providers, either being SMEs or large industries, from the conceptualisation of the cloud business up to the management of incidents detected in the cloud environment.

3.2.2 How we set up the demo

The demonstration of final A4Cloud use case prototype in the context of CSA Congress 2015 was performed through the two following two activities.

Organising a workshop

A4Cloud actively participated in the organisation of the workshop on “Governance: Accountability-Compliance in the Cloud”, in the context of the CSA EMEA Congress by joining up efforts with other research initiatives. The workshop aimed to:

- Showcase the latest practices & tools developed through research in the area of Cloud Governance, and how they support the objectives of the Digital Single Market Communication Strategy
- Identify synergies between projects’ achievements and the CSA WGs’ outputs
- Validate results and identify possible go to market strategies for the tools and services developed.

Figure 14: Screenshot from the organisation of the workshop in the context of the CSA EMEA Congress 2015.

During this workshop, the project representatives were actively involved in the formulation and running of the following presentations (see Figure 14):

- Project objectives
- Market requirements based on the public and private sector
- Synergies between CSA activities and EU Funded projects
- Tool demos and best practices presentations

Also, a project representative participated in the open discussion panel to deliberate on the A4Cloud contributions to the Digital Single Market activities and the CSA research WG's.

Holding an exhibition booth

Apart from the workshop, during the main programme of the CSA EMEA Congress, A4Cloud held an exhibition booth, with the aim to demonstrate the final A4Cloud use case prototype and collect the audience feedback on their understanding about the project achievements and their perception on how these results can enter the cloud service security market.

Figure 15 presents the setup of the A4Cloud booth.

The demonstration emphasised on two parts, namely i) checking data protection requirements and ii) applying measures to showcase compliance with these requirements. In that respect, the first part focused on the use of the DPIAT tool (see Figure 16), while the second part demonstrated how a data transfer incident is detected and is populated to the cloud service supply change of the wearables use case (see Figure 17).

Figure 15: Screenshot from the A4Cloud booth at the CSA EMEA Congress 2015.

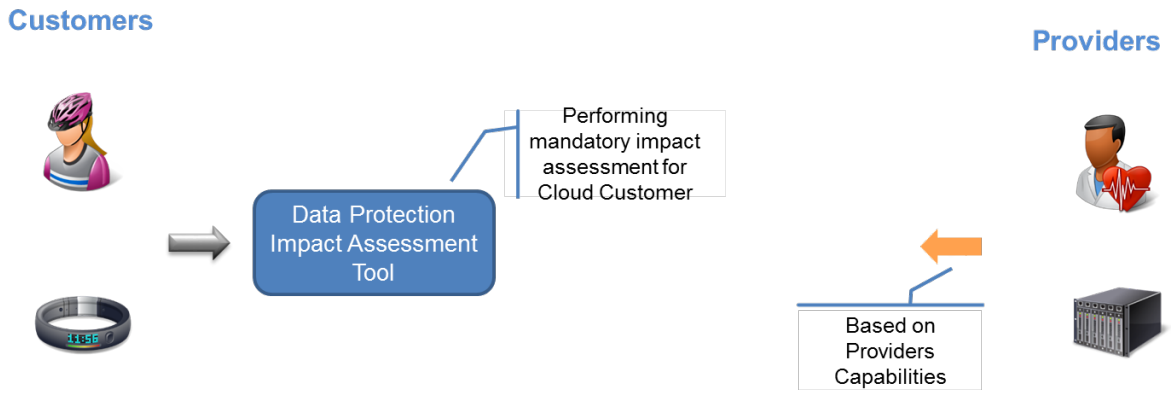

Figure 16: Evaluating the A4Cloud tools for checking data protection requirements at the CSA EMEA Congress 2015.

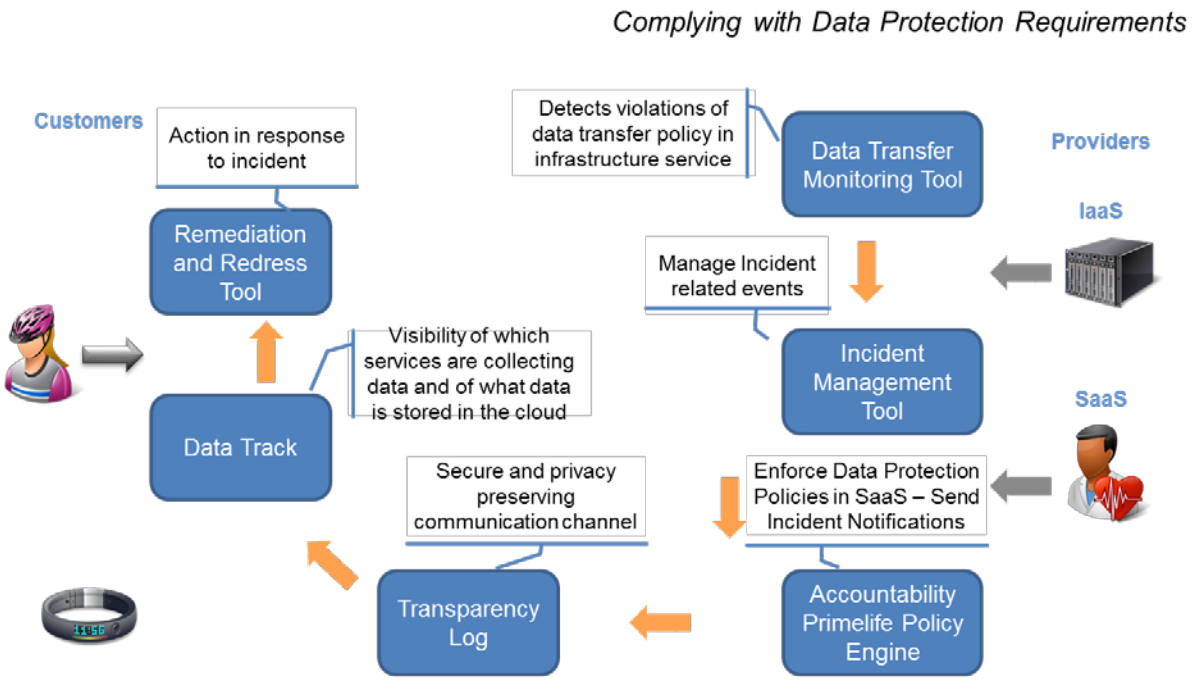

Figure 17: Evaluating the A4Cloud tools for showing compliance with data protection requirements at the CSA EMEA Congress 2015.

3.2.3 Profile of the audience

During this evaluation session, a mixture of cloud business and IT communities joined both the workshop and the exhibition booth (see Figure 18).

Figure 18: Screenshot from the exhibition hall of the CSA EMEA Congress 2015.

3.2.4 Presentation of results

During the evaluation both in the workshop and at the booth, the audience showed their interest in the tools and best practices produced by the project, although the felt that there is an expected overlap among the work conducted in A4Cloud and other EU research projects. They all raised their satisfaction about the progress of research in the accountability tools, but they highlighted that the most interesting

part starts when the market needs to adopt such solutions. A major concern lies on the applicability of the privacy level agreements beyond big cloud providers, who mainly offer SLAs in a “take it or leave it” mode.

A common feeling is that research managed to identify the needs of the cloud security market, but a lot of work is still in progress until the development activities achieve addressing these needs. Most important is the fact that data protection goes beyond privacy and currently the main emphasis is on privacy. In any case, the project results set a good basis to work for the future and, in order to do so, the project must develop good sustainability through early market adopters and volunteers to continue this work. Standardisation is also another avenue to raise impact to the society and the business market.

Looking more on the potential impact of this evaluation, the audience was sceptical about the balance between the cost for the implementation of accountability and the benefits for the cloud chain. They all agreed that there is a tradeoff to implement privacy, but enforcing accountability requires decisions on a political level, as well as developing accountability as a culture, across business organisations.

3.3 CloudScape 2016

The final evaluation activity of the A4Cloud use case prototype was performed in the context of the CloudScape 2016[5] event, which was held in Brussels, on March 8th and 9th, 2016.

3.3.1 Objectives of the evaluation

As happened with the previous evaluation events, the scope of this demonstration activity was to enlarge the community of A4Cloud followers and understand their perception and acceptance on the A4Cloud tools to demonstrate accountability.

3.3.2 How we set up the demo

As happened with the evaluation in the context of the CSA EMEA Congress 2015, the relevant activities for the demonstration of final A4Cloud use case prototype in the context of the CloudScape 2016 event were split into the following two parts.

Organising a workshop

The project organised the workshop[6] on “Accountability for Cloud and Other Future Internet Services”, in which we emphasised on the following items:

- Presentation on the legacy of the Cloud Accountability Project, such as the Accountability Framework, the Reference Architecture, the Lifecycle for Accountability and the contribution of the A4Cloud project to standards.
- Demonstrator Use Cases and Tools, by demonstrating the accountability tools in the context of the five scenario use cases tailored to cloud stakeholders being involved in the wearables use case.
- Provision of the Account and Assurance, by demonstrating the SPACE tool and how A4Cloud can support cloud providers in providing continuous assurance on how they handle personal data in the cloud.

Holding an exhibition booth

Apart from the workshop, during the main programme of the CloudScape event, we held an exhibition booth, aiming to demonstrate the final A4Cloud use case prototype and collect feedback from the event participants on how they realise the usefulness and applicability of the A4Cloud prototype in the future cloud security market.

Figure 19 presents the setup of the A4Cloud booth.

[5] http://www.cloudscapeseries.eu/.

[6] http://www.cloudscapeseries.eu/content/a4cloud-accountability-cloud-and-other-future-internet-services.

Figure 19: Screenshot from the A4Cloud booth at CloudScape 2016.

The demonstration of the final A4Cloud prototype both during the workshop and at the exhibition hall followed the flow adopted in the October 2015 advisory board meeting, as it was presented in Section 3.1.2, with some variations. More specifically, the five demonstration scenarios are grouped into four evaluation scenarios, each one targeting a specific community, as described below.

3.3.2.1 Business and security experts

This group consists of members of the business cloud service user community and the cloud provider technical community being responsible for the definition and enactment of security and data protection solutions for cloud services and applications. The demonstration scenario involves the A4Cloud tools for policy definition, management and enforcement, namely:

- COAT: capabilities-based selection of a compliant cloud service provider
- DPIAT: impact assessment regarding the use of a specific cloud service provider to process personal data. The use of this tool for providing a data protection impact assessment involves certificate and assessment, which is based on the defined organisational and business operations, exhibiting certain capabilities with respect to functional, security and privacy provisions, and the resulting obligations, which are compliant to social and regulatory norms and the already established SLAs, PLAs or contracts, between the selected provider and their third parties.
- DPPT for the compilation of machine readable policies, based on the human readable accountability policies and the abstract policy statements, with respect to the capabilities of the selected cloud provider, the existing SLAs, PLAs or contracts and the social and regulatory norms, which the provider has accepted to take responsibility over.
- AccLab for the contract and policy matching when preparing the machine readable policies, which is based on the abstract policy statements of the providers, expressing their capabilities from a data protection perspective.

For this scenario, the objective was to demonstrate the use of these tools resulting in the development of machine readable policies to be enforced in the cloud.

3.3.2.2 Individuals

This group consists of representatives of the end user community, who are responsible for empowering the rights of citizens, particularly with respect to privacy, and individuals selecting and using cloud

services themselves on PCs, tablets, and mobile devices. The demonstration scenario involves the A4Cloud tools for validation and remediation, namely:

- DT: provides an assessment on the compliance of the cloud providers with the claimed policies, through enabling data subjects in monitoring their data disclosures in the cloud.
- RRT: addresses the exception handling process to enable data subjects in remediation and redress. The tool provides support for responding to the discovery of an incident and the notification reports received by the end users and can be used to guide data subjects in compiling specific claims.

For this scenario, the objective was to demonstrate the use of these tools resulting end users in taking control over how their data is handled in the cloud.

3.3.2.3 Cloud Providers

This group consists of members of the cloud service market, responsible for development, deployment and operations of cloud services (in various cloud service models, like SaaS, PaaS and IaaS) and applications. The demonstration scenario involves the A4Cloud tools for the operational analysis and exception handling of cloud business (covering the accountability support services for monitoring and environment state collection, collection and management of evidence, incident management and notification), namely:

- Tools for generating and/or collecting machine-generated logs:
    - A-PPLE: generates logs with respect to actual decisions made in the policy enforcement part;
    - DTMT: generates logs with respect to data transfers occurred in a cloud environment;
    - AAS: collect slogs from various layers in protocol stack of the cloud service delivery models (SaaS, PaaS, IaaS, etc.) that may relate to potential security breaches or policy violations;
    - TL: secure and encrypted logs collection channel.
- Tools (AAS) for compiling logs into evidence records.
- Tools for incident management and notification, namely:
    - DTMT: Raises incidents about data transfers;
    - AAS: Raises incidents related to potential security breaches or policy violations;
    - IMT: Manages incidents and supports their lifetime and validity in a cloud context through generating notification reports for the appropriate recipients;

For this scenario, the objective was to demonstrate the use of these tools in the context of the wearables use case resulting in the management of incidents related to data transfer and intrusion detection attempts.

3.3.2.4 Auditors and Supervisory Authorities

This group consists of members of the business compliance process, like Cloud Auditors and Compliance Managers, responsible for regulatory and business process compliance in large, medium and small enterprises and representatives from the regulatory community, like Public regulatory agencies and Data Protection Authorities, responsible for making policy and enforcing cloud service and data protection rules. The demonstration scenario involves the A4Cloud tools for the validation of the business process compliance with data protection requirements, namely:

- AAS: demonstration of compliance to established and agreed data processing practices through the execution of (both internal and external) audits. The result of this process is the generation of audit reports, including evidence records and related objects such as related machine-generated logs and machine readable policies.

For this scenario, the objective was to demonstrate the use of AAS in the context of the wearables use case resulting in the conduction of audits, with respect to specific audit scenarios for accountability requirements.

3.3.3 Profile of the audience

Figure 20 presents a screenshot of the audience attended the workshop at the CloudScape 2016. The event was selected for demonstrating the final A4Cloud use case prototype due to the affiliation of the participants[7], coming from different community groups of the target stakeholders.

Figure 20: Screenshot from the workshop at CloudScape 2016.

The whole CloudScape event gathered together more than 130 participants working on cloud topics from industry, academia, policy makers and representative from the European Commission.

3.3.4 Presentation of results

Following a different approach than in the other evaluation events, in the CloudScape evaluation we decided to adopt a structured way to collect the feedback from the audience. To this end, we compiled a questionnaire asking from responders to reflect their perception to the demonstration scenarios and the work conducted in A4Cloud, their acceptance to the use of tools and their assessment on the impact that the project results could have on both the society and the practices followed by the community of target stakeholders.

The questionnaire is presented in Annex 6.1.

In this section, we present the results from the compilation of responses collected through this questionnaire. Unfortunately, only 5 attendees returned their responses in the form of this questionnaire. Almost half of them were in the age group of 25-35, the majority were males, holding a PhD or other post graduate degree and they were familiar with the use of cloud technologies and the provisions of the General Data Protection Regulation for the operation and use of cloud services.

User Perception

The majority of the responders found the scenarios of Section 3.3.2 interesting from a data protection perspective and comprehensive, as shown in Figure 21. From Figure 22, we understand that all the responders raise unanimity on the effectiveness of the involvement of the A4Cloud tools for the accomplishment of the scenarios, although they found it difficult to use the tools in such a scenario without any guidance, as shown in Figure 23. Finally, all the responders answered that their feeling is

[7] http://www.cloudscapeseries.eu/content/cloudscape2016-participant-list

that they received the expected outcome from the use of the A4Cloud tools in the demonstration scenarios.

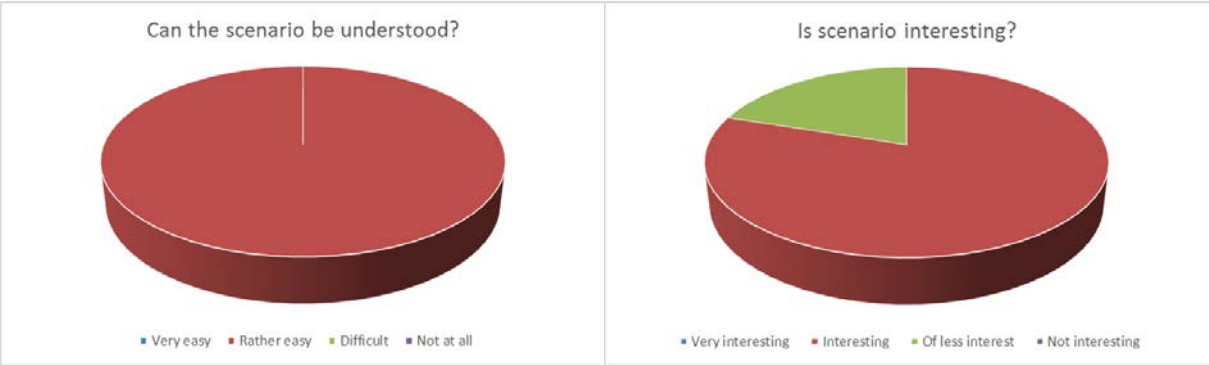

Figure 21: Assessment of the demonstration scenarios.

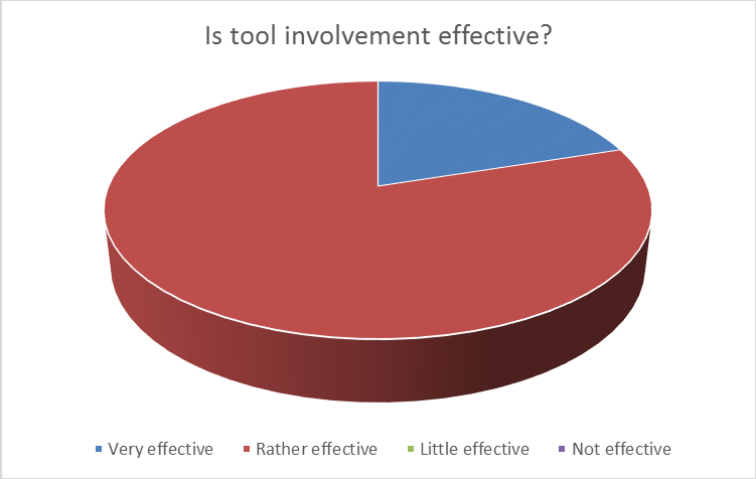

Figure 22: Perception of the responders on the effectiveness of the A4Cloud tools.

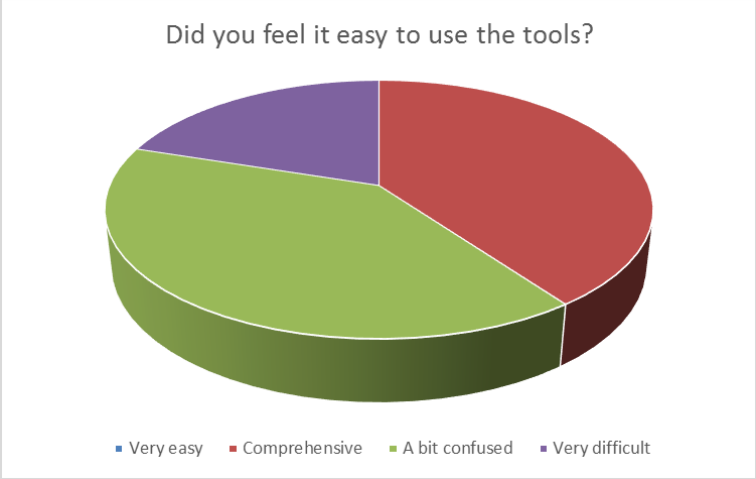

Figure 23: Perception of the responders on whether the use of the A4Cloud tools in the scenarios was easy.

User Acceptance

We summarise here the responses of the attendees with respect their acceptance to the use of the A4Cloud tools for addressing data protection and privacy requirements in a cloud environment, based on the demonstration scenarios presented to them. In Figure 24, we show that most of the responders found the tools to be rather useful for individuals, while they express some doubts for the tools

addressing the practices of cloud providers (see Figure 25). They was an expected response, since the market lacks of accountability tools targeting individuals, while a lot of security tools exist for the cloud service market. What is probably discouraging for the responders is the fact that the A4Cloud tools are software prototypes, which are the outcome of a research project, while the growth of the cloud service market demands for commercial tools, which can address the evolving threats in cloud environments.

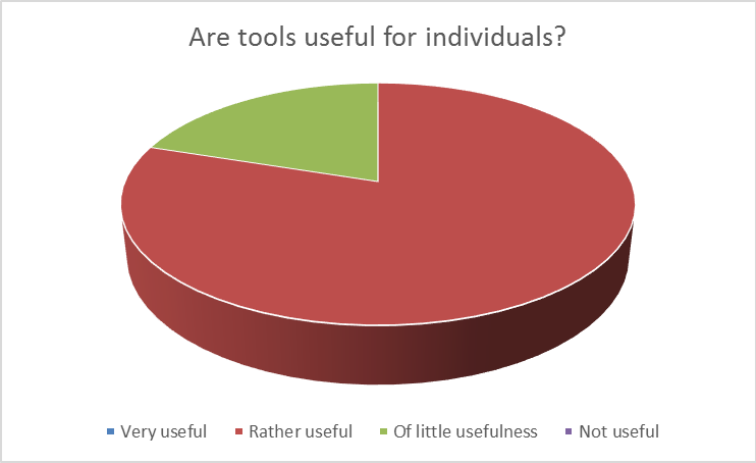

Figure 24: Usefulness of the A4Cloud tools for individuals.

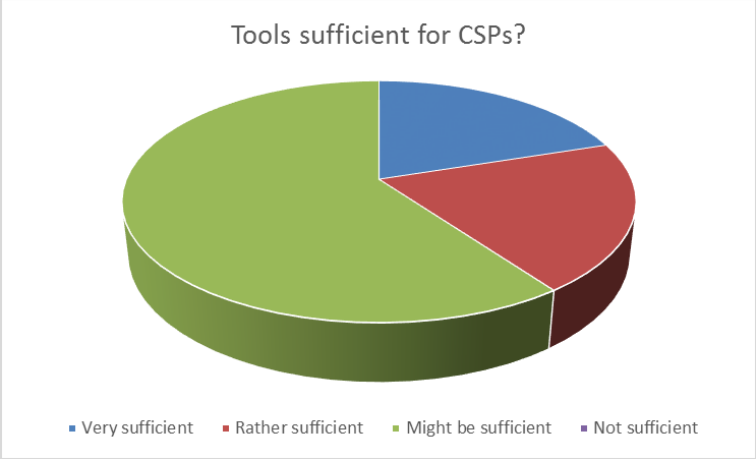

Figure 25: Sufficiency of the A4Cloud tools to address the needs of the cloud providers.

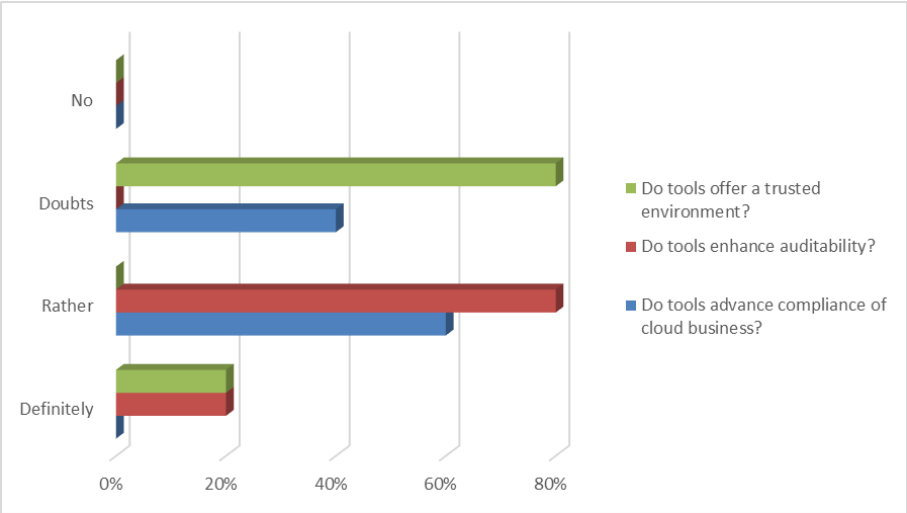

Figure 26: Summary of findings for the acceptance of the A4Cloud tools.

In Figure 26, we summarise the responses of the attendees with respect to whether the feel that the tools enhance the current practices in a cloud environment. As shown there, auditability processes can be definitely enhanced through the current maturity of the tools, while they can also support CSPs in demonstrating their compliance with regulations and policies when running a cloud business. However, further work is required to convince people that the tools themselves can facilitate trustworthiness when they are deployed in the cloud service supply chain.

Finally, Figure 27 shows that more than half of the participants realise that they should invest some time in learning how to integrate the A4Cloud tools into their cloud business.

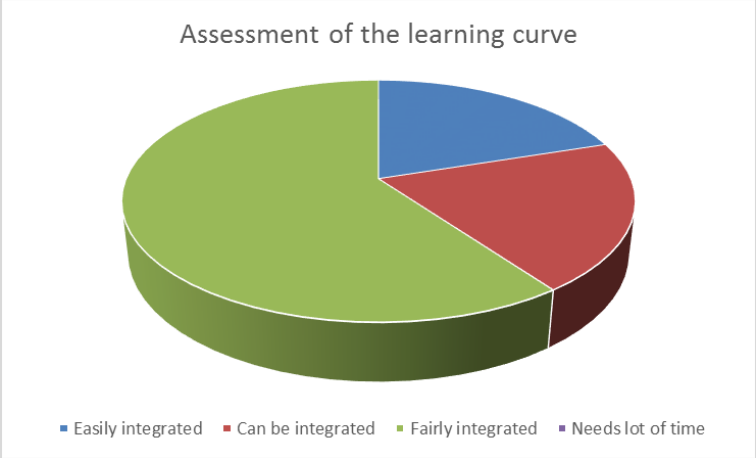

Figure 27: Assessment of the learning curve for the use of the A4Cloud tools.

Impact Assessment

Regarding the assessment of the tools impact in the target cloud security market, the majority of responders feel that the A4Cloud tools do bring benefits to the cloud market, as shown in Figure 28. In the same figure, we see that one responder did not see any benefits brought by the tools. This can be justified by the fact that the same responder felt a bit confused with the use of the tools to implement the demonstration scenarios (see Figure 23).

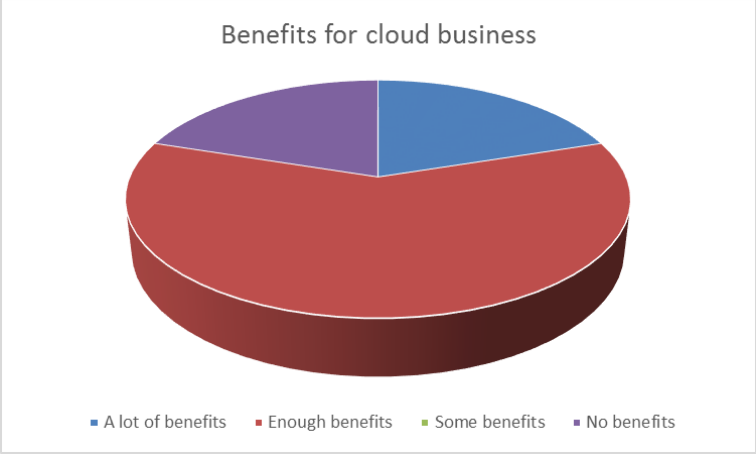

Figure 28: Assessment on whether the A4Cloud tools introduce benefits to the cloud market.

Further to it, as it is concluded from Figure 29, the attendees would be willing to adopt the tools, if they were cloud providers or customers, and they would support the use of the Cloud Accountability framework in the target community of the cloud service market. Actually, they recognise that the Cloud Accountability Reference Architecture is a pioneer result of the project, while they see a lot of challenges towards the wider use of the A4Cloud tools, mainly on the specification of the business models to run the tools and how the cloud providers would compensate any potential overhead in their system deployment.

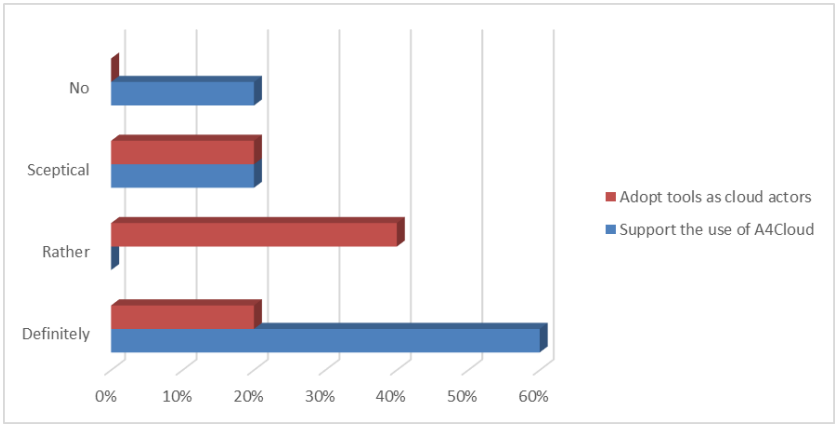

Figure 29: The responders' view on their involvement in the tools' sustainability plans.

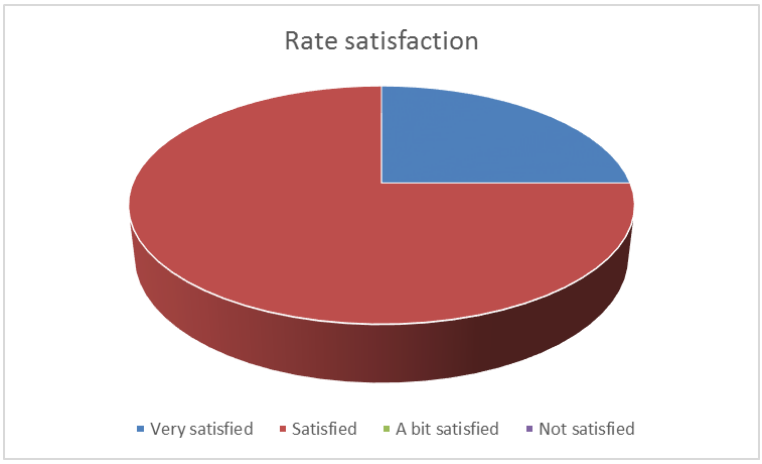

Figure 30: Overall assessment.

Overall, the responders were satisfied with the results of the A4Cloud project, as shown in Figure 30, while they pointed out that it is important for CSPs to understand the gap cost between not being accountable and being an accountable CSP to better understand whether it is worthy to implement accountability.

4 Conclusions

This deliverable presented the results of the evaluation process performed on the technical results of the A4Cloud project. More specifically, within this deliverable we participated in various dissemination events with the aim to demonstrate the first and the final A4Cloud use case prototype and how the use of the A4Cloud tools address accountability requirements for the different roles involved in a cloud environment.

The evaluation process was conducted in two phases, namely the intermediate and the final evaluation one. For each of them, the evaluation teams had the chance to provide their assessment as potential adopters of the A4Cloud tools through the demonstration of the respective releases of the A4Cloud tools and the use case prototype in the wearables domain.

Taking advantage of these activities, this report provided the results of these evaluation phases, structuring the feedback collected from the participants in the evaluation sessions into the following dimensions: i) the perception of the evaluation teams on the use of the A4Cloud prototype to implement the wearables use case, ii) the level of acceptance provided by the evaluation teams on the scope and the coverage of the A4Cloud tools to address accountability requirements, and iii) the assessment of the A4Cloud impact in the cloud security market and the practices currently adopted by the various stakeholders' groups to address privacy and data protection requirements.

As shown from the results of this evaluation, the involved stakeholders realise the potentials of the A4Cloud technical results and they expect that the tools and the cloud Accountability Reference Architecture will bring innovation into the cloud security market.

5 References

[1] A4Cloud, Deliverable D47.1: " D:D-7.1: First system and use case prototype", May 2015.

[2] A4Cloud, Deliverable D47.2: "D:D-7.2: Final system and use case prototype", March 2016.

[3] A4Cloud, Deliverable D13.3: "D:A-3.3: Report of consolidated dissemination activities", March 2016.

6 Appendices

6.1 The evaluation questionnaire

Introduction

The Cloud Accountability Project (or A4Cloud for short) focuses on the notion of accountability for cloud and other future Internet services as the most critical prerequisite for effective governance and control of personal data processed by cloud-based IT services. In A4Cloud, accountability is:

the state of accepting allocated responsibilities, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly; responsibilities being derived from law, social norms, agreements, organizational values and ethical obligations.

The project introduces the Cloud Accountability Reference Architecture, which provides an abstract, yet powerful, model for designing accountability in modern cloud and future Internet ecosystems. It is as an essential step towards addressing the requirements of the target stakeholders by defining the architecture vision and capabilities and delivering a roadmap to implement such requirements in specific cases, aligned with selected business goals.

As part of the accountability mechanisms and in order to provide support for the automated accountability interface in the implementation of cloud accountability support services, the project delivers a set of tools. More specifically, the A4Cloud tools enable cloud service providers to give their users appropriate control and transparency over how their data is used, confidence that their data is handled according to their expectations and is protected in the cloud, delivering increased levels of accountability to their customers. The tools monitor and check compliance with users' expectations, business policies and regulations and support cloud end users in making choices about how cloud service providers may use and will protect data in the cloud, and be better informed about the risks, consequences, and implementation of those choices.

This questionnaire aims to capture your perception, as being representatives of the cloud market stakeholders groups, with respect to the level that the A4Cloud tools address the objectives of accountability in a cloud service ecosystem. It also aims to identify the potentials of the tools to have a long term impact on the data protection practices in operating a cloud business.

Your feedback is highly appreciated to evaluate the usefulness of the Cloud Accountability (A4Cloud) Tools

Personal Information

Your age is between:

- ☐ 18-25
- ☐ 25-35
- ☐ 35-50
- ☐ Over 50

Your Gender is:

- ☐ Male
- ☐ Female

Your educational level is:

- ☐ High school
- ☐ Bachelors / College degree
- ☐ Post graduate degree
- ☐ Other - please specify: ……

How familiar are you with the use of cloud technologies and tools?

- ☐ Very familiar
- ☐ Rather familiar
- ☐ Little familiar
- ☐ Not familiar at all

How familiar are you with the provisions of the General Data Protection Regulation for the operation and use of cloud services?

- ☐ Very familiar
- ☐ Rather familiar
- ☐ Little familiar
- ☐ Not familiar at all

User Perception

How would you assess the demonstration scenario?

- ☐ Very easy to be understood
- ☐ Rather easy understood
- ☐ Difficult to be understood
- ☐ Not understood at all

Did you find the scenario interesting from a data protection perspective?

- ☐ Very interesting
- ☐ Interesting
- ☐ Of less interest
- ☐ Not interesting at all

How would you assess the involvement of the A4Cloud Tools to accomplish the demonstration scenario?

- ☐ The use of the tools was very effective
- ☐ The use of the tools was rather effective
- ☐ The use of the tools was little effective
- ☐ The use of the tools was not effective at all

Do you feel that you would be able to easily use the A4Cloud tools in such a scenario?

- ☐ It is very easy to use the tools
- ☐ The use of the tools is comprehensive
- ☐ I'm a bit confused on the use of the tools
- ☐ It is very difficult to use the tools

Do you feel that you got the expected outcome from the use of the A4Cloud tools in this scenario?

- ☐ Yes
- ☐ No
    - o If no, please elaborate why……

User Acceptance

If you were an individual, do you feel that the A4Cloud tools would be useful to exercise your rights in the protection of data in the cloud?

- ☐ They would be very useful
- ☐ They would be rather useful
- ☐ They would be of little usefulness
- ☐ It would not be useful at all

Do you feel that the A4Cloud tools would be sufficient to cloud providers to implement fundamental accountability functions?

- ☐ They would be very sufficient
- ☐ They would be rather sufficient
- ☐ They might be sufficient
- ☐ It would not be sufficient at all

If you were a cloud provider or a cloud customer, do you feel that the A4Cloud tools would advance the compliance of your cloud business in regards to the applied regulation framework for data protection?

- ☐ They would definitely do
- ☐ They would rather do
- ☐ I have some doubts on whether they advance it
- ☐ I do not feel that they contribute to this direction at all

Do you feel that the A4Cloud tools would enhance the auditability potentials of the cloud environment?

- ☐ They would definitely do
- ☐ They would rather do
- ☐ I have some doubts on whether they would enhance it
- ☐ I do not feel that they contribute to this direction at all

If you were a cloud provider or a cloud customer and based on the demonstration scenario, how would you assess the expected learning curve to integrate the A4Cloud tools in your cloud business?

- ☐ The tools can be easily integrated
- ☐ The tools can be integrated
- ☐ The tools can be fairly integrated
- ☐ It needs a lot of time to learn the tools

Do you feel that the A4Cloud tools offer you a trusted environment to interact in the cloud?

- ☐ They definitely offer a trusted environment
- ☐ They rather offer a trusted environment
- ☐ They might offer a trusted environment
- ☐ I would not feel confident in using A4Cloud for my cloud business

Impact Assessment

Do you feel that A4Cloud could introduce any benefits in your interaction in the cloud with respect to security, privacy and data protection aspects?

- ☐ I see a lot of benefits for my cloud business
- ☐ It could be of benefit for my cloud business

- ☐ It might be of benefit for my cloud business
- ☐ I do not see any benefits at all

Which are the main features of the A4Cloud tools that you consider as being pioneer for the implementation of accountability in the cloud environment? (Please elaborate in free text)

Do you feel that the A4Cloud tools lack on addressing any important dimension of the accountability mechanisms in the cloud? (Please elaborate in free text)

***Which are the main challenges that would you face in order to introduce A4Cloud in your current practices? (*Please elaborate in free text)**

Would you support the use of the Cloud Accountability framework in the cloud market community?

- ☐ I would definitely support
- ☐ I would rather support
- ☐ I would be hesitant in supporting
- ☐ I would not be interested to do so

If you were a cloud provider or a cloud customer, would you be willing to integrate tools like the A4Cloud tools in your current product lifecycle development?

- ☐ I would definitely do so
- ☐ I would rather do so
- ☐ I would be sceptical to do so
- ☐ I would not integrate them

How would you rate your level of satisfaction from the A4Cloud results?

- ☐ Very satisfied
- ☐ Satisfied
- ☐ A bit satisfied
- ☐ Not satisfied at all

Please provide any other remarks that you may want to share with us. (Please elaborate in free text)

7 List of Figures

Figure 1: The execution environment used for the demonstration of the A4Cloud project at the CSP EU Forum 2015. 6

Figure 2: The booth for demonstrating A4Cloud at the CSP EU Forum 2015. 7

Figure 3: Screenshots from the A4Cloud-CocoCloud workshop at the CSP EU Forum 2015. 8

Figure 4: Screenshot from the exhibition hall of the CSP EU Forum 2015. 9

Figure 5: Screenshot from the audience attending the A4Cloud presentation on implementing privacy policies in the context of the CSP EU Forum 2015. 9

Figure 6: Demonstrating A4Cloud from the perspective of the business actors in the final Advisory Board meeting. 13

Figure 7: The demonstration scenarios of the final A4Cloud use case prototype. 14

Figure 8: The setup of demonstration scenario 1 in the final advisory board meeting. 15

Figure 9: The setup of demonstration scenario 2 in the final advisory board meeting. 15

Figure 10: The setup of demonstration scenario 3 in the final advisory board meeting. 16

Figure 11: The setup of demonstration scenario 4 in the final advisory board meeting. 16

Figure 12: The setup of demonstration scenario 5 in the final advisory board meeting. 17

Figure 13: Screenshot of the audience being engaged in the demonstration of the five scenarios in the final advisory board meeting. 17

Figure 14: Screenshot from the organisation of the workshop in the context of the CSA EMEA Congress 2015. 19

Figure 15: Screenshot from the A4Cloud booth at the CSA EMEA Congress 2015. 20

Figure 16: Evaluating the A4Cloud tools for checking data protection requirements at the CSA EMEA Congress 2015. 20

Figure 17: Evaluating the A4Cloud tools for showing compliance with data protection requirements at the CSA EMEA Congress 2015. 21

Figure 18: Screenshot from the exhibition hall of the CSA EMEA Congress 2015. 21

Figure 19: Screenshot from the A4Cloud booth at CloudScape 2016. 23

Figure 20: Screenshot from the workshop at CloudScape 2016. 25

Figure 21: Assessment of the demonstration scenarios. 26

Figure 22: Perception of the responders on the effectiveness of the A4Cloud tools. 26

Figure 23: Perception of the responders on whether the use of the A4Cloud tools in the scenarios was easy. 26

Figure 24: Usefulness of the A4Cloud tools for individuals. 27

Figure 25: Sufficiency of the A4Cloud tools to address the needs of the cloud providers. 27

Figure 26: Summary of findings for the acceptance of the A4Cloud tools. 27

Figure 27: Assessment of the learning curve for the use of the A4Cloud tools. 28

Figure 28: Assessment on whether the A4Cloud tools introduce benefits to the cloud market. 28

Figure 29: The responders' view on their involvement in the tools' sustainability plans. 29

Figure 30: Overall assessment. 29